RENACE
cada 11 tiene su 13

El IMPERIO de la VIGILANCIA

IGNACIO RAMONET

ediciones MINCI

EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES
DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL
MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI -
EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES
DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL
MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI -
EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES
DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL
MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI -
EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES
DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL
MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI -
EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES
DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL
MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI -
EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES
DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL
MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI -
EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES
DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL
MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI -
EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES
DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL
MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI -
EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES
DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL
MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI -
EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES
DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL
MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI -
EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES
DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL
MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI -
EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES
DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL
MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI -
EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES
DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL
MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI -
EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES
DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL
MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI -
EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES
DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL MINCI - EDICIONES DEL

REPÚBLICA BOLIVARIANA DE VENEZUELA

NICOLÁS MADURO MOROS
PRESIDENTE DE LA REPÚBLICA BOLIVARIANA DE VENEZUELA

DELCY ELOÍNA RODRÍGUEZ
VICEPRESIDENTA DE LA REPÚBLICA BOLIVARIANA DE VENEZUELA

FREDDY ÑÁÑEZ CONTRERAS
VICEPRESIDENTE SECTORIAL DE COMUNICACIÓN Y CULTURA (E)

EDGAR PADRÓN
VICEMINISTRO DE PLANIFICACIÓN Y ESTRATEGÍA COMUNICACIONAL

ISBEMAR JIMÉNEZ
VICEMINISTRA DE GESTIÓN COMUNICACIONAL

MARDI MEDINA
VICEMINISTRA DE SOPORTE DE PLATAFORMA COMUNICACIONAL

JOHANIL RODRÍGUEZ
VICEMINISTRO DE COMUNICACIÓN E INFORMACIÓN

EL IMPERIO DE LA VIGILANCIA

IGNACIO RAMONET

Nació en Redondela, Pontevedra (España) en 1943. Doctorado en Semiología e Historia de la Cultura en la École des Hautes Études en Sciencies Sociales de París, ha desarrollado una vasta y prestigiosa carrera periodística. Desde 1990 hasta 2008 dirigió la edición francesa de *Le Monde Diplomatique*, y desde ese año la edición española del periódico. Cofundador de la organización no gubernamental Media Watch Global (Observatorio Internacional de los Medios de Comunicación), fundador y presidente de honor de la organización ATTAC, es unos de los promotores del Foro Social Mundial de Porto Alegre.

Ramonet es autor o coautor de una veintena de libros, entre los que se puede mencionar *La tiranía de la comunicación* (1998); *La golosina visual* (2000); *Marcos, la dignidad rebelde* (2001); *Guerras del siglo XXI* (2002); *Irak: historia de un desastre* (2005); *Fidel Castro: biografía a dos voces* (2006); *París rebelde: guía política y turística de una ciudad* (2008); *La catástrofe perfecta: crisis del siglo y refundación del porvenir* (2010); *La explosión del periodismo: Internet pone en jaque a los medios tradicionales* (2011) y *Hugo Chávez: mi primera vida* (2013). De este último la editorial José Martí realizó la edición cubana en el año 2014.

EL IMPERIO de la VIGILANCIA

IGNACIO RAMONET

ediciones MINCI

ediciones MINCI

EL IMPERIO DE LA VIGILANCIA
© Ignacio Ramonet

Primera edición, 2016
Editorial Galilée, París / Clave Intelectual, Madrid
Traductor del francés Martín Sacristán

Primera reimpresión, 2018
Editorial José Martí, Cuba

Segunda edición, 2022
© Ediciones del Minci
Ministerio del Poder Popular
para la Comunicación e Información

Al cuidado de
Freddy Ñáñez

Revisión de los textos
Yulianny Morales y Coral Pérez

Diseño y cuidado de edición gráfica
José Gregorio Vásquez

Imagen de portada
© https://pixabay.com/es/users/bertsz-1667539

Foto de autor
Foto de archivo personal

HECHO EL DEPÓSITO DE LEY:
Depósito Legal: DC2022000398
ISBN: 978-980-227-465-9

Ediciones MinCI
Ministerio del Poder Popular para la Comunicación e Información
Final Bulevar Panteón, Torre Ministerio del Poder Popular
para la Comunicación e Información
Parroquia Altagracia, Caracas-Venezuela.
Teléfonos (0212) 8028314-8028315 - Rif: G-20003090-9

Impreso en Venezuela

AGRADECIMIENTOS

Debo comenzar por expresar mi total reconocimiento a Michel Foucault, del que fui asiduo oyente en el Collège de France, especialmente por su curso sobre «La sociedad punitiva», en 1972-1973, que completó más adelante en su obra fundamental *Surveiller et punir* (1975), y también porque fue el primero que nos puso en guardia contra la perspectiva de una sociedad que busca el control absoluto y la vigilancia total.

Mi homenaje también para mi amigo Armand Mattelart, cuya obra entera da testimonio de su preocupación crítica contra los aparatos de manipulación de masas, y cuyo magistral libro *La Globalisation de la surveillance* (2008) establece una base teórica indispensable para todo estudio serio sobre el nuevo orden *securitario*.

Mi profundo reconocimiento a Adrien Gévaudan, gran conocedor de este tema, que como prueba de amistad, ha aceptado dedicar una parte de su tiempo a la fastidiosa tarea de releer mi manuscrito. Sus muchas y pertinentes observaciones y sus fecundas sugerencias me han permitido

hacer nuevas e indispensables aportaciones que han enriquecido considerablemente el texto.

Mis grandes amigos y colegas habituales: Bernard Cassen y Christophe Ventura, también han releído atentamente el manuscrito. El libro no hubiera sido lo mismo sin sus importantes y decisivas observaciones. Mi inmenso agradecimiento para los dos.

Mi cariñosa gratitud también para mi hijo Flavien, de 21 años, diplomado en Ciencias Políticas, que ha realizado una lectura analítica muy minuciosa y exigente del manuscrito. Sus múltiples anotaciones y sus comentarios críticos —en los que he creído ver en cierta medida, los de su joven generación— han sido una aportación esencial.

Finalmente, este libro no habría podido ver la luz sin la amistosa atención de mi editor de siempre: Michel Delorme. Su apoyo, así como el del pequeño y valiente equipo de Galilée, especialmente los de las talentosas Cécile Bourguignon y Agnès Rauby, han sido cálidos estímulos para llegar al final del trabajo de documentación y de escritura.

A propósito de esta edición cubana, desearía expresar mi particular agradecimiento al editor Jorge Fernández Era por su meticulosa y exigente relectura. También a mis queridos amigos Lydia y Camilo Pérez Casal por sus aportes fundamentales, así como a todos los amigos del Instituto Cubano del Libro y en particular de la Editorial José Martí.

Para todos, mi reconocimiento más afectuoso.

INTRODUCCIÓN

«Vigilar: observar atentamente algo
o a alguien para controlarlo».
Diccionario Larousse

Durante mucho tiempo, la idea de un mundo «totalmente vigilado» ha parecido un delirio utópico o paranoico, fruto de la imaginación más o menos alucinada de los obsesionados por los complots. Sin embargo, hay que rendirse a la evidencia: aquí y ahora vivimos bajo el control de una especie de *imperio de la vigilancia*. Sin que nos demos cuenta, estamos cada vez más siendo observados, espiados, vigilados, controlados, fichados. Cada día se perfeccionan nuevas tecnologías para el rastreo de nuestras huellas. Empresas comerciales y agencias publicitarias cachean nuestras vidas. Con el pretexto de luchar contra el terrorismo y otras plagas,[1] los gobiernos, incluso los más

1 Julian Assange afirma que las democracias se enfrentan, de hecho, a los «cuatro jinetes del *infocalipsis*»: el terrorismo, la pornografía infantil, el blanqueo de dinero y las guerras contra la droga y el narcotráfico. Cada una de estas plagas, a las que evidentemente hay que combatir, sirve también de pretexto para reforzar permanentemente los sistemas de vigilancia global sobre las poblaciones. Julian Assange y Jacob Apppelbaum, Andy Müller-Maughn y Jérémie Zimmerman, *Ménace sur nos libertés. Comment Internet nus espionne. Comment résister.*

democráticos, se erigen en Big Brother y no dudan en quebrantar sus propias leyes para poder espiarnos mejor.

En secreto, los nuevos Estados "orwellianos" intentan, muchas veces con la ayuda de los gigantes de la Red, elaborar exhaustivos ficheros de nuestros datos personales y de nuestros contactos,[2] extraídos de los diferentes soportes electrónicos.

Tras la oleada de ataques terroristas que desde hace veinte años viene golpeando ciudades como Nueva York, Washington, París, Toulouse, Bruselas, Boston, Ottawa, Oslo, Londres, Madrid, Túnez, Marrakech, Casablanca, Ankara, etc., las autoridades no han dejado de utilizar el enorme pavor de una sociedad en estado de *shock* para intensificar la vigilancia y reducir en la misma proporción, la protección de nuestra vida privada.

Que se entienda bien: el problema no es la vigilancia en general, es la *vigilancia clandestina masiva.* Ni qué decir tiene: que en un Estado democrático las autoridades están completamente legitimadas para vigilar a cualquier persona que consideren sospechosa, apoyándose en la ley y con la autorización previa de un juez. Como dice Edward Snowden:

> No hay problema cuando se trata de escuchas telefónicas a Osama Bin Laden. Los investigadores pueden hacer este trabajo mientras tengan permiso de un juez —un juez independiente,

2 Se trata esencialmente de informaciones que permiten identificarnos, ya sea directa o indirectamente. A saber: nombre y apellidos, foto, fecha y lugar de nacimiento, estado civil, dirección postal, número de la seguridad social, número de teléfono, número de tarjeta bancaria, placa de la matrícula del vehículo, correo electrónico, cuentas de redes sociales, dirección IP del ordenador, grupo sanguíneo, huellas digitales, huella genética, elementos de identificación biométrica, etc.

> un juez de verdad, no un juez anónimo—, y puedan probar que hay una buena razón para autorizar la escucha. Y así es como se debe hacer. El problema surge cuando nos controlan a todos, en masa y todo el tiempo, sin una justificación precisa para interceptar nuestras comunicaciones, sin indicio jurídico alguno que demuestre que hay una razón plausible para violar nuestros derechos.[3]

Con la ayuda de algoritmos cada vez más perfeccionados, miles de investigadores, ingenieros, matemáticos, estadísticos e informáticos persiguen y criban las informaciones que generamos sobre nosotros mismos. Desde el espacio nos siguen satélites y drones de mirada penetrante. En las terminales de los aeropuertos, escáneres biométricos analizan nuestros pasos, leen nuestro iris y nuestras huellas digitales. Cámaras infrarrojas miden nuestra temperatura corporal. Las pupilas silenciosas de cámaras de video nos escudriñan en las aceras de las ciudades o en los pasillos de los supermercados.[4] Nos siguen la pista también en la oficina, en las calles, en el autobús, en el banco, en el metro, en el estadio, en los aparcamientos, en los ascensores, en los centros comerciales, en carreteras, estaciones, aeropuertos…

Además, con el desarrollo en marcha de la «Internet de las cosas», muchos elementos de nuestro hogar (refrigerador, botiquín, bodega, etc.), incluso nuestro vehículo,[5] van a suministrar también informaciones valiosas sobre nuestras costumbres más personales.

---

3 Katrina Vanden Heuvel y Stephen F. Cohen, «Entrevista con Edward Snowden», *The Nation*, Nueva York, 28 de octubre de 2014. *Le Monde Diplomatique* en español, octubre de 2015.

4 Como se puede ver claramente en la película *La Loi du marché*, de Stéphane Brizé, 2015.

5 «La voiture, cette espionne», *Le Monde*, 2 de octubre de 2015.

Hay que decir que la inimaginable revolución digital que estamos viviendo y que trastoca ya tantas actividades y profesiones, también ha desbaratado completamente el campo de la información y el de la vigilancia. En la era de Internet, la vigilancia se ha vuelto omnipresente y totalmente inmaterial, imperceptible, indetectable, invisible. Además, ya es técnicamente de una excesiva sencillez.

Software espía

Ya no son necesarios toscos trabajos de albañilería para instalar cables y micros, como en la célebre película *La conversación*,[6] en la que un grupo de fontaneros presenta en un salón dedicado a las técnicas de vigilancia, chivatos más o menos chapuceros, equipados con cajas rebosantes de hilos eléctricos, que había que disimular en las paredes o bajo los techos. Varios estrepitosos escándalos de la época —el caso Watergate,[7] en los Estados Unidos; el de los fontaneros de Le Canard,[8] en Francia— fueron fracasos humillantes de los servicios de información, que mostraron los límites de estos viejos métodos mecánicos, fácilmente detectables y perceptibles.

---

6 Francis Ford Coppola, 1973.

7 El caso Watergate fue un asunto de espionaje político con múltiples ramificaciones, que empezó con la detención, en 1972, de falsos ladrones que habían colocado micrófonos en las oficinas del Partido Demócrata, en el edifico Watergate, en Washington, y desembocó en la dimisión en 1974 de Richard Nixon, presidente de los Estados Unidos.

8 Escándalo político bajo la presidencia de Georges Pompidou. En diciembre de 1973, en París, se descubrió en los locales del semanario satírico *Le Canard enchaîné* un sistema de escuchas que habían colocado una decena de agentes de la Dirección de la Vigilancia del Territorio (DST: siglas en francés), disfrazados de fontaneros.

En la actualidad, poner a alguien bajo escucha es asombrosamente fácil y está al alcance de cualquiera. Quien quiera espiar su entorno encuentra una larga lista de opciones[9] de libre acceso en el comercio, en primer lugar manuales de instrucción muy didácticos «para aprender a seguir la pista y espiar a la gente».[10] Y al menos media docena de *software* espías (mSpy, GSmSpy, FlexiSpy, Spyera, EasySpy) que leen sin problemas el contenido de los teléfonos móviles[11] y sus sms, así como de correos electrónicos, cuentas en Facebook, WhatsApp, Twitter, etc.

Con el impulso del consumo en línea se ha desarrollado considerablemente la vigilancia de tipo comercial, que ha generado un gigantesco mercado de datos personales, convertidos en mercancía. Cuando nos conectamos a una web, las *cookies*[12] guardan en la memoria el conjunto de las búsquedas realizadas, lo que permite establecer nuestro perfil de consumidor. En menos de veinte milisegundos, el

---

9 Aunque el artículo 226-1 del Código Penal francés impone una pena «de un año de prisión y 45.000 euros de multa por atentar voluntariamente, mediante cualquier procedimiento, contra la intimidad de la vida privada de otro: captando, grabando o transmitiendo, sin el consentimiento de su autor, palabras pronunciadas a título privado o confidencial; fijando, grabando o transmitiendo, sin su consentimiento, la imagen de una persona mientras se encuentra en un lugar privado».

10 Léase, por ejemplo, Charles Cohle, *Je sais qui vous êtes. Le manuel d'espionnage sur Internet*, Institut Pandore, Nantes, 2014.

11 Incluso existen «comparadores de *software* de vigilancia» que la publicidad presenta de esta manera: «Un comparador claro y completo de los programas chivato para el móvil, que le permitirá elegir y poder tomar una decisión acertada y económica antes de comprar su aplicación de localización» (http://www.smartsupervisors.com/).

12 La *cookie* equivale a un pequeño archivo de texto almacenado en el terminal del internauta. Permite a los programadores de sitios de Internet conservar los datos del usuario con el fin de facilitar su navegación. Las *cookies* siempre han sido cuestionadas, ya que contienen información personal residual que potencialmente puede ser utilizada por terceros. (Fuente: Wikipedia).

editor de la página que visitamos vende a potenciales anunciadores informaciones que nos afectan. Apenas algunos milisegundos después, aparece en nuestra pantalla la publicidad que supuestamente tiene más impacto en nosotros. Y ya estamos definitivamente fichados.[13]

Una alianza sin precedentes

En cierto modo, la vigilancia se ha privatizado y «democratizado». Ya no es un asunto reservado únicamente a los servicios gubernamentales de información. Aunque —gracias también a la estrecha complicidad que los Estados han entablado con las grandes empresas privadas que dominan las industrias de la informática y de las telecomunicaciones— su capacidad en materia de espionaje de masas ha crecido de forma exponencial. En la entrevista con Julian Assange que publicamos en la segunda parte de este libro, el fundador de WikiLeaks[14] afirma:

> Las nuevas empresas, como Google, Apple, Microsoft, Amazon y más recientemente Facebook han establecido estrechos lazos con el aparato del Estado en Washington, especialmente con los responsables de la política exterior. Esta relación se ha convertido en una evidencia (…). Comparten las mismas ideas políticas y tienen idéntica visión del mundo. En última instancia, los estrechos vínculos y la visión común del mundo de Google y la Administración estadounidense están al servicio de los objetivos de la política exterior de los Estados Unidos.[15]

---

13 http://digital-society-forum.orange.com/fr/.

14 Sobre WikiLeaks, léase *La explosión del periodismo*, Ignacio Ramonet, Clave Intelectual, Madrid, y *Capital Intelectual*, Buenos Aires, 2011, pp. 93-123.

15 *Infra*, p. 138.

Esta alianza sin precedentes —Estado más aparato militar de seguridad más industrias gigantes de la Web— ha creado este imperio de la vigilancia cuyo objetivo claro y concreto es poner Internet y a todos los internautas bajo escucha.

En esta situación, es necesario tener en cuenta dos ideas muy concretas:

1. El ciberespacio se ha convertido en una especie de quinto elemento. El filósofo griego Empédocles sostenía que nuestro mundo estaba formado por una combinación de cuatro elementos: tierra, aire, agua y fuego. Pero el surgimiento de Internet, con su misterioso interespacio superpuesto al nuestro, formado por miles de millones de intercambios digitales de todo tipo, por su *streaming* y su *clouding,* ha engendrado un nuevo universo, en cierto modo cuántico, que viene a completar la realidad de nuestro mundo contemporáneo como si fuera un auténtico quinto elemento.

   En este sentido, hay que señalar que cada uno de los cuatro elementos tradicionales constituye históricamente un campo de batalla, un lugar de confrontación. Desde el desarrollo de la aviación militar en 1914-1918, los Estados han tenido que desarrollar componentes específicos de las fuerzas armadas para cada uno de estos elementos: el Ejército de tierra, el Ejército del aire, la Armada y con carácter más singular, los bomberos o «guerreros del fuego». De manera natural, todas las grandes potencias han añadido hoy, a los tres ejércitos tradicionales y a los combatientes del fuego, un ejército cuyo ecosistema es el quinto elemento:

el ciberejército, encargado de la ciberdefensa, que tiene sus propias estructuras orgánicas, su estado mayor, sus cibersoldados y sus propias armas: superordenadores preparados para librar la ciberguerra digital[16] en el ámbito de Internet.

2. Internet se ha centralizado. Al principio, se percibió la Red como una explosión de posibilidades de expresión individuales, que permitía escapar de la dependencia de los monopolios estatales (correos, telégrafo, teléfono…), de los gigantes de las telecomunicaciones y de los grandes medios de comunicación dominantes (prensa, radio, televisión). Era sinónimo de libertad, de evasión, de creatividad. Veinticinco años después, la Red está a punto de sufrir una violenta centralización en torno a ciertas colosales empresas privadas: las Gafam (Google, Apple, Facebook, Amazon, Microsoft), todas estadounidenses, que a escala planetaria acaparan las diferentes facetas de la red, y de las que son extraordinariamente dependientes los aproximadamente tres mil quinientos millones de internautas, quienes a su vez, las alimentan con todos sus datos personales. Y de este modo, las enriquecen descomunalmente.

Para las generaciones de menos de 40 años, la Red es sencillamente el ecosistema en el que han madurado su pensamiento, su curiosidad, sus gustos y su personalidad.[17]

---

16 «Entrevista exclusiva: vicealmirante Arnaud Coustillière, oficial general *ciberdefensa* del estado mayor de los ejércitos», *Cyber Risques News*, 7 de abril de 2015. http:// www.cyberisques.com/fr/motscles-11/433-entretien-exclusif-vice-admiral-arnaud-coustulliere-officier-general-cyberdefenseal-etat-major-des-armees.

17 Es interesante destacar que si el 60 % de los franceses percibe la existencia

Para ellos, Internet no es solo una herramienta autónoma que se utiliza para tareas concretas. Es una inmensa esfera intelectual, en la que se aprende a explorar libremente todos los saberes. Y al mismo tiempo, un ágora sin límites, un foro donde la gente se encuentra, dialoga, intercambia y adquiere cultura, conocimientos y valores, generalmente compartiéndolos.

Para estas nuevas generaciones, Internet representa lo que para sus antepasados fueron simultáneamente la escuela y la biblioteca, el arte y la enciclopedia, la ciudad y el templo, el mercado y la cooperativa, el estadio y el escenario, el viaje y los juegos, el circo y el burdel… Es tan fabuloso que «por el placer de evolucionar en un universo tecnológico, el individuo no se preocupa de saber y aún menos de comprender, que las máquinas gestionan su vida cotidiana. Que cada uno de sus actos y gestos es registrado, filtrado, analizado y eventualmente vigilado. Que, lejos de liberarle de sus ataduras físicas, la informática de la comunicación constituye sin duda la herramienta de vigilancia y control más formidable que el hombre haya puesto a punto jamás».[18]

Y esto no ha acabado, ya que, insaciables, los gigantes de la Red —Google, Facebook y, concretamente Microsoft— quieren ahora extender su dominio al conjunto de la humanidad, con el pretexto de la emancipación y la liberación. Paul Virilio, al evocar las catástrofes industriales, que

---

de ficheros de vigilancia como un «atentado a la vida privada», el intervalo de edad de los 18 a los 24 años, es decir, el de los principales usuarios de Internet, es el que se muestra más preocupado en este sentido: el 78 % de ellos denuncia que su vida privada está insuficientemente protegida en Internet. Estudio realizado a instancias de la Comisión Nacional de Informática y Libertades (CNIL), París, 2008.

18 Jean Guisnel, prólogo a la edición francesa de *Tous fliqués! La vie privée sous surveillance*, de Reg Whitaker, Denoël, París, 2001.

son por definición contemporáneas a la era industrial, nos ha enseñado que, por ejemplo, la invención del ferrocarril conllevó simultáneamente la invención de los accidentes de tren. Con la Web pasa algo parecido. La catástrofe industrial de Internet es la vigilancia masiva, de la que solo escapan —consuelo de pobres— los que no tienen Internet, es decir, alrededor de la mitad de los habitantes del planeta.

Pero los gigantes de la Red quieren acabar con esta injusticia: «Si conectamos a Internet a los cuatro mil millones de personas que no tienen acceso a la Red, tenemos la oportunidad histórica de educar al conjunto del mundo en las próximas décadas», ha declarado, por ejemplo, el dueño de Facebook, Mark Zuckerberg.[19]

El 26 de septiembre de 2015, Zuckerberg, Bill Gates —fundador de Microsoft—, Jimmy Wales —fundador de Wikipedia— y otros,[20] insistieron ante la Organización de las Naciones Unidas (Onu), inscribiendo su posición en el marco de los objetivos de desarrollo sostenible fijados por esta para erradicar la pobreza extrema hasta el año 2030:[21] «Internet pertenece a todo el mundo, por lo tanto debe ser accesible a todo el mundo».[22] Aunque Facebook no había esperado para lanzar, en agosto de 2013, Internet.org, una aplicación para *smartphones* que permite a los países pobres acceder gratuitamente a la red Facebook y a una selección de unos cuarenta sitios web, Wikipedia entre ellos.[23]

---

19 «To Unite the Earth, Connect It», *The New York Times*, 26 de septiembre de 2015.

20 El propietario de Virgin, Richard Branson; la fundadora del *Huffington Post*, Ariana Huffington; el cantante Bono, la actriz Charlize Theron, la cantante Shakira, el actor George Takei, etc.

21 http://www.globalgoals.org.

22 AFP, 27 de septiembre de 2015.

23 Aunque sobre el papel es elogiable, el proyecto se enfrenta a fuertes críti-

Por su parte, Alphabet (Google) ha puesto a punto su propio proyecto de ampliar al mundo entero el acceso a Internet. Para proporcionar gratuitamente a los condenados de la Tierra los beneficios de su motor de búsqueda, esta empresa global cuenta sobre todo con apoyarse en su programa Loon: globos de helio instalados en la estratosfera.

Sin dudar en absoluto de la intención de estos gigantes de la Red de mejorar el destino de la humanidad, podemos preguntarnos si no les motivan también consideraciones más comerciales, puesto que la principal riqueza de estas empresas ineludibles —casi en situación de monopolio planetario— es el número de conectados. Facebook o Google, por ejemplo, no venden nada a los internautas: venden sus miles de millones de usuarios a los anunciantes publicitarios. Es lógico, por lo tanto, que a partir de ahora quieran venderles a *todos* los habitantes de la Tierra. Simultáneamente, cuando el mundo entero esté conectado, podrán transmitir a la Agencia de Seguridad Nacional,[24] en una doble operación, todos los datos personales de todos los habitantes de la Tierra… ¡Bienvenidos al imperio de la vigilancia!

---

cas, especialmente en la India. Estos son los reproches: con internet.org, Facebook perjudicaría la neutralidad de la Red al decidir por sí mismo los sitios web a los que se pueden conectar los internautas. Además, crearía una Red a dos velocidades: la de los ricos, capaces de acceder a toda ella, y la de los pobres, conectados únicamente a algunos servicios. Léase, por ejemplo, *Le Monde*, París, 29 de diciembre de 2015.

24 La National Security Agency (NSA), situada en Fort Meade, Maryland, es un organismo relevante del Departamento de Defensa de los Estados Unidos, y fue creada en 1952 agrupando a las diferentes agencias de información militares (ejército, marina, aviación…).

Este propósito de control total de Internet representa, para nuestras sociedades democráticas, un peligro inédito: «Permitir la vigilancia de Internet —afirma Glenn Greenwald, el periodista estadounidense que difundió las revelaciones de Edward Snowden— [25] llevaría a someter a un exhaustivo control estatal prácticamente todas las formas de interacción humana, incluido el pensamiento mismo».[26]

Esta es la gran diferencia con respecto a los sistemas de vigilancia del pasado. Sabemos, siguiendo a Michel Foucault, que la vigilancia ocupa un lugar primordial en la organización de las sociedades modernas, que son también «sociedades disciplinarias», en las que el poder trata de ejercer el mayor control social posible mediante complejas técnicas y estrategias de vigilancia.[27]

Esta voluntad del Estado de saberlo todo sobre sus ciudadanos se legitima políticamente mediante la promesa de una mayor eficacia en la administración burocrática de la sociedad: el Estado afirma que será mucho más eficaz y por

---

25 Edward Snowden nació el 21 de junio de 1983. Exconsultor de los servicios secretos estadounidenses, trabajó para la CIA y la NSA. Reveló los detalles de varios programas estadounidenses y británicos de vigilancia masiva. Como consecuencia de sus revelaciones, el 22 de junio de 2013 el Gobierno de los Estados Unidos lo acusó de espionaje, robo y «utilización ilegal de bienes gubernamentales». Refugiado en Hong Kong en junio de 2013, pidió asilo político a veintiún países, entre ellos Francia. El 1 de agosto de 2014 obtuvo el derecho a residir en Rusia durante tres años. (Fuente: Wikipedia).

26 Glenn Greenwald, *No Place to Hide, Edward Snowden, the NSA and the US Surveillance State,* Metropolitan Books, Nueva York, 2014; edición en español: *Sin un lugar donde esconderse,* Ediciones B, 2014.

27 Michel Foucault, *Surveiller et punir*, Gallimard, París, 1975; edición en español: *Vigilar y castigar,* Biblioteca Nueva, 2012.

lo tanto, servirá mucho mejor a los ciudadanos si los conoce mejor, mucho más profundamente. No obstante, al ser cada vez más invasiva, la intromisión del Estado ha terminado por provocar, desde hace tiempo, un creciente rechazo por parte de los ciudadanos apegados al santuario de su vida privada. En 1819, Benjamin Constant, en su célebre discurso «De la libertad de los antiguos comparada con la de los modernos», reclamaba la protección de la esfera privada. Y ya en 1835, Alexis de Tocqueville señalaba que las modernas democracias de masas crean ciudadanos individuales, una de cuyas principales preocupaciones es la protección de sus derechos. Y esto los hace especialmente puntillosos y beligerantes contra las abusivas pretensiones de intromisión del Estado.[28]

Esta tradición se prolonga hoy en la persona de los «lanzadores de alertas», como, por ejemplo, Julian Assange y Edward Snowden, ambos ferozmente perseguidos por las autoridades de los Estados Unidos, y a quienes defiende valientemente el gran intelectual estadounidense Noam Chomsky en la entrevista que se publica en la segunda parte de este libro:

> En lo que respecta a los lanzadores de alertas, su lucha por una información libre y transparente es una cosa casi natural. ¿Tendrán éxito? Eso depende de la gente. Si Snowden, Assange y otros hacen lo que hacen, es en calidad de ciudadanos. Están ayudando a la opinión pública a descubrir lo que hacen sus propios gobiernos. ¿Existe algo más noble para un ciudadano libre? Y se les quiere castigar. Si los Estados Unidos pudieran echarles el guante, sería peor… En los Estados Unidos hay una ley de espionaje que data de la Primera Guerra Mundial; Obama se ha servido de ella para evitar que las informaciones difundidas por Assange y Snowden lleguen al público. El Gobierno va a

28 Alexis de Tocqueville, *La democracia en América*, Akal, 2007.

intentarlo todo, incluso lo inconfesable, para protegerse de su «enemigo principal». Y el «enemigo principal» de todo gobierno es su propio pueblo.[29]

¿El fin de la vida privada?

En la era de Internet, el control del Estado puede alcanzar dimensiones alucinantes. Porque de una u otra forma, ahora confiamos a Internet nuestros pensamientos más personales e íntimos, tanto profesionales como emocionales. Por eso, cuando el Estado decide escanear nuestro uso de la Web con la ayuda de tecnologías superpotentes, no solo sobrepasa sus funciones, sino que profana nuestra intimidad, deshuesa literalmente nuestra alma y saquea el refugio de nuestra vida privada.

Sin que tengamos conciencia de ello, a ojos de los nuevos «Estados de control» nos volvemos semejantes al protagonista de la película *El show de Truman*,[30] directamente expuestos a la mirada de miles de cámaras y bajo la escucha de miles de micrófonos que exponen nuestra vida privada a la curiosidad planetaria de los servicios de información.

En este sentido, Vinton Cerf, uno de los creadores de la red, piensa que «en la época de las modernas tecnologías digitales, la vida privada es una anomalía».[31] Leonard Kleinrock, uno de los pioneros de Internet, es incluso más pesimista: «Esencialmente —dice—, nuestra vida privada se ha terminado, y puede decirse que es imposible recuperarla».[32]

---

29 *Infra*, p. 170.

30 Peter Weir, *The Truman Show*, 1998.

31 *Marianne*, 10 de abril de 2015.

32 *El País*, Madrid, 13 de enero de 2015.

Tanto más cuanto que las empresas privadas, sobre todo las Gafam, tratan también de saber lo máximo sobre nosotros, invocando los beneficios que un mayor conocimiento de nuestros datos personales podría procurarnos, de acuerdo con el principio: «Dime todo sobre ti, y te serviré mejor». Que en realidad quiere decir: «Te controlaré mejor y ya no podrás escapar de mí».

Muchos ciudadanos se resignan a que se ponga fin a su derecho al anonimato, como si fuera una especie de fatalidad de nuestro tiempo. Ante esta indiferencia respecto a una de nuestras libertades fundamentales, reacciona el sociólogo Zygmunt Bauman, que exclama: «Lo que me asusta no es la llegada de una sociedad de la vigilancia, sino que vivamos ya en ella sin que ello nos preocupe». Por otra parte, el deseo de defender nuestra vida privada puede parecer reaccionario o sospechoso, porque solo los que tienen algo que ocultar tratan de esquivar el control público. Por lo tanto, las personas que piensan que no tienen nada que reprocharse, nada que esconder, no son hostiles a la vigilancia del Estado, sobre todo, si como prometen las autoridades, la vigilancia va acompañada de sustanciales beneficios en materia de seguridad.

Pero este discurso: «Dadme un poco de vuestra libertad y os devolveré el céntuplo en seguridad», es una trampa para pardillos. La seguridad total no existe, no puede existir. Mientras que la vigilancia total se ha convertido, por el contrario, en una realidad cada vez más verosímil.

Contra la estafa de la seguridad, cantinela constante de todos los poderes, recordemos la lúcida advertencia lanzada por Benjamin Franklin, uno de los padres de la Constitución de los Estados Unidos: «Un pueblo dispuesto a sacrificar un poco de libertad por un poco de seguridad no merece

ni una ni otra. Y acaba perdiendo las dos». Una reflexión de completa actualidad, que debería alentarnos a defender nuestro derecho a la vida privada, cuya principal función no es otra que salvaguardar nuestra intimidad. Jean-Jacques Rousseau, el filósofo de la Ilustración, el primer pensador que «descubrió» la intimidad, nos dio ejemplo de ello. ¿No fue acaso el primero en rebelarse contra la sociedad de su tiempo y contra la voluntad inquisitorial de controlar la conciencia de los individuos?

El fin de la vida privada sería una auténtica calamidad existencial, ha señalado también la filósofa Hannah Arendt en su libro *La condición humana*.[33] Con enorme clarividencia, apunta en ese ensayo los peligros que representa para la democracia una sociedad que no distinga suficientemente entre vida privada y vida pública, lo cual supondría, según Arendt, el fin del hombre libre. Y arrastraría inexorablemente a nuestras sociedades hacia nuevas formas de totalitarismo.

33 Hannah Arendt, *La condición humana*, Paidós, 2011.

I

TERROR Y ANTITERROR

«El terrorismo es ante todo un acto político que trata de provocar un efecto político. Si por su causa cambiamos nuestra sociedad, sale ganando».
Tom Clancy

En la era digital se está intensificando, en todo el mundo, un debate social sobre tres realidades que chocan entre sí: la amenaza de una vigilancia electrónica generalizada técnicamente posible a partir de ahora; la indispensable salvaguardia de la vida privada; y la necesidad de seguridad frente a nuevas formas de criminalidad y terrorismo.

El uso del terror con fines políticos viene de hace mucho tiempo. Aunque no tanto, pues no hay terrorismo, en el sentido moderno del término, sin medios de comunicación de masas que amplifiquen el efecto del miedo colectivo.[34] Ahora bien, los medios de masas no aparecen hasta la segunda mitad del siglo XIX. Por chocante que pueda parecer, un acto terrorista es casi siempre un (sangriento)

34 Ignacio Ramonet, *Guerres du XXI ème siècle. Peurs et menaces nouvelles*, Galilée, París, 2002; edición en español: *Guerras del siglo XXI. Nuevos miedos, nuevas amenazas,* Random House, Barcelona, 2003. Herfried Münkler, *Viejas y nuevas guerras: asimetría y privatización de la violencia,* Siglo XXI, Madrid, 2005.

mensaje dirigido a una colectividad por una organización, generalmente clandestina. El uso indiscriminado de la violencia mortífera contra civiles inocentes tiene normalmente como objetivo promover una causa de la que inevitablemente se harán eco los medios.

En el transcurso de la historia, un gran número de organizaciones políticas han recurrido al terrorismo para fomentar sus tesis. Partidos —tanto de derecha como de izquierda—, grupos nacionalistas, étnicos, religiosos o revolucionarios, incluso Estados, han practicado el terrorismo. Pero tras los atentados del 11 de septiembre de 2001,[35] reivindicados por la organización salafista-yihadista Al Qaeda, se puede decir que tanto el terrorismo como el antiterrorismo entraron en una nueva dimensión.

Los ataques del 11 de septiembre de 2001 abrieron una nueva etapa en la historia contemporánea. El ciclo geopolítico que acabó ese día había comenzado el 9 de noviembre de 1989 con la caída del muro de Berlín y más tarde, con la desaparición de la Unión Soviética el 25 de diciembre de 1991. Una etapa que además, conoció el auge de la mundialización neoliberal. Sus principales características, celebradas sin descanso por los grandes medios, fueron: la exaltación del régimen democrático, la celebración del Estado de derecho y la glorificación de los derechos humanos. En política interior y exterior, esta moderna trinidad fue considerada como una especie de imperativo categórico ético. Este tríptico, no desprovisto de ambigüedades —¿de verdad

35 El 11 de septiembre de 2011, comandos de la organización yihadista Al Qaeda, obedeciendo a su jefe Osama Bin Laden, desviaron varios aviones de línea y atacaron con ellos las dos torres del World Trade Center en Nueva York y el edificio del Pentágono en Washington, matando aproximadamente a 3.000 personas e hiriendo a más de 6.000. Es el atentado terrorista más mortífero de la historia.

se pueden conciliar mundialización neoliberal y democracia planetaria?—, contó con la adhesión de los ciudadanos, que con razón, veían en él un avance del derecho contra la barbarie.

A este respecto, la «respuesta democrática» a las atrocidades del 11 de septiembre de 2001 marcó un claro retroceso. En nombre de una «guerra justa» contra el terrorismo, pareció como si, de pronto, todas las transgresiones, incluso las más innobles, estuvieran permitidas. Para emprender una guerra de venganza contra Afganistán, Washington no dudó de entrada, en entablar alianzas con autócratas antes políticamente intratables: el general golpista Pervez Musharraf de Pakistán; el dictador de Uzbekistán Islam Karimov… En la democracia, valores morales que en la víspera aún eran considerados «fundamentales» abandonaban a hurtadillas la escena política.

La Ley Patriot Act

Simultáneamente, el Gobierno de George Bush[36] desató un huracán de medidas liberticidas, a veces secretas. Desde el día siguiente a los atentados, se aplicó una justicia de excepción. El 26 de octubre de 2001, el ministro de Justicia, John Ashcroft, hizo aprobar una ley antiterrorista llamada Patriot Act,[37] que permitió a las autoridades arrestar a los

36 Desde entonces, y con el pretexto del antiterrorismo, se adoptaron medidas similares en unos sesenta países —especialmente en China, Turquía y Pakistán—, que condujeron a la detención de aproximadamente 120.000 personas, a las que se acusó de terrorismo, lo cual permitió a los gobiernos de esos Estados desembarazarse de opositores políticos y de disidentes. (Fuente: Associated Press, septiembre de 2011).

37 Propuesta por el presidente George W. Bush, esta «ley para unir y reforzar a los Estados Unidos de América proporcionando los instrumentos

sospechosos por tiempo casi indefinido, deportarlos, encarcelarlos en celdas de aislamiento, espiar su correo, sus conversaciones telefónicas, sus e-mails y ordenar el registro de su domicilio sin autorización judicial.

De este modo, desde los primeros días que siguieron al 11 de septiembre fueron abusivamente arrestados no menos de 1.200 extranjeros, de los cuales más de la mitad permanecieron durante meses encarcelados y sin juicio. Muchos de ellos no fueron siquiera puestos a disposición judicial ni tuvieron la posibilidad de ser asistidos por un abogado.[38] Además, las autoridades declararon su intención de someter a interrogatorio a unos 5.000 hombres de entre 16 y 45 años que permanecían en los Estados Unidos con visado de turista, convertidos de pronto en sospechosos por el simple hecho de ser originarios de Oriente Próximo. [39]

A pesar de que los tribunales estadounidenses ordinarios eran totalmente competentes para juzgar a extranjeros sospechosos de terrorismo,[40] el presidente George W. Bush decidió el 13 de noviembre de 2001, crear tribunales mili-

---

adecuados para descubrir y contraatacar al terrorismo (…) elimina la distinción jurídica entre las investigaciones realizadas por los servicios de información exterior y las de las agencias federales responsables de las investigaciones criminales (FBI) cuando impliquen a terroristas extranjeros». Crea también los estatutos de «combatiente enemigo» y «combatiente ilegal», que permiten al Gobierno de los Estados Unidos detener, sin límite de tiempo y sin acusación, a cualquier persona sospechosa de «proyecto terrorista». En la práctica, la Patriot Act autoriza a los servicios de seguridad a que accedan a los datos informáticos conservados por particulares y empresas, sin autorización previa y sin informar a los usuarios» (Fuente: Wikipedia). La ley Patriot Act fue sustituida el 15 de junio de 2015 por la ley Freedom Act, que ha mantenido la mayoría de sus aspectos más importantes.

38 *El País*, Madrid, 10 de noviembre de 2001.

39 *Le Monde*, 30 de noviembre de 2001.

40 *International Herald Tribune*, 1ro. de diciembre de 2001.

tares específicos, con procedimientos especiales, y ubicarlos fuera del territorio estadounidense, para que las leyes de los Estados Unidos —y, desde luego, la Convención de Ginebra— no pudieran en modo alguno proteger a los acusados. Estos procesos secretos podían celebrarse, por ejemplo, a bordo de barcos de guerra o en bases militares situadas en el extranjero. De ahí la elección, entre otras, de la base de Guantánamo, que es un territorio de soberanía cubana arrendado abusivamente por tiempo indefinido por los Estados Unidos. Las sentencias se dictaban por una comisión formada por oficiales; no se requería unanimidad para condenar a muerte a un acusado; no se podía apelar contra el veredicto; las conversaciones del acusado con su abogado podían ser escuchadas clandestinamente; se mantenía en secreto el procedimiento judicial; y los detalles del proceso solo podían hacerse públicos una vez transcurridas varias décadas.

El Buró Federal de Investigaciones (FBI)[41] propuso que algunos acusados fueran extraditados a «países seguros» bajo un régimen dictatorial, para que las policías locales pudieran interrogarlos utilizando métodos «duros y eficaces». En las columnas de las revistas más importantes[42] se exigió abiertamente recurrir a la tortura. En la cadena CNN,[43] el comentarista republicano Tucker Carlson fue muy explícito: «La tortura no está bien, pero el terrorismo es peor. Por lo que, en determinadas circunstancias, la tortura es un mal menor». En las columnas del *Chicago Tribune*, el editorialista Steve Chapman propuso seguir el ejemplo de un Estado

41 En inglés: Federal Bureau of Investigation.

42 *Newsweek*, 5 de noviembre de 2001.

43 Cable News Network (CNN) es una cadena de televisión estadounidense fundada por el empresario Ted Turner en 1980.

democrático como Israel, que no dudaría en su opinión, en aplicar la tortura al 85 % de los detenidos palestinos.[44]

Al abolir una decisión de 1974, que prohibía a la Agencia Central de Inteligencia (CIA) asesinar a dirigentes extranjeros, George W. Bush volvió a darle carta blanca para llevar a cabo todas las operaciones secretas necesarias para eliminar físicamente a los jefes de Al Qaeda. Ignorando las Convenciones de Ginebra,[45] la guerra de Afganistán fue dirigida bajo el mismo principio: liquidar a los miembros de Al Qaeda incluso si se rendían. Donald Rumsfeld, en esa época secretario estadounidense de Defensa, se mostró inflexible al rechazar cualquier solución negociada y pidió que mataran a los prisioneros árabes que combatían con los talibanes.[46] Más de cuatrocientos de ellos fueron masacrados en Afganistán durante el levantamiento del fuerte "Qala-i-Jangi", en noviembre de 2001, y un número sin duda más elevado durante la toma de Tora Bora, en diciembre de 2001.

Para que no prosperara ninguna demanda contra militares estadounidenses que hubieran participado en este tipo de operaciones armadas en el extranjero, los Estados Unidos se enfrentaron al Tribunal Penal Internacional (TPI), cuya autoridad no reconocen. Y en agosto de 2002 el Senado aprobó una ley de protección de los miembros del servicio estadounidense (American Servicemembers' Protection Act, ASPA), que permite a Washington adoptar medidas extremas —pueden llegar a la invasión militar de un país—

---

44 *El País,* Madrid, 7 de noviembre de 2001.

45 Convenciones de Ginebra: conjunto de los cuatro convenios internacionales que regulan el derecho internacional humanitario. Su propósito es proteger a las víctimas de los conflictos armados.

46 *Le Monde,* 14 de diciembre de 2001.

para recuperar a cualquier ciudadano estadounidense detenido y amenazado con ser llevado ante el TPI.

Globalización del terrorismo

La mayoría de estas medidas «antiterroristas» se ha mostrado poco eficaz. El número de auténticos terroristas detenidos es irrisorio y lamentablemente, no se han impedido otros horribles atentados. Sin embargo, es enorme el precio en erosión de los derechos humanos que la colectividad debe pagar, lo cual ha llevado a Martin Scheinin, relator especial de la ONU, a afirmar que «la utilización actual de las leyes antiterroristas es mala no solo para los derechos humanos, sino también para luchar verdaderamente contra el terrorismo».[47]

Es conocido el caos en el que hundieron a Oriente Próximo las intervenciones estadounidenses en Afganistán y en Irak, apoyadas por la mayoría de sus aliados europeos. Quince años después, el desastre permanece y se ha extendido incluso a una gran parte de Siria, lo que ha provocado la huida de millones de refugiados. Mientras tanto, el terrorismo yihadista, lejos de haber sido erradicado, se ha generalizado y extendido a todo el planeta, tanto en lo relativo a los objetivos como a los atacantes. Prueba de ello es, por ejemplo, el llamamiento lanzado el 13 de septiembre de 2015 por Ayman al-Zawahiri, sucesor de Osama Bin Laden al frente de Al Qaeda, en el que se dirige a todos los musulmanes del mundo para conminarles a que ataquen a los países occidentales: «Llamo a todos los musulmanes que puedan perjudicar a los países de la coalición de cruzados a que no duden en hacerlo. A partir de ahora debemos trabajar para

47 Presstv.com, 4 de septiembre de 2011.

llevar la guerra al corazón de los hogares y de las ciudades del Occidente coaligado, en especial de los Estados Unidos de América».[48]

Con la violencia paroxística ejercida por la organización Estado Islámico (EI) o Daesh, que de alguna forma ha tomado el relevo de Al Qaeda, tanto a escala local —en Irak y en Siria— como internacional, el terrorismo yihadista globalizado se ha convertido según los especialistas, en un medio de «hostigar continuamente al enemigo, especialmente por medio de atentados, con objeto de debilitarlo moral y materialmente» antes de pasar a la segunda fase, la de la «administración de la brutalidad».[49] Deliberadamente, Daesh trata de internacionalizar su lucha por medio de atentados cometidos en todos los lugares en los que puedan actuar sus militantes, ataques que ya han tenido lugar en Túnez, Turquía, Kenia, Nigeria, Bélgica, Canadá, Australia, Dinamarca, Francia, los Estados Unidos (San Bernardino)…

En lo que se refiere a Francia, el autor del secuestro y asesinato de cuatro personas de confesión judía en el Hyper Cacher de la Porte de Vincennes, en París, el 9 de enero de 2015, manifestó pertenecer también a Daesh. Y el atacante del tren Thalys del 21 de agosto de 2015, acusado de haber intentado cometer una carnicería, es, asimismo, sospechoso de mantener vínculos con la organización Estado Islámico.

Por lo tanto, tenemos que vérnoslas, por primera vez, con la mundialización del terrorismo.

---

48 *Le Parisien,* 13 de septiembre de 2015.

49 Nabil Mouline, «Daesh: harcèlement, violence, propagande… Le plan de conquête en 3 étapes de l'EI», *L'Obs.*, 5 de julio de 2015.

Es una realidad innegable. Y los Estados tienen necesariamente que cumplir con su papel de proteger a los ciudadanos. Sin embargo, ¿es necesario convertir a cada ciudadano en sospechoso? ¿Y poner bajo vigilancia al conjunto de la sociedad? Ya en el siglo XVIII, el filósofo irlandés Edmund Burke respondió a estas preguntas: el problema es que, si no tenemos cuidado, la guerra acaba haciendo desaparecer incluso los valores por los que se inicia: la justicia, la moral, la humanidad. Con el terrorismo ocurre lo mismo, nos dice Edward Snowden:

> Para el mundo de la información, el terrorismo ha sido siempre una excusa para pasar a la acción. Provoca tal reacción emocional que, bajo la influencia del *shock*, la gente acepta leyes y programas que en otro caso no habrían votado jamás.[50]

El miedo a los «lobos solitarios»

Con motivo de los atentados perpetrados en Francia en enero de 2015, las autoridades francesas recordaron que la policía tenía fichadas por «islamismo radical» a unas 5.000 personas y que por razones presupuestarias, era imposible vigilarlas las veinticuatro horas del día. El procurador de la República de París, François Molins, manifestó que, de estos 5.000 sospechosos, los servicios de información vigilaban apenas a 1.700 en agosto de 2015. Añadió que este tipo de terrorismo no tiene ni estructura organizativa ni células ni cadena de mando: «Tenemos que ocuparnos —declaró— de comportamientos individuales, de "lobos

50 «Internet no es el enemigo, al igual que no lo es Irak», entrevista con Edward Snowden, *Publico.es*, 2 de septiembre de 2014 (http://blogs.publico.es/el-cuarto-poder-en-red/2014/09/02/ internet-no-es-el-enemigo-al-igual-que-no-lo-es-irak).

solitarios"». Ahora bien, si existe un perfil que los servicios de información temen especialmente es el de un sospechoso desconocido por la policía, sin antecedentes, sin vínculos con cualquier movimiento extremista, y sin figurar en ninguna base de datos.

Según François Molins, en julio de 2015 unos 1.800 franceses o residentes en Francia se habrían unido a las filas de los movimientos yihadistas en Irak y Siria. Y alrededor de 500 de ellos estarían participando en los combates. Se estima que el número de nuevos voluntarios que se enrolan cada día no deja de crecer, que incluso se habría duplicado en 2015. Más inquietante aún: entre 200 y 300 excombatientes de Daesh habrían vuelto a Francia, lo cual hizo temer a las autoridades un 11 de septiembre francés. «Tenemos que prepararnos para nuevos atentados y en consecuencia, protegernos», alertó el presidente François Hollande.[51]

Esa llamada de alerta no impidió los odiosos atentados en Saint-Denis y en París del 13 de noviembre de 2015, cuando tres comandos yihadistas, obedeciendo a consignas de Daesh, asesinaron a 150 personas e hirieron a más de 300 en el peor atentado de la historia de Francia.

En semejantes circunstancias, ¿cómo establecer la frontera entre seguridad y libertades civiles? ¿Hasta dónde están dispuestos los ciudadanos a sacrificar sus libertades para garantizar su seguridad? Muchos temen que se imponga una especie de sofisma liberticida, cuya fórmula podría ser esta: «La libertad es la seguridad, la seguridad es la vigilancia, luego la libertad es la vigilancia».[52]

---

51 *La Dépêche*, Toulouse, 28 de agosto de 2015.

52 Jean-Christophe Rufin, *Globalia*, Gallimard, París, 2005.

La ley Renseignement

Todas estas cuestiones se debatieron intensamente en Francia con motivo de la ley Renseignement, votada el 25 de junio de 2015.[53] Con el pretexto de luchar contra el terrorismo, esta ley permite claramente llevar a cabo prácticas de vigilancia masiva cuando, tras las revelaciones de Edward Snowden, empiezan a ser condenadas por los tribunales europeos. Así, por ejemplo, el Tribunal de Justicia de la Unión Europea (TJUE), al que apeló la asociación irlandesa Digital Rights Ireland, invalidó en abril de 2014 la directiva de 2006 sobre la conservación de datos.[54] El fallo condena el principio de una recogida indiferenciada de datos relativos a personas para las que, según el Tribunal, no hay «ningún indicio que permita pensar que su comportamiento pudiera tener algún vínculo, incluso indirecto o lejano, con infracciones graves».[55]

Insensible a esta histórica decisión del TJUE, la ley francesa Renseignement permite, sobre todo a los investigadores, que sin la previa autorización de un juez escuchen y graben a cualquiera de nosotros con la mera decisión del primer ministro.[56] Objetivo principal: la detección automática

---

53 La ley relativa a la información fue promulgada el 25 de julio de 2015 y publicada en el *Journal officiel* del 26 de julio de 2015.

54 Esta directiva de la Comisión Europea fue adoptada tras los atentados de Madrid y de Londres. Imponía a los operadores la obligación de salvaguardar el conjunto de los datos de conexión de sus abonados durante un periodo de entre seis meses y dos años, y de mantenerlo a disposición de las autoridades judiciales.

55 Félix Tréguer, «Résistence multiforme», *Le Monde Diplomatique,* junio de 2015.

56 Marc Rees, «Loi Renseignement: ce que dit le mémoire de la Quadrature, FDN et FFDN», *NextINpact*, 24 de junio de 2015 (http://www.nextinpact.com/news/95538-loi-renseignement-ce-que-dit-memoire-quadrature-fdn-et-ffdn.htm).

de comportamientos determinados. La ley permite que se utilice un *software* llamado «espía» para seguir de cerca la actividad informática de un sospechoso. A partir de ahora, toda navegación en la Red puede ser grabada en tiempo real por medio de «cajas negras algorítmicas»[57] instaladas en los operadores de telecomunicación, en los proveedores de acceso a Internet, en los alojamientos web y en los diferentes servicios en línea.

Se echa un ojo a todas las consultas e intercambios en Google, Facebook, WahtsApp, Skype, etc. También se autoriza a los agentes para que instalen dispositivos GPS en los coches, para que vigilen las conversaciones y los datos informáticos de todo sospechoso, incluso de su entorno y para que se coloquen clandestinamente micrófonos y cámaras en su casa. En adelante, los operadores privados, los sitios web o los proveedores de acceso a Internet deberán «detectar, mediante tratamiento automático, cualquier sucesión sospechosa de datos de conexión», como precisa el texto. Finalmente, se legalizan las «IMSI catchers»,[58] pequeños maletines que permiten interceptar a distancia las comunicaciones telefónicas de los móviles.

En consecuencia, los agentes del servicio francés de información pueden a partir de ahora, saberlo todo, espiar-

57 Con ayuda de un algoritmo secreto, estas «cajas negras» capturan considerables cantidades de datos relativos a las actividades de los internautas en la Red. Solo se graban los metadatos: informaciones que permiten saber qué sitio web se ha visitado, dónde, a qué hora, qué día, durante cuánto tiempo y qué cantidad de datos se ha intercambiado. Los metadatos son informaciones interesantes que pueden mostrar algo de nosotros a los servicios de información. La grabación de metadatos no es, por lo tanto, menos intrusiva que la recopilación de datos.

58 La International Mobile Subscriber Identity (IMSI) es un número, único en cada teléfono, que permite a una red móvil identificar a un usuario. Se guarda en la tarjeta SIM, y no es conocido por este. Equipadas con antenas repetidoras, las «IMSI *catchers*» («cazadores de IMSI») permiten espiar los teléfonos móviles.

lo todo: quién dirige correos a quién, con qué regularidad. La ley precisa que cualquier persona que incite a «violencias colectivas» o represente un peligro para «los intereses fundamentales de la política exterior de Francia», o amenace sus «intereses económicos o científicos», podrá ser sometida a vigilancia. Pero la autoridad judicial no tiene voz en este capítulo: en lo sucesivo, el control de las escuchas lo llevará la Comisión Nacional de Control de las Técnicas de Información.[59]

El Consejo Constitucional francés censuró, en un primer momento, las medidas de la ley que se refieren a la vigilancia internacional.[60] Muchos medios de comunicación[61] y varias organizaciones —especialmente la Quadrature du Net, la Liga de los Derechos del Hombre y el Sindicato de la Magistratura— han señalado los abusos de esta ley Renseignement: «…cajas negras, exclusión del juez, no protección del secreto profesional de los abogados y de otras

59 En francés: Commission nationale de contrôle des techniques de renseignement (CNCTR). Sustituye a la CNCIS (Comisión Nacional de Control de las Interceptaciones de Seguridad). Está compuesta por nueve miembros: dos diputados y dos senadores; dos miembros o antiguos miembros del Consejo de Estado; dos magistrados o antiguos magistrados al margen de la jerarquía del Tribunal de Casación, nombrados a propuesta conjunta del primer presidente y del procurador general del Tribunal de Casación; y una personalidad cualificada por sus conocimientos en materia de comunicaciones electrónicas, nombrada a propuesta del presidente de la Arcep (Autoridad Reguladora de las Comunicaciones Electrónicas y de Correos). La CNCTR entró en funcionamiento el 3 de octubre de 2015, presidida por Francis Delon, consejero de Estado.

60 Pero el Gobierno de Manuel Valls volvió al ataque con una propuesta de ley adoptada por la Asamblea Nacional en octubre de 2015, y finalmente confirmada por el Consejo Constitucional en noviembre de 2015.

61 Por ejemplo, los diarios en línea *Basta!* (http://www.bastamag.net/Surveillance-generalisee-du-net-traitement-automatise-des-donnees-manque-de), 4 de mayo de 2015, y *Undernews*, (http://www.undernews.fr/anonymat-cryptographie/loi-renseignement-comment-sen-roteger.html), 8 de mayo de 2015.

profesiones protegidas, así como del secreto de las fuentes de los periodistas, ausencia de transparencia en los abusos que han sido ya constatados…».[62] Por su parte, el Consejo Nacional de lo Digital (CNN)[63] se mostró preocupado, según su comunicado del 19 de marzo de 2015, por «una ampliación del ámbito de vigilancia», e invitó a «reforzar las garantías y los medios de control democráticos». Este organismo lamenta «la ampliación significativa de los límites de vigilancia, sin que esta ampliación se haya acompañado de suficientes garantías en términos de libertades». Y considera además, que algunas nuevas técnicas de información constituyen «una forma de vigilancia masiva».

Por su parte, el defensor de los derechos —equivalente al defensor del pueblo— Jacques Toubon ha expresado sus reservas basándose en la Convención Europea de Derechos Humanos.[64] Y el Comité de Derechos Humanos de las Naciones Unidas publicó un informe en el que condenó severamente esta «peligrosa ley». En los Estados Unidos, un editorial de *The New York Times*[65] llamó a los diputados franceses a no votar esta ley, de la que el juez antiterrorista Marc Trévidic[66] piensa que «abre el camino a la generalización de métodos intrusivos, fuera del control de los jueces, que, sin embargo, son los garantes de las libertades individuales» en Francia.

---

62 http://www.laquadrature.net/fr/honte-sur-la-france-le-conseil-constitutionnel-valide-largement-la-loi-renseignement.

63 Conseil National du Numérique.

64 *Challenges*, 24 de abril de 2015 (http://www.challenges.fr/politique/20150423.CHA5216/loi-sur-le-renseignement-lesreserves-de-jacques-toubon-html).

65 *The New York Times*, 31 de marzo de 2015.

66 Este magistrado ha instruido casos delicados, como el del atentado de Karachi, Pakistán, y el del asesinato de los monjes cristianos de Tibhirine, Argelia.

Además, el 3 de octubre de 2015, el Tribunal Europeo de Derechos Humanos (CEDH, por sus siglas en francés) estudió el recurso contra la ley Renseignement presentado por periodistas de la Asociación de la Prensa Judicial (APJ). Ciento ochenta periodistas, que representan a la mayoría de los medios escritos, audiovisuales y digitales, se alarman ante «las nuevas amenazas contra la libertad de informar». Reprochan a la ley que vapulee el secreto de las fuentes, viole la vida privada y restrinja la libertad de información. Finalmente, protestan contra la vigilancia masiva sobre simples ciudadanos que la ley permite.[67]

A su vez, el Consejo de la Orden de Abogados de París decidió impugnar la ley Renseignement ante el Tribunal Europeo de Derechos Humanos, el 7 de octubre de 2015. El decano Pierre-Olivier Sûr declaró que esta ley «es un texto que ante nuestros ojos representa una doble mentira de Estado. Primero, haciéndonos creer que se trata de proteger la nación contra el terrorismo, cuando su alcance es muchísimo más amplio. Y segundo, pretendiendo que se garantiza el control judicial designando a un juez administrativo, cuando, en un régimen de libertades, el único juez es el juez jurisdiccional. No designa al tribunal administrativo ni al tribunal de apelación, sino al Consejo de Estado, al que ni siquiera los profesionales del derecho pueden apelar».[68]

Añadió el decano Sûr: «Este texto no garantiza el secreto profesional de los abogados, por lo que debería ser pura y simplemente censurado. Hay una gran jurisprudencia sobre libertades públicas en la CEDH, que hoy día es creadora

67 *Le Monde*, 4 de octubre de 2015.

68 M. Rees, «Le bâtonnier de Paris attaque la loi Renseignement devant la Cour européenne», *NextInpact*, 8 de octubre de 2015 (http://www.nextinpact.com/news/96810/le-batonnier-paris-attaque-loi-sur-renseignement-devant-cour-europeenne-htm).

de un derecho ejemplar, hasta tal punto que pone de manifiesto que nuestro derecho francés lleva un tiempo de retraso». Recordemos que la Convención Europea de Derechos Humanos protege especialmente el derecho a la privacidad. Según su artículo 8, «toda persona tiene derecho a que se respete su vida privada y familiar, su domicilio y su correspondencia».

El misterioso Big Brother[69] *francés*

Y hay algo más grave. El periódico *Le Monde* reveló que desde 2013, existe en Francia un misterioso servicio, clasificado como «secreto de defensa» y disimulado en el seno de los servicios de información, dedicado a recoger y almacenar de forma masiva datos personales. Su nombre: Plataforma Nacional de Análisis y Desciframiento de Códigos.[70] Durante mucho tiempo la República negó su existencia,[71] hasta tal punto que este dispositivo intrusivo —con el que los servicios franceses de información podrían obtener datos a su antojo, sin más control que el de su propia jerarquía— fue totalmente silenciado en la ley Renseignement de junio de 2015.

Este Big Brother francés, que se aloja en el sótano de la sede de la Dirección General de Seguridad Exterior (DGSE),[72] en el número 141 del bulevar Mortier de París,

69 Big Brother: personaje del libro *1984*, de George Orwell.

70 Plateforme nationale de criptanalyse et de décryptement (PNCD).

71 Los sucesivos gobiernos y los parlamentarios han negado su existencia en nombre de la razón de Estado. El ministro de Defensa, Jean-Yves Le Drian, acabó admitiendo, el 15 de abril de 2015, que la PNCD se creó realmente en 1999.

72 La DGSE forma parte de la comunidad francesa de Inteligencia con la Dirección de Información Militar (DRM), la Dirección de Protección

dispondría de las supercalculadoras más potentes, y emplearía a unos 150 especialistas, sobre todo matemáticos e informáticos de muy alto nivel.

En este inmenso espacio —afirma Vincent Jauvert—, el segundo centro de descodificación informática en Europa, por detrás de su equivalente británico, ordenadores gigantes filtran cada día decenas de millones de correos electrónicos, de sms, de intercambios por Skype, WhatsApp, Facebook… Aíslan automáticamente, mediante los números de teléfono o las direcciones IP, los intercambios que llevan a cabo las personas elegidas. Un programa reconoce la voz, otro traduce. De esta manera, se criba todo el tráfico de datos, país por país. Hay programas que cachean mediante palabras clave, todas las conversaciones por correo electrónico, Facebook o Skype; otros analizan millones de metadatos.[73]

Estos metadatos son conservados y almacenados durante años, igual que hace la NSA estadounidense, para poder realizar investigaciones retrospectivas. El objetivo es disponer de un registro completo de las comunicaciones en todo el mundo durante los últimos cinco años, con el fin de que, en el caso de que una persona llame un día la atención, se pueda buscar entre esa masa de datos almacenados, y encontrar la lista de los interlocutores del sospechoso para poder reconstruir su red de relaciones.

Por medio de satélites o de ondas hertzianas, pero sobre todo a través de cables submarinos de fibra óptica, transita

---

y Seguridad de la Defensa (DPSF), la Dirección General de Seguridad Interior (DGSI), la Dirección Nacional de Información e Investigación de Aduanas (DNRED), el Servicio de Tratamiento de la información y acción contra los circuitos financieros clandestinos (Tracfin) y la Plataforma Nacional de Análisis y Desciframiento de Códigos (PNCD).

73 Vincent Jauvert, «Comment la France (aussi) écoute le monde», *L'Obs.*, 2 de julio de 2015.

ya lo esencial de las comunicaciones mundiales. Miles de millones de datos, que afectan a ciudadanos tanto franceses como extranjeros, son de esta forma interceptados, descifrados, acumulados y clasificados.[74] Ninguna autoridad judicial vela por salvaguardar la legalidad de estas escuchas. Y otra traición capital: en el marco de los intercambios de Francia con los Estados Unidos y el Reino Unido, la DGSE estaría entregando regularmente a sus homólogos del Cuartel General de Comunicaciones del Gobierno del Reino Unido (GCHQ)[75] y de la NSA bloques de datos muchas veces sin descodificar.

74 Este inmenso banco de datos está a disposición de los demás servicios de información franceses. (Fuente: *Le Monde*, 12 de abril de 2015).

75 Government Communications Headquarters, uno de los tres servicios de inteligencia del Reino Unido, ubicado en Cheltenham, Inglaterra.

II

LOS «CINCO OJOS» Y LA RED ECHELON

«Siempre, permanentemente, te vigilan estos ojos inquisidores,
en tu casa o en la calle, en el trabajo o en el bar, de noche y de día:
no hay ninguna intimidad posible».
George Orwell, *1984*.

Hace quince años y en nombre de la «necesaria protección» a la población, el arsenal de medidas de control y vigilancia, que desde la Segunda Guerra Mundial no había dejado de reforzarse, explotó literalmente.

Todo comienza en la primavera de 1941, en pleno conflicto mundial. Para penetrar en el secreto de la célebre máquina alemana de codificación Enigma,[76] considerada inviolable, los Estados Unidos y el Reino Unido deciden sellar una alianza Sigint[77] y cooperar en materia de información. Intercambian sus protocolos de recogida de información, comparten sus códigos y unifican su terminología.

76 Enigma es una máquina electromecánica portátil que sirve para cifrar y descifrar la información. Considerada inviolable, fue utilizada principalmente por los militares alemanes durante la Segunda Guerra Mundial.

77 La información de origen electromagnético, en inglés *Signals Intelligence*, o Sigint, es una información cuyas fuentes son las comunicaciones que utilizan ondas (radio, satélite), un radar o herramientas de telemedición. Además de las escuchas telefónicas, el Sigint incluye la vigilancia de los correos electrónicos y de las redes sociales, lo cual plantea evidentes problemas de respeto a la vida privada. (Fuente: Wikipedia).

Los analistas estadounidenses, que acababan de descifrar el código japonés Purple, transmiten a Londres sus técnicas y conocimientos.[78] Estadounidenses y británicos se ponen también de acuerdo sobre la forma de gestionar las informaciones recogidas y las telecomunicaciones interceptadas por todos los medios posibles (radio, radar, cable, etc.).

Gracias a esta colaboración, los servicios militares de información estadounidenses y sobre todo, el equipo de criptógrafos británicos agrupados alrededor de Alan Turing en Bletchley Park, Buckinghamshire, consiguen por fin, en 1942, romper el código Enigma.[79] Los dos países firman entonces, en marzo de 1943, el acuerdo Brusa, que pone las primeras bases de un sistema mundial de vigilancia masiva y de interceptación de las telecomunicaciones, en estrecha relación con las principales industrias de la comunicación.

Los acuerdos Ukusa

Acaba la guerra y con objeto de seguir espiando las comunicaciones en todo el mundo, son los británicos quienes defienden mantener con Washington la alianza a la que desean incorporar a Canadá, Australia y Nueva Zelanda. A partir de septiembre de 1945, el presidente de los

78 Simon Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography,* Fourth State, 1999; edición en español: *Los códigos secretos; el arte y la ciencia de la criptografía, desde el antiguo Egipto a la era Internet*, Debate, Madrid, 2000.

79 Alan Turing, matemático, físico y genial criptógrafo británico, fue quien principalmente ideó el método para quebrar el código Enigma, y el que plantó las bases de la informática y de los ordenadores modernos. Véase la película *Enigma* (1982), de Michael Apted, y sobre todo *The Imitation Game* (2014), de Morten Tyldum (en España se estrenó con el título *Descifrando Enigma* y en América Latina con el de *El código Enigma*).

Estados Unidos, Harry Truman, acepta entablar negociaciones secretas para crear, en tiempos de paz, una alianza SIGINT entre todos estos países. En marzo de 1946, en vísperas de la Guerra Fría, y con el fin de espiar a la Unión Soviética y a sus aliados, se firmó el importante y ultrasecreto acuerdo Ukusa[80] entre los servicios de información de cinco países anglosajones: la NSA; el GCHQ; el Defense Signal Directorate (DSD), con base en Kingston, Australia; el Communication Security Establishment (CSE), instalado en Ottawa, Canadá; y el Government Communications Security Bureau (GCBS), con sede en Wellington, Nueva Zelanda. Esta alianza, también conocida como la de los *Five Eyes* (cinco ojos), es históricamente la primera colaboración internacional oficial —aunque secreta— en materia de vigilancia de las comunicaciones mundiales. Durante toda la Guerra Fría (1948-1989), las interceptaciones internacionales alcanzarán unos niveles y una calidad desconocidos hasta entonces.

En el plano interior, durante el periodo macartista de la «caza de brujas», el FBI de John Edgar Hoover[81] no dudó en violar la correspondencia, en escuchar de manera ilícita las conversaciones telefónicas y en colocar micrófonos en los domicilios de las personas sospechosas de ser comunistas, homosexuales o de simplemente no adherirse a la política del gobierno estadounidense, entre las cuales se encontraban grandes escritores y artistas como Ernest Hemingway,

80 United Kingdom-United States of America Communications Intelligence Agreement (Ukusa). Se pueden consultar todos los documentos originales relativos a esta alianza en la web de la NSA (https://www.nsa.gov/public/_info/declass/ukusa.shtml).

81 Ver *J. Edgar*, película de Clint Eastwood, 2011.

John Steinbeck, Norman Mailer, Pete Seeger o Gabriel García Márquez.[82] Todo ello sin autorización judicial.

«Como un ladrón silencioso…»

A comienzos de la década de los cincuenta, y en el marco de los acuerdos Ukusa, los cinco países signatarios[83] deciden, con total sigilo, poner en marcha la red Echelon, un sistema mundial de interceptación de comunicaciones privadas y públicas que ha permanecido desconocido para la opinión pública durante más de cuarenta años.[84]

Echelon es el resultado de una decisión política. Se trata de una red mundial formada por decenas de satélites espías y de potentes bases de escucha diseminadas por todo el mundo.[85] Todavía hoy puede «escuchar» los cables submarinos de fibra óptica y puede interceptar las conversaciones telefónicas, los fax, los sms, los e-mails… Con ayuda de ordenadores supereficientes, sus innumerables agentes están en condiciones de seleccionar y ordenar todas estas comunicaciones mediante algunas palabras clave que se utilizan en los intercambios escritos y a través del tono de voz, incluso en los diálogos orales.

Esta formidable máquina de control, creada en secreto después de la Segunda Guerra Mundial por cinco potencias

82 *El País*, Madrid, 5 de septiembre de 2015.

83 A los que más tarde se añadirían los países llamados «terceros»: Alemania, Suiza, Japón, Filipinas, Taiwán, Dinamarca, Turquía y Noruega.

84 La opinión pública no tendrá conocimiento de ello hasta el 24 de febrero de 1999, cuando *The New York Times* publica un artículo que describe con detalle el funcionamiento del sistema Echelon.

85 Philippe Rivière, «Le système Echelon», *Le Monde Diplomatique*, julio de 1999.

anglosajonas —los *Five Eyes*—, extiende su red sobre todo el planeta conectándose a los satélites y cables que canalizan la mayor parte de las comunicaciones del mundo.[86] Echelon puede registrar hasta dos millones de conversaciones por minuto… Su principal misión consiste en espiar a los gobiernos amigos o enemigos, a los partidos políticos, los sindicatos, los movimientos sociales y las empresas. Una quincena de grandes bases repartidas por todo el mundo interceptan las comunicaciones que los superpotentes ordenadores de la NSA «tamizan» a continuación detectando palabras concretas en varias lenguas.[87]

En el marco de Echelon, los servicios de información estadounidenses y británicos han podido establecer una dilatada y secreta colaboración, lo cual ha dado lugar al más potente sistema de vigilancia del mundo, que se utiliza tanto para misiones militares como políticas y económicas. Las informaciones recogidas por Echelon son dirigidas y diseccionadas en el cuartel general de la NSA, no lejos de Washington. Allí, «tras impresionantes vallas metálicas electrificadas (…), una nube de cerebros llevan a cabo actividades tan variadas como las de oficial superior en lenguaje SIGINT, analista del lenguajes, experto lingüista-criptoanalista, experto en investigación lingüística, experto en criptoanálisis, ingeniero de criptoanálisis, criptoanalista cualificado de máquina, criptoanalista cualificado manual, experto en análisis de signos, programador, desarrollador, controlador de operaciones de recopilación, experto en conversaciones de signos, especialista en gestión de frecuencias de radio,

86 Sobre la red Echelon, véase Sébastien-Yves Laurent, *Atlas du renseignement. Géopolitique du pouvoir,* Les Presses de Sciences Po, París, 2014, pp. 124-129.

87 Christophe Ventura «La bataille du cyberespace», Mémoire des luttes, 14 de junio de 2013 (hhtp://www.medelu.org/ la-bataille-du-cyberespace).

matemático criptoanalista, analista de investigación, preparador en criptología, examinador del polígrafo, detector de mentiras de la CIA».[88] Todos ellos criban, desde hace sesenta años, casi todas las comunicaciones del mundo. Escribe el novelista angloaustraliano Terry Hayes:

> Echelon no descansa nunca, no duerme jamás. Patrulla por el gran vacío del espacio sin tener necesidad de aire, de alimento, de confort; trabaja como un ladrón silencioso en los centros mundiales de fibra óptica, y pilota innumerables radomos[89] en bases militares repartidas por todo el mundo. En resumen, Echelon, que escucha cada comunicación electrónica en la Tierra, es una vasta red electrónica de satélites tan secreta que ni siquiera los cinco países de lengua inglesa[90] que la crearon durante la Guerra Fría han reconocido su existencia.

Los miles de millones de octetos de datos que Echelon registra cada nanosegundo son cargados a distancia en una serie de superordenadores —entre los más rápidos del mundo, como los Roadrunner de IBM, enfriados por agua— situados en el cuartel general de la NSA. Allí, programas ultrasecretos utilizan palabras clave, frases tipo, incluso —según informes también secretos— reconocimiento de voz para extraer cualquier fragmento que merezca una investigación más exhaustiva.[91]

---

88 Rémi Kauffer, *Histoire mondiale des services secrets*, Perrin, París, 2015.

89 Un radomo (de *radar* y *domo*) es una carpa en forma de enorme pelota de golf blanca que, en el ámbito de escucha o interceptación de las comunicaciones, se utiliza para proteger de la vista una antena gigante, con objeto de no divulgar su orientación. (Fuente: Wikipedia).

90 Bernard Cassen, «Cinq yeux, une seule langue», *Mémoire des luttes,* 1ro. de agosto de 2013 (http://medelu.org/ cinq-yeux-une-seule-langue).

91 Terry Hayes, *I am Pilgrim,* Simon & Schuster, 2015; edición en español: *Yo soy Pilgrim,* Salamandra, 2015.

Al final de la Guerra Fría se creyó que la voluntad política de espiar masivamente las comunicaciones se esfumaría. Pero el auge de Internet en esa época y las excepcionales facilidades que ofrecía la Red, lograron que venciera la decisión de proseguir y amplificar la vigilancia.

Desde 1994, una ley secreta —la Communications Assistance for Law Enforcement Act (Calea)—[92] autoriza al gobierno de los Estados Unidos a escuchar las comunicaciones telefónicas privadas. Pero para adaptarla a los progresos tecnológicos y en especial a la evolución de Internet, el Congreso la modificó varias veces en sentido cada vez más intrusivo, especialmente en 2004 y 2006. De manera regular, a medida que cambiaba el uso de las comunicaciones, las agencias federales estadounidenses presionaron a las empresas de Internet y al Congreso para lograr nuevas adaptaciones de la ley en materia de vigilancia y espionaje.

Por ejemplo, en noviembre de 2010, el director del FBI, Robert S. Mueller, acudió a Silicon Valley para reunirse con los directivos de Google y de Facebook, y convencerles de que autorizaran la instalación de sistemas que permitieran al FBI interceptar y descifrar los mensajes de todos los clientes de estas dos empresas globales. El FBI quería convencerlos también para que impusieran a sus filiales en el extranjero la obligación de desviar todas sus comunicaciones hacia los servidores instalados en los Estados Unidos,

92 https://askcalea.fbi.gov. A propósito de Calea, véase también el dossier realizado por el equipo de la asociación Electronic Frontier Foundation (https://www.eff.org.fr/ fr/issues/calea).

donde serían analizadas antes de reencaminarlas a su destino final.[93]

La voluntad de control se extiende también a los europeos que viajan en avión a los Estados Unidos. En virtud de un acuerdo entre la Unión Europea y las autoridades federales estadounidenses, algunas informaciones personales son entregadas por la compañía aérea a las aduanas de los Estados Unidos sin el consentimiento del viajero.[94] Antes incluso de que el viajero entre en el avión, las autoridades conocen su nombre, apellidos, edad, domicilio, número de pasaporte y de tarjeta de crédito, su estado de salud, sus preferencias alimentarias —que pueden reflejar su religión—, sus viajes anteriores, etcétera.

Estas informaciones se pasan por un filtro llamado CAPPS[95] para detectar eventuales sospechosos. Cruzando la identidad de cada viajero con las informaciones de los servicios policiales, del Departamento de Estado, del Ministerio

93 *The New York Times,* 16 de noviembre de 2010.

94 Los pasajeros procedentes del extranjero que llegan a un país de la Unión Europea también son incluidos en el fichero europeo de datos de pasajeros aéreos (llamado PNR, Passenger Name Record). Después de los atentados de París del 13 de noviembre de 2015, y tras muchas dudas, la Comisión de Libertades Civiles (Libe) adoptó, el 10 de diciembre de 2015, una propuesta de la Comisión Europea, adoptada por los Estados miembros de la Unión Europea, y sobre la cual el Parlamento Europeo debía pronunciarse a principios de 2016. La propuesta autoriza la creación de este fichero, y obliga a las compañías que prestan servicios en el Viejo Continente a transmitir información sobre los viajeros (nombre, número de cuenta bancaria, lugar de tránsito, etc.) a los servicios de policía e información de los países miembros. Los datos se conservan durante cinco años para delitos de terrorismo, y cuatro años para delitos graves de criminalidad transnacional (tráfico de drogas, de armas, de personas, blanqueo, cibercriminalidad, etc.).

95 Computer Assisted Passenger Pre-Screeing, o Sistema de control preventivo asistido por ordenador.

de Justicia y de los ficheros de los bancos, CAPPS evalúa el grado de peligrosidad del pasajero y le asigna un código de color: verde para los inofensivos, amarillo para los casos dudosos y rojo para aquellos a los que se impedirá subir al avión. El programa de seguridad de fronteras autoriza a los agentes de aduanas para que fotografíen a todos los viajeros que entran a los Estados Unidos y tomen sus huellas digitales. Si el visitante es musulmán u originario de Oriente Próximo, se le atribuye de oficio el código amarillo como sospechoso.

Los latinoamericanos también están en el punto de mira. Se ha sabido que 65 millones de mexicanos, 31 millones de colombianos y 18 millones de centroamericanos estaban fichados en los Estados Unidos sin que ellos lo supieran. En cada ficha figuran la fecha y el lugar de nacimiento, el sexo, la identidad de los padres, una descripción física, el estado civil, el número de pasaporte y la profesión que declararon. A menudo estos ficheros recogen otras informaciones confidenciales, como las direcciones personales, los números de teléfono, de la cuenta bancaria y de la matrícula del vehículo. También consignan las huellas digitales. Todos los latinoamericanos están avocados a que Washington los etiquete poco a poco.

¿Un mundo más seguro?

«El objetivo es instaurar un mundo más seguro. Es necesario estar informados sobre el riesgo que representan las personas que entran en nuestro país», afirmó James Lee, uno de los responsables de ChoicePoint, la empresa que compró estos ficheros para revenderlos a las autoridades

estadounidenses.[96] En efecto, la ley prohíbe a la Administración de los Estados Unidos almacenar informaciones personales, pero no prohíbe que le pida a una empresa privada que lo haga por ella.

Instalada cerca de Atlanta, ChoicePoint[97] no es una empresa desconocida. En el año 2000, durante el escrutinio presidencial en Florida, su filial Database Technologies (DBT) fue contratada por el gobernador del estado para reorganizar sus listas electorales. Resultado: millares de personas —especialmente afroamericanos y pobres, que suelen votar por los demócratas— fueron privadas de su derecho al voto, lo cual modificó el resultado del escrutinio, que ganó el conservador George W. Bush por solo 537 votos de ventaja sobre el demócrata Al Gore. Hay que recordar que esta victoria permitió a G. W. Bush acceder a la presidencia por primera vez.[98]

Los extranjeros no son el único objeto de la creciente vigilancia en los Estados Unidos. Los ciudadanos estadounidenses tampoco escapan a esta paranoia. Como se ha visto, los nuevos controles que autoriza la Patriot Act han cuestionado la vida privada y el secreto de la correspondencia. Los investigadores pueden acceder a las informaciones personales de los ciudadanos sin mandato de registro. El FBI puede pedir a las bibliotecas que le proporcionen la lista de los libros y de las páginas web consultados por sus abonados para trazar a partir de estos datos, un «perfil intelectual» de cada lector.[99]

---

96 *La Jornada.* México, 22 de abril de 2003.

97 En 2008, *ChoicePoint* fue adquirida por la compañía *LexisNexis Group*, filial a su vez del gran grupo internacional de edición *Reed Elsevier* (que, entre otras cosas, organiza el *Salon du Livre* de París).

98 *The Guardian*, Londres, 5 de mayo de 2003.

99 *The Washington Post National Weekly Edition*, 21 a 27 de abril de 2003.

Total Information Awareness

El más delirante de todos los proyectos de espionaje masivo ilegal es el que elaboró el Pentágono con el nombre de Total Information Awareness (TIA), sistema de vigilancia total de las informaciones[100] encargado al general John Pointdexter, quien fuera condenado en los años ochenta por haber sido el instigador del caso Iran-Contra o Irangate.[101] El proyecto consiste en recopilar una media de cuarenta páginas de información sobre cada uno de los siete mil millones de habitantes del planeta y en confiar su tratamiento a una batería de hiperordenadores.

Con el procesamiento de todos los datos personales disponibles —pagos con tarjeta de crédito, suscripciones a medios de comunicación, movimientos bancarios, llamadas telefónicas, consultas en Internet, correos electrónicos, redes sociales, informes médicos, ficheros policiales, informes de aseguradoras, listados de compañías aéreas, informaciones de la seguridad social, etc.—, el Pentágono piensa fijar la trazabilidad completa de cada persona viva sobre la Tierra. Oficialmente, se ha abandonado este proyecto tota-

---

100 Ante las protestas de los defensores de la vida privada, se ha cambiado el nombre por el de Terrorism Information Awareness (TIA). Véase Armand Mattelart, *Histoire de la société de l'information,* La Découverte, París, 2003; edición en español: *Historia de la sociedad de la información,* Paidós, 2002.

101 En los años ochenta, algunos miembros de la Administración Reagan vendieron ilegalmente armas a Irán, país considerado «enemigo» por los Estados Unidos. Utilizaron los beneficios de estas ventas para financiar en secreto —a pesar de la prohibición explícita del Congreso— un movimiento contrarrevolucionario en Nicaragua, los «contras», que mantenía una lucha armada contra el legítimo gobierno sandinista de Daniel Ortega. En el marco de la Guerra Fría, la Administración Reagan intentaba de este modo derribar un gobierno considerado comunista, situado en una zona que Washington cree su coto privado.

litario, pero en realidad todos sus objetivos se mantienen clandestinamente y una de las misiones actuales de la NSA es llevarlos a término.[102]

Igual que en la película *Minority Report*,[103] las autoridades creen que de este modo podrán prevenir los delitos antes de que se cometan: «Habrá menos vida privada, pero más seguridad», afirma John L. Petersen, presidente del Arlington Institute.[104] «Gracias a la interconexión de todas las informaciones que os atañen podremos anticipar el futuro. Mañana sabremos todo de vosotros».[105]

102 Ignacio Ramonet, entrevista con Julian Assange.

103 Steven Spielberg, *Minority Report,* 2002, basada en una novela de Philip K. Dick.

104 Situado cerca de Washington DC, The Arlington Institute (http://www.arlingtoninstitute.org) es un centro de investigaciones prospectivas especializado en el estudio de los «cambios globales en el futuro».

105 *El País,* Madrid, 4 de julio de 2002.

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 ciento por ciento de seguridad, el ciento por ciento de respeto a la vida privada y cero inconvenientes. Es necesario

que, como sociedad, elijamos».[106] 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—[107] subcontratista de la NSA, reveló a Glenn Greenwald,[108] periodista del diario británico *The Guardian*, y a Laura Poitras,[109] 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.[110]

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 la principal revelación de Snowden fue otro programa secreto, desarrollado por la NSA a partir de 2007 y

106 *L'Obs.*, 8 de junio de 2013.

107 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».

108 Glenn Greenwald, *Sin un lugar donde esconderse*, *ob. cit.*

109 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.

110 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.

cuyo nombre de 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: Aol, Apple, Facebook,[111] Google, Microsoft, Paltalk, Yahoo, Skype y YouTube. Hay que destacar la ausencia de Twitter.[112]

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 exhaustivas.[113] Según el *Washington*

111 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.

112 «L'absence de Twitter du programme PRISM, défense des libertés ou manque d'intérêt?», *Le Monde,* 11 de junio de 2013.

113 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

Post, los mil ojos de la NSA pueden «ver literalmente lo que usted teclea» en su ordenador.[114]

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».[115] Para protegerse contra esta intromisión, solo hay que hacer una cosa: quitar la batería del teléfono —cuando se puede; en los iPhones, por ejemplo, ya es imposible— 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 electróni-

---

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, 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).

114 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.

115 T. Hayes, *Yo soy Pilgrim, ob. cit.*

cos. 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.[116] 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.[117]

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 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.[118]

116 G. Greenwald, *ob. cit.*

117 E. Snowden, citado en *ibid.*

118 *Ibid.*

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 la ley al vigilar sin justificación legal a los ciudadanos estadounidenses.[119] 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 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 USA Freedom Act solo afecta la recogida de información en los

119 *Le Monde,* 7 de mayo de 2015.

Estados Unidos. No cambia nada sobre la vigilancia que la NSA practica clandestinamente en el extranjero.[120]

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 1998, una excelente película, *Enemigo público*,[121] 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, quien explicaba en el film:

> Tú telefoneas a tu mujer 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 cuarenta, el Estado está compinchado con las empresas de telecomunicación y accede a todo: extractos bancarios, datos in-

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

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

> formáticos, 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 espías 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 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, en 1982, durante la guerra de las Malvinas entre Argentina y el Reino Unido, 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 los noventa, 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 —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 que, a diferencia de los documentos difundidos por Snowden en 2013, 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 entonces, 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 de Pierre Lellouche, secretario de Estado de Comercio Exterior; y el de Jean-Pierre Jouyet, de Asuntos Europeos. Y lo más preocupante: también aparece en ella el número de

una sección telefónica del Elíseo 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.[122]

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.[123]

Numerosos jefes de Estado «amigos» —Dilma Rousseff (Brasil), Enrique Peña Nieto (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 *Der 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

122 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-affairedes-ecoutes-de-la-nsa-pourquoi-la-france-savait).

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

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 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 Palacio del Elíseo, varios ministerios estatales (Interior, Justicia, Defensa, Asuntos Exteriores), la Asamblea Nacional…

Se sabe que las embajadas, sean del país que sean, suelen ser nidos de espías que se dedican a completar de forma ilegal, las informaciones recogidas abiertamente por los diplomáticos de carrera.[124] Tratándose de los Estados Unidos, esta particularidad alcanza proporciones desmesuradas. Desde hace mucho tiempo, ese país se invistió a sí mismo de la función geopolítica de «potencia imperial», así que sus embajadas en capitales extranjeras albergan innumerables servicios secretos.

---

124 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.

Esto se puede observar con claridad en la película *Zero dark Thirty*,[125] 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 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 puede 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

125 Kathryn Bigelow, *Zero Dark Thirty,* 2013.

> con el fin de vigilar masivamente los teléfonos móviles y las comunicaciones electrónicas de la población local.[126]

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 secretos alemanes (Buendesnachrichtendienst, 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.

---

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

En España, según reveló la prensa, el Centro Nacional de Inteligencia (CNI) tambien facilitó el espionaje masivo de los Estados Unidos. Los servicios de Inteligencia españoles conocían el trabajo de la NSA 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

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.[127]

Por otro lado, han puesto a punto su propio programa secreto de vigilancia electrónica, Tempora, que les permite acumular cantidades colosales de informaciones robadas. Solo en 2012, el GCHQ vigiló unos 600 millones de contactos telefónicos ¡cada día! Con total ilegalidad, sus agentes llegaron a conectarse a más de 200 cables de fibra óptica. Cada cable transporta 10 gigabytes[128] por segundo. En teo-

127 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.

128 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.

ría, los ordenadores del GCHQ pueden procesar unos 21 petabytes[129] 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.

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 y Unisys— 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

129 Un petabyte (PT) equivale a 10^{15} bytes.

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[130] y Nicky Hager[131] sabemos que, desde los años cincuenta, 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 o salen de los Estados Unidos. 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 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».[132]

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 las Naciones Unidas, en Nueva York, cuyo proveedor de acceso a Internet es esa coorporación. Paralelamente, se ha sabido también que AT&T suminis-

130 Duncan Campbell es el autor del primer artículo sobre Echelon, publicado el 12 de agosto de 1988 por el semanario británico *New Statesman.*

131 Nicky Hager es autor del libro *Secret Power* (1996), en el que, por primera vez, devela el funcionamiento de la red Echelon, y donde describe el papel que juega su país, Nueva Zelanda.

132 http://echelononline.free.fr/pages/chrono.html.

traba a la agencia de Fort Meade más de mil millones de lecturas de móviles al día.[133]

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 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.

133 *Le Monde*, 18 de agosto de 2015.

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 han sido calificadas de «liberticidas» por numerosas organizaciones de defensa de los derechos humanos,[134] 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 de punta. «En nuestra lucha contra el terrorismo —ha declarado, por ejemplo, el presidente Obama— necesitamos disponer de *todos* los instrumentos eficaces».[135]Según esta doctrina,

134 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/ (Nota del Traductor).

135 *Rue89* (http://rue89.nouvelobs.com), 31 de mayo de 2015.

la guerra asimétrica contemporánea, sobre todo contra el fenómeno yihadista —tanto el de Al Qaeda como, más recientemente, el del Estado Islámico o Daesh—, muy en especial contra sus «células durmientes» y 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,[136] 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».[137]

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 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,

136 Stephen Graham, *Villes sous contrôle. La militarisation de l'espace urbain*, trad. fr. de R. Toulouse, La Découverte, París, 2012. Edición original: *Cities Under Siege: The New Military Urbanism,* Verso, Londres, 2011.

137 Éric Verdeil, «Stephen Graham, *Villes sous contrôle. La militarisation de l'espace urbain*», *Lectures*, 25 de agosto de 2012 (http://lectures.revues.org/9021).

drones,[138] 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.[139]

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 3D Robotics, 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».[140] 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».[141] Nos dirigimos así hacia un mundo semejante al que imaginó, en 1987, el novelista británico Arthur C. Clarke en su relato de

138 A. Gévaudan, «Drones de combat», *Ragemag*, 7 de enero de 2014 (http://ragemag.fr/drone-combat-asimov-herbert-present-59198).

139 Anna Minton, «Attention, un robot volant vous espionne», *Courrier international*, 1ro. de abril de 2010.

140 *El País,* Madrid, 31 de agosto de 2015.

141 A. Gévaudan, «Drones: tu le sens bien, mon gros Male?», *Ragemag,* 27 de mayo de 2013 (http://ragemag.fr/dronest-le-sens-bien-mon-gros-male-29770).

ciencia ficción *2061: Odysea tres*.[142] 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[143] multiplican la cantidad de chivatos de todo tipo que nos cercan. En los 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.

Los televisores graban todo lo que los espectadores consumen en materia de programas audiovisuales, tanto

142 Este libro es el tercero de una tetralogía de novelas cuyos títulos en español son: *2001: una Odisea espacial*; *2010: Odisea dos*; *2061: Odisea tres* y *3001: Odisea final*.

143 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 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.[144]

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 micrófono oculto, capaz de grabar las conversaciones de los telespectadores, sin que estos lo supieran y transmitirlas a terceros.[145] Mike Gatto, quien preside la Comisión de protección del consumidor y de la vida privada en el Congreso de California, presentó incluso una proposición de ley para prohibir que los televisores pudieran espiar a la gente.

---

144 *El País,* Madrid, 2015.

145 A partir de entonces, Samsung anunció que cambiaría de política, y aseguró que, en lo adelante, el sistema de grabación instalado en sus televisores solo se activaría cuando el usuario apretara el botón de grabación.

Por el contrario, Jim Dempsey, director del Centro de 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 solo interesará a los anunciantes. También podría permitir la realización de evaluaciones psicológicas o culturales que, por ejemplo, interesarán también a las compañías de seguros»,[146] 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 llaman por teléfono en busca de empleo.

Nunca más solos

Repartidos por todas partes, los detectores de nuestros actos y gestos abundan alrededor de nosotros, incluso, como acabamos de ver, en televisores: sensores que registran la velocidad de nuestros desplazamientos e 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),[147] que descubren automáticamente nuestro perfil de consumidor, como hacen ya las «tarjetas de fidelidad» que generosamente ofrecen la mayoría de los grandes supermercados (Carrefour, Casino, Alcampo, Erozki…) y las grandes marcas (FNAC, el Corte Inglés, Galeries Lafayette, Printemps…).

---

146 *El País*, Madrid, agosto de 2015.

147 Que ya forman parte de muchos de los productos habituales de consumo, así como de los documentos de identidad.

Ya no estamos solos frente a la pantalla del 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, empresas publicitarias, entidades financieras, partidos políticos o autoridades gubernamentales.

El necesario equilibrio entre libertad y seguridad corre, por tanto, el peligro de romperse. En la película *1984*, de Michael Radford, basada en la novela de George Orwell, el presidente supremo, Big Brother, define así su doctrina: «La guerra no tiene por objetivo ser ganada, su objetivo es continuar. (…) La guerra la hacen los dirigentes contra sus propios ciudadanos y tiene por objeto mantener intacta la estructura misma de la sociedad».[148] Dos principios que, extrañamente, hoy están a la orden del día[149] 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, 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

148 Michael Radford, *1984*, 1984.

149 Ignacio Ramonet, entrevista con Noam Chomsky, *Infra,* pp. 168 y ss.

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».[150] 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*[151] («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: «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».[152]

---

150 A. Mattelart, *La Globalisation de la surveillance*, La Découverte, París, 2007; edición en español: *Un mundo vigilado*, Paidós, 2009.

151 Imaginado en 1791 por el filósofo utilitarista inglés Jeremy Bentham.

152 G. Greenwald, *Nulle part où se cacher*, *ob. cit.*

Hoy día, el sistema panóptico se ha reforzado con una particularidad nueva en relación con 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 impresionante número de sensores para espiar el comportamiento de cada usuario:[153] 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 —empresa matriz de Google— todo lo que hace el usuario en materia de navega-

153 «Google et le comportement de l'utilisateur», *AxeNet* (http:// blog-axe-net-fr/google-analyse-comportement-internaute).

ción. 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,[154] 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 donde 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

154 Ignacio Ramonet, entrevista con Julian Assange, *Infra,* pp. xxx y ss.

una de las miles de personas presentes en un estadio, una manifestación o un mitin político. [155]

A pesar de que hay estudios serios que han demostrado la débil eficacia de la videovigilancia[156] 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»,[157] 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.

---

155 Ver, 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=033ef14483ee899496648c-2b4b06233c).

156 «"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.

157 *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 solo 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».[158]

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

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

dico por exhibirse, que, con el apogeo de Internet, ha conocido una especie de explosión a través de las *webcams*, 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 *webcams*, se exhibían en línea (www.hereandnow.net) todos los días, a todas 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.[159]

Otro signo del poco apego que algunas personas tienen por 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».[160]

---

159 Denis Duclos, «La vie privée traquée par les technologies», *Le Monde Diplomatique,* agosto de 1999; Paul Virilio, «Le règne de la délation optique», *Le Monde Diplomatique*, agosto de 2000.

160 *Le Monde*, 14 de noviembre de 2000.

Por otra parte, desde principios del presente siglo 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 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.[161]

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, quien, 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».[162]

---

161 *Libération*, 25 de noviembre de 2000; *Le Monde*, 30 de noviembre de 2000.

162 *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, bajo la presidencia de George W. Bush el Departamento de Justicia de los Estados Unidos 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[163] 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 en cualquier parte del mundo puede

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

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 solo 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.[164] 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.

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

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 que iniciaba su segundo mandato, fue publicado con el título *Global Trend 2030. Alternative Worlds* («Tendencias mundiales 2030: nuevos mundos posibles»).[165] ¿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

165 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*, éditions des Équateurs, París, 2013.

ejemplo, Facebooklandia: más de mil millones de usuarios; o Twitterlandia: más de 800 millones. Su influencia en el juego de tronos de la 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.

Al 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 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,[166] un servicio de información ultrasecreto especializado en la captación clandestina de informaciones de origen electromagnético que depende

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

conjuntamente de la 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.[167]

167 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 guion de Mark Bomback y David Marconi (autor del guion de *Enemigo de Estado*) basado en el artículo de John Carlin «A Farewell to Arms», *Wired*, 5 de mayo de 1997. El filme se estrenó en España con el título *La jungla 4,0*, y en América Latina con el de *Duro de matar 4,0*.

CONCLUSIONES

«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*[168] 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 propias tradiciones. En este sentido, hay que recordar que el

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

acto fundador de los Estados Unidos fue la revuelta de los colonos norteamericanos contra una ley inglesa que autorizaba la violación de la vida privada. La explosión de cólera desembocó en la revolución norteamericana de 1776. La cuarta enmienda de la Constitución de los Estados Unidos protege siempre a los ciudadanos estadounidenses contra cualquier abuso de una administración que quisiera someterlos a una violación ilegal de su intimidad: «No será violado el derecho de los ciudadanos a la seguridad de sus personas, domicilios, documentos y bienes; contra cualquier registro o detención arbitrarios…».

El auge de Internet y de las nuevas redes electrónicas ofrece actualmente a los principales servicios estatales de escucha de las comunicaciones —la NSA, en los Estados Unidos; el GHCQ, en el Reino Unido; la DGSE, en Francia; el CNI en España— una inesperada ocasión para instaurar fácilmente una vigilancia sistemática y generalizada de todas las protestas políticas y sociales, precisamente porque Internet ya no es ese espacio de libertad descentralizado que permitiría escapar a la dependencia de los grandes medios de comunicación dominantes. Sin que la mayoría de los internautas se haya dado cuenta, Internet se ha centralizado en torno a algunas empresas gigantes que lo monopolizan y de las que ya casi no se puede prescindir. Lo confirma Laurent Chemla, uno de los pioneros de la Internet militante en Francia:

> No se vio venir la centralización de Internet, no entendimos que el modelo económico de publicidad-contra-gratuidad crearía un peligroso fenómeno de centralización, porque los anunciantes tienen interés en trabajar con los más grandes, aquellos que tienen más audiencia. En la actualidad, hay que conseguir ir en contra de esta lógica, para descentralizar de nuevo Internet. La

> opinión pública debe comprender que la gratuidad conlleva una centralización tal de Internet que, poco a poco, el control se vuelve más fuerte y la vigilancia se generaliza.[169]

Otro cambio: hoy la vigilancia se basa esencialmente en la información tecnológica, que es automática, más que en la información humana. Como en *Minority Report*, es el «predelito» lo que a partir de ahora se persigue. Para «anticiparse a la amenaza», las autoridades tratan de «diagnosticar la peligrosidad» de un individuo a partir de elementos de sospecha más o menos comprobados. Con la paradójica idea de que, para garantizar las libertades, hay que empezar por limitarlas.

Retorno del determinismo genético

En el nuevo Estado de vigilancia, toda persona es considerada sospechosa *a priori*. Sobre todo, si las cajas negras algorítmicas la clasifican mecánicamente como amenazante después de analizar sus contactos y sus comunicaciones. Esta nueva teoría de la seguridad, que es una variante del funesto determinismo genético, considera que el ser humano está desprovisto de verdadero libre arbitrio o de pensamiento autónomo. El hombre no sería sino una mera máquina sometida a la influencia de pulsiones de nacimiento y a fatalidades biológicas. Es inútil, por lo tanto, que, para prevenir eventuales desviaciones, se busque intervenir retroactivamente en el entorno familiar o en las causas sociales. Lo único que ahora quiere el Estado, con la fe puesta en los informes de vigilancia, es reprimir lo antes posible, antes

169 «Entretien avec Laurent Chemla», *Le Journal du Net*, 11 de marzo de 2015 (http://www.journaldunet.com/edbusiness/le-net/laurent-chemla-laurent-chemla-project-caliopen-shtml).

de que se cometa el delito. Esta concepción determinista de la sociedad, imaginada hace más de sesenta años por el excelente escritor estadounidense de ciencia ficción Philip K. Dick, se impone poco a poco en numerosos países, a medida que son golpeados por la tragedia del terrorismo.[170]

Metamorfosis de la justicia

El gran cambio arrancó en los Estados Unidos. Tras los atentados del 11 de septiembre de 2001, la ley Patriot Act modificó por primera vez en el seno de una democracia, la relación seguridad-vida privada. Explica la jurista francesa Mireille Delmas-Marty:

> Más que un cambio, es una auténtica metamorfosis de la justicia penal y por extensión, del control social (…). La Patriot Act ha hecho posible que, por orden del presidente, emerjan una vigilancia masiva y un régimen penal derogatorio, y que se llegue a amparar el uso de la tortura e incluso la organización de asesinatos selectivos (…). Se ha pasado muy rápidamente a una «guerra contra el terrorismo» desplegada sobre el conjunto del planeta; primero, con la apertura del campo de concentración de Guantánamo fuera del territorio de los Estados Unidos; y más tarde, con la «tela de araña» estadounidense, denunciada en 2006 por el Consejo de Europa: el mapa de centros secretos de detención en todo el mundo y las transferencias ilegales de detenidos. [171]

170 Recordemos que, en Francia, el antiguo ministro del Interior, Nicolas Sarkozy, afirmó en abril de 2007 que ciertos comportamientos, en especial la pedofilia y el suicidio de los jóvenes, tenían en su opinión «causas genéticas». *Philosophie Magazine*, abril de 2007.

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

Otras democracias han imitado a los Estados Unidos. De la Terrorism Act[172] en el Reino Unido, a la ley Renseignement en Francia, pasando por la Ley de Seguridad Ciudadana[173] en España, se ha multiplicado la legalización de la vigilancia clandestina de masas. Expresar en Internet una simple intención de cometer un acto irregular puede llevar hoy en algunos países democráticos, a la detención del internauta,[174] lo cual es contrario a uno de los principios fundadores de la justicia penal moderna. El jurista Beccaria[175] estableció en el Siglo de las Luces, que para declarar criminal a una persona, primero tiene que haberse cometido realmente el crimen o al menos haberse iniciado su ejecución.

La cuestión de la libertad

Nada que hacer: nuestro uso de Internet nos delata, lo cual ha llevado a Julian Assange a decir: «Internet ha sido transformado para convertirse en el más peligroso vehícu-

---

172 La ley Terrorism Act se promulgó en 2006, tras los atentados de Londres de julio de 2005. Fue reforzada en 2008 por la Counter-Terrorism Act, que, sobre todo, prolonga el plazo de retención hasta los 42 días.

173 Conocida popularmente como Ley Mordaza, entró en vigor el 1 de julio de 2015. Viene a completar el importante arsenal de medidas antiterroristas en España, especialmente la ya muy severa Ley Antiterrorista de 1984.

174 El 10 de marzo de 2004 entró en vigor el artículo 221-5-1 del Código Penal, que creó, en Francia, el delito de intención criminal. Esta ley castiga el «mandato criminal», es decir, el hecho de solicitar a una persona afín que cometa un delito, aunque el mandante no cometa la infracción principal. Castigar actos que aún no se han cometido constituye toda una innovación. Por lo tanto, con este artículo hay una derogación efectiva del principio de legalidad de los delitos y las penas, establecido por Cesare Beccaria.

175 Cesare Beccaria (1738-1794), jurista y filósofo italiano perteneciente al periodo de las Luces. En su libro *De los delitos y las condenas* funda el derecho penal moderno y se destaca por desarrollar la primera argumentación contra la pena de muerte.

lo del totalitarismo que jamás hayamos conocido». La red es «de ahora en adelante una amenaza para la civilización humana».[176]

Hay que admitir finalmente que, con la centralización de Internet, la «democracia digital», en la que se pudo creer en los albores, se ha revelado como una impostura y un engañabobos. Así lo explica François de Bernard:

> La «República digital» no es el gobierno del interés público por medio de las leyes —lo cual, según Rousseau, constituye la condición, si no la esencia, de toda República—, sino solamente el gobierno de los números, por los números y para los números; el gobierno de las cifras, de lo cifrado y destinado a la cifra, con el fin de que, con un simple clic del ratón, la República pueda ser gobernada con el menor número de obstáculos que pudieran dificultar el despliegue del proyecto de sus dirigentes.[177]

Succionados por la dinámica centralizadora, los gobiernos, los servicios de seguridad y las empresas gigantes de la Red se fusionan ante nuestros ojos en un complejo securitario-digital que tiene un objetivo preciso: controlar Internet para controlarnos mejor. En Internet, cada internauta está interconectado y proporciona, en tiempo real, una cantidad incalculable de informaciones personales que ningún Estado ni empresa privada habría soñado nunca poder recopilar.

Como «un ejército de ocupación» que controla los puntos de paso, los Estados impiden la independencia de la Red. Llevados al extremo, pueden alimentarse, como sanguijuelas, en las venas y las arterias de nuestras nuevas sociedades, atiborrándose con cada intercambio expresado o comunicado,

176 J. Assange *et al, ob. cit.*

177 François de Bernard, *L'Homme post-numérique*, éditions Yves Michel, París, 2015.

con cada mensaje enviado y con cada pensamiento *googleado*, y almacenar luego y para siempre, todo este saber —miles de millones de interceptaciones diarias, un poder inimaginable— en centros de procesamiento de datos.

Frente a este rodillo compresor, muchos ciudadanos tiran la toalla y se resignan a ver amenazada su libertad de expresión y violados sus derechos fundamentales. Están equivocados. Porque la auténtica cuestión no es la vigilancia, sino la libertad, como explica Edward Snowden:

> Cuando alguien dice: «No tengo nada que ocultar», en realidad está diciendo: «Me río de mis derechos». (…) Si dejáis de defender vuestros derechos pensando: «No necesito mis derechos en este contexto», ya no se trata de derechos. Los habéis convertido en algo de lo que disfrutáis como de un privilegio revocable por el gobierno. (…) Y ello reduce el perímetro de la libertad en el seno de una sociedad.[178]

Resistir, encriptar

¿Cómo defenderse? En primer lugar informándose y consultando las numerosas páginas web especializadas en seguridad informática.[179] También uniéndose a las diferentes organizaciones que luchan contra la vigilancia masiva, especialmente WikiLeaks[180] y en Francia, La Quadrature du Net.[181] Y sobre todo optando, en primer lugar, por la auto-

178 K. van den Huevel y S. F. Cohen, art. cit.

179 http://www.nextinpact.com; www.anonymat.org; http:// www.udernews.fr; http://assite.com.free.fr; http://sous-surveillance.fr. Véase también el sitio web de la Agencia Nacional de Seguridad de los sistemas informáticos (ANSSI): http:// www.ssi.gouv.fr.

180 https://wikileaksactu.wordpress.com.

181 www.laquadrature.net/fr.

defensa mediante la encriptación o codificación, como nos aconseja Edward Snowden: «La encriptación es una responsabilidad cívica, un deber cívico».

Solamente la encriptación permite enviar y recibir mensajes de correo electrónico codificados. Impide que una herramienta automática de vigilancia pueda leerlos si los intercepta. Aunque no se tenga nada que ocultar, la encriptación nos ayuda a proteger nuestra vida privada y la de las personas con quienes nos comunicamos, lo cual hará más difícil el trabajo de los espías del nuevo complejo securitario-digital.

Aunque muchos gobiernos, sobre todo después de los odiosos atentados del 13 de noviembre en París, están planteándose la prohibición de todo sistema de encriptación de mensajes, las revelaciones de Edward Snowden han permitido la emergencia y la democratización de varias herramientas de encriptación de mensajes sms y de comunicaciones telefónicas: Signal, Telegram, Wickr, TrueCrypt, ProtonMail, Threema, etc.

Oponerse a la vigilancia del Estado cuando se es inocente, es una lucha política. Y aprender a protegerse es la primera etapa de esta lucha. Después hay que pasar a la guerrilla digital: engañar a los espías, cegarlos, disimular nuestras conexiones a Internet, cifrar nuestros correos electrónicos, proteger nuestros mensajes. El objetivo es hacer que los algoritmos enloquezcan, crear zonas de opacidad y escapar a la inspección y al cacheo de los chivatos digitales secretos.

El derecho está de nuestra parte. Una importante sentencia del Tribunal de Justicia de la Unión Europea (TJUE), dictada el 6 de octubre de 2015, constituye efectivamente una gran victoria jurídica y alienta la rebelión de los ciudadanos contra la vigilancia masiva. En respuesta a

la demanda contra Facebook interpuesta por un joven austriaco, Maximilian Schrems, que a raíz de las revelaciones de Edward Snowden, acusó a la empresa gigante de haber colaborado con la NSA, el TJUE decidió ese día invalidar el acuerdo entre la Unión Europea y los Estados Unidos, firmado en el año 2000, llamado comúnmente Safe Harbor («Esfera de Seguridad»), que autorizaba a las empresas estadounidenses y especialmente a las GAFAM, a exportar a los Estados Unidos los datos personales de los europeos y almacenarlos allí.[182]

La sentencia Schrems debería obligar a Facebook a suspender la transferencia de datos a los servidores estadounidenses. También debería obligar a la Comisión Europea a ser más severa en la renegociación del acuerdo con Washington.[183] Y forzar a las GAFAM —que obtienen la mayor parte de sus ingresos de la explotación a gran escala de nuestros datos personales— a revisar sus prácticas.

Finalmente, el Consejo de Europa[184] ha estimado en un informe reciente que «mientras los Estados no acepten fijar límites a los programas de vigilancia masiva que llevan a cabo sus agencias de información, la codificación generalizada y orientada a proteger la vida privada, es la solución de repliegue más eficaz para permitir a la gente proteger sus datos».[185]

---

182 *Le Monde,* 7 de octubre de 2015.

183 Marc Rees, «*Safe Harbour:* Bruxelles prône la poursuite des flux des données transatlantiques», *NextINpact*, 6 de octubre de 2015 (www.nexintpact.com/news/96777-safeharbor-bruxelles-prone-poursuite-flux-donnees-transatlantiques.htm).

184 Creado en 1949, el Consejo de Europa tiene la misión de promover los derechos humanos en todo el continente. Sus principios han sido retomados por el Tribunal Europeo de Derechos Humanos (TEDH).

185 E. Tréguer, «Résistance multiforme», art. cit.

Más aún. Con ánimo de resistencia, algunos sitios web asociativos permiten iniciarse fácilmente en el cifrado de las comunicaciones digitales.[186] Hay también otras armas: la red de anonimato Tor[187] sobre todo; las empresas ProtonMail (Alemania) y Tutanota (Suiza), que ofrecen servicios para proteger mejor los correos; el sistema de explotación Tails;[188] la solución de ciframiento TrueCript, que permite ante todo cifrar archivos; o proyectos de mensajería como Caliopen, un software libre destinado a proteger la confidencialidad de los intercambios de sus usuarios, lanzado en septiembre de 2013 por Laurent Chemla.[189] Al parecer las revelaciones de Edward Snowden han generado una toma de conciencia de la importancia de la encriptación,[190] incluso en el seno de algunos organismos más oficiales, como el Internet Engineering Task Force (IETF), encargado de la estandarización de los protocolos de Internet a escala global.

Los lanzadores de alertas

Desde hace varios años, hackers, militantes contra el espionaje y lanzadores de alertas colaboran y se relevan para denunciar los abusos. Resisten al imperio de la vigilancia y

186 Por ejemplo, la web Autodefensa del correo (https:// emailselfdefense.fsf.org/es).

187 La red Tor puede hacer anónimos los intercambios en Internet basados en el protocolo de comunicación TCP; es decir, aproximadamente el 95 % de todo el tráfico de Internet.

188 Tails es un sistema cuyo objetivo es preservar la vida privada y el anonimato. Permite utilizar Internet de manera anónima y esquivar la censura en cualquier ordenador y en casi todos los sitios que se visitan. Tails no deja rastro alguno de lo que se hace, salvo que se le pida expresamente (https://tails.boum.org/about/index.fr.html).

189 Con respecto a Caliopen, véase «Entretien avec Laurent Chemla», art. cit.

190 F. Tréguer, «Résistance multiforme», art. cit.

son los héroes de la era Internet. Conocemos desde luego, a los tres más célebres: Julian Assange, Chelsea Manning y Edward Snowden, pero recordemos que otros iniciaron la resistencia antes que ellos. Por ejemplo, Mark Klein, un exejecutivo de la empresa AT&T, y el jurista Thomas Tamm, en los Estados Unidos. También algunos exagentes de la NSA, inspirados probablemente en el ejemplo de Daniel Ellsberg, un analista de la Rand Corporation que, en 1971, se atrevió a publicar los célebres *Pentagon Papers*,[191] que sacaron a la luz las razones ocultas de la intervención militar de los Estados Unidos en Vietnam —55.000 muertos del lado estadounidense, más de un millón del vietnamita—, un conflicto que jamás fue autorizado por el Congreso.

Entre los lanzadores de alertas anteriores a Snowden y exagentes de la NSA se puede citar también a Perry Fellwock y a Russell D. Tice. Y más recientemente, a William Binney, Thomas Drake, Edward Loomis y J. Kirk Wiebe, quienes junto a Diane Roark, del Comité para la Información de la Cámara de Representantes, llegaron a difundir públicamente un manifiesto contra la vigilancia masiva, el 17 de enero de 2014.[192]

En muchos países se han lanzado campañas para incitar a los agentes de información a que dimitan. Por ejemplo, en septiembre de 2015 y a iniciativa del colectivo berlinés Peng (www.pen.gg), grupos de artistas y activistas defensores de las libertades públicas pegaron, delante de las agencias de información estadounidenses y alemanas, banderolas animando a los espías con remordimientos a que abandonasen

191 http://www.wllsberg.net/archive.

192 «We Need Real Protection From The NSA» (http://www. information-clearinghouse.info/article37397.htm).

su trabajo. «¿Queríais servir a vuestros conciudadanos? Habéis terminado por espiarlos. ¡Dimitid!».[193]

De igual modo, ante la entrada de la base militar estadounidense de Danger, en Alemania, donde hay una importante estación de escucha de la NSA, unos activistas instalaron un panel estratégico en el que se podía leer: «Escuchad vuestro corazón, no nuestras conversaciones». Por otra parte, el sitio web IntelExit (www.intelexit.org) ofrece muchos consejos y argumentos para convencer a los agentes de que dejen sus funciones, y les ayuda también a redactar automáticamente una carta de dimisión.[194]

Por una Carta de Internet

Pero hay que hacer más y contraatacar. Muchos militantes anticibervigilancia proponen el lanzamiento de una Carta de Internet, semejante a la Carta de la ONU. Dice Snowden: «Es necesario que nuestra generación cree lo que Tim Berners-Lee, el inventor de la Red, llama la Gran Carta de Internet. Queremos definir lo que deben ser los "derechos digitales". ¿Qué valores debemos esforzarnos en proteger? ¿Cómo vamos a garantizarlos?».[195]

En una entrevista en *The Guardian*,[196] Tim Berners-Lee deseó, efectivamente, que esta Gran Carta[197] mundial que

193 *Le Monde,* 30 de septiembre de 2015.

194 Wired, 28 de septiembre de 2015 (http://www.wired. com/2015/09/campaign-help-surveillance-agents-quitnsa-gchq).

195 K. Vanden Heuvel y S. F. Cohen, art. cit.

196 *The Guardian,* Londres, 12 de marzo de 2014 (http:// www.theguardian.com/technologyu/2014/mar/12/online-magna-carta-berners-lee-web).

197 En alusión a la *Magna Carta* de 1215, que limitó por primera vez el poder absoluto de la Corona, y fue el fundamento del derecho y las libertades inglesas.

él exige consagre la vida privada, la libertad de expresión y el anonimato:

> Sin un Internet libre y neutral, sobre el que podamos apoyarnos sin tener que preocuparnos por lo que pasa entre bastidores, no podemos tener un gobierno abierto, ni una buena democracia, ni un buen sistema de salud, ni comunidades conectadas entre sí, ni diversidad cultural. (…) Nuestros derechos son pisoteados cada vez más en todas partes. Y el peligro es que nos acostumbremos a ello. Quiero, por tanto, aprovechar el 25 aniversario del nacimiento de la Web para invitarnos a todos a ponernos manos a la obra con el fin de retomar las riendas y definir la Web que queremos para los próximos veinticinco años.[198]

Con la cooperación de ONG internacionales y de juristas de todo el mundo, WikiLeaks ha creado también su propia Carta. Consta de trece principios,[199] denuncia la vigilancia del Estado como «un atentado a las leyes internacionales sobre los derechos humanos» y rechaza que los gobiernos utilicen su poder para controlarnos. Otros pensadores, como el filósofo François de Bernard, reclaman el derecho a «una objeción de conciencia digital».[200]

¿Cómo resistir? La solución está en buscar una multitud de microrresistencias, que pasan por la educación popular, la formación en herramientas informáticas de cifrado, la búsqueda de soluciones alternativas para volver caducas las actuales normas dominadas por las GAFAM.

---

198 *Numérama*, 12 de marzo de 2014 (http://www.numerama.com/magazine/28719-1-inventeur-du-web-veut-unecharte-mondiale-pour-proteger-internet-html).

199 Se puede leer el texto íntegro en la web https://wikileaksactu.wordpress.com.

200 F. de Bernard, «Pour une objection de conscience numérique», *Mémoire des luttes*, 2 de septiembre de 2015 (http://www. medlu.org/Pour-une-objection-de-conscience).

La batalla por los nuevos derechos cívicos en la era digital no ha hecho más que comenzar. Los Estados de vigilancia se apoyan en su carácter democrático para manifestarse especialmente implacables contra los nuevos disidentes. No es casualidad que Snowden decidiera difundir sus espectaculares revelaciones sobre el programa PRISM justo el día en el que comenzaba en los Estados Unidos el proceso contra Chelsea Manning —antes Bradley Manning—, acusada de transmitir archivos secretos a WikiLeaks; la misma fecha en la que se cumplía también el primer aniversario de la reclusión de Julian Assange en los locales de la embajada de Ecuador en Londres, donde hubo de encontrar refugio para evitar ser extraditado a los Estados Unidos vía Suecia.

Snowden, Manning, Assange, tres héroes de nuestro tiempo, acosados y perseguidos por el imperio de la vigilancia. Edward Snowden se arriesga a una pena de treinta años de prisión tras haber sido acusado por los Estados Unidos de espionaje, robo y utilización ilegal de bienes gubernamentales. El 21 de agosto de 2013, Chelsea Manning fue condenada a treinta y cinco años de prisión. Y Julian Assange está amenazado con la pena de muerte.[201]

A aquellos que se preguntan por qué estos tres paladines de la libertad asumen tantos riesgos, Snowden les responde:

> Cuando te das cuenta de que el mundo que has ayudado a crear será peor para la nueva generación y para las siguientes, y de que no deja de reforzarse la capacidad de esta arquitectura de la opresión, comprendes que hay que denunciarla y que, por

201 La ley sobre espionaje, promulgada en 1917, en el momento en que el presidente de los Estados Unidos, Woodrow Wilson, buscaba criminalizar a todos aquellos que se oponían a entrar en guerra, prevé sanciones muy duras: cadena perpetua e incluso pena de muerte.

eso, debes aceptar todos los riesgos. Cualesquiera que sean las consecuencias.

A todos los ciudadanos libres de actuar de la misma forma, una sola consigna: «¡Contra la vigilancia masiva, resistencia masiva!».

ANEXOS

I

ENTREVISTA CON JULIAN ASSANGE[202]

«Google nos espía e informa de ello al gobierno de los Estados Unidos».

Desde el 19 de junio de 2012, Julian Assange, paladín de la lucha por una información libre, vive en Londres, refugiado en las oficinas de la embajada de Ecuador. Este país latinoamericano tuvo el coraje de brindarle asilo diplomático cuando el fundador de WikiLeaks se hallaba perseguido y acosado por el gobierno de los Estados Unidos y varios de sus aliados: Reino Unido, Suecia… La justicia sueca ha tratado de oír su testimonio sobre las acusaciones de agresión sexual hechas por dos mujeres a las que él habría mentido sobre el uso de un preservativo. Julian Assange niega estas acusaciones y sostiene que las relaciones con estas dos demandantes habían sido consentidas y afirma ser víctima de un complot organizado por Washington. Se niega a ir a Suecia, a menos que la justicia de ese país le garantice que no será extraditado a los Estados Unidos, donde podría ser llevado ante un tribunal y quizás, según sus abogados, condenado a la pena de muerte por delito de espionaje.

En varias ocasiones, Assange ha propuesto responder por videoconferencia a las preguntas de los encargados de la

202 Revisada por Julian Assange.

investigación. Estos lo han rechazado, argumentando que él huyó de Suecia a sabiendas de que había abierta una investigación en su contra. El Tribunal Supremo sueco rechazó, el 11 de mayo de 2015, su demanda de que fuera anulada la orden de detención.

En realidad, el único crimen de Assange es haber difundido, vía WikiLeaks, los archivos sobre los crímenes de guerra cometidos durante los conflictos de Irak y Afganistán, y los tejemanejes e intrigas de la diplomacia estadounidense. Como Edward Snowden y Chelsea Manning, Julian Assange forma parte de un nuevo grupo de disidentes políticos que, por luchar por una nueva forma de emancipación, son actualmente rastreados, perseguidos y hostigados no por regímenes autoritarios, sino por Estados que pretenden ser «democracias ejemplares».

En su nuevo libro, *Cuando Google encontró a WikiLeaks*,[203] Julian Assange va más lejos en sus revelaciones, siempre muy bien documentadas. Todo parte de una larga conversación que Assange sostuvo en junio de 2011, con Eric Schmidt, presidente ejecutivo de Google.[204] Este vino a entrevistar al creador de WikiLeaks para un ensayo que estaba preparando sobre el porvenir de la era digital, titulado *The New Digital Era*.[205] Cuando se publicó, Assange constató que sus declaraciones habían sido tergiversadas y

---

203 OR Books, Nueva York, 2014. Edición en español: Clave Intelectual, Madrid, 2014.

204 En agosto de 2015, tras el anuncio de la creación del conglomerado Alphabet, casa matriz que controla a partir de ahora todas las actividades del gigante de Silicon Valley, Google se ha convertido en una simple filial. Eric Schmidt ha sido nombrado presidente del consejo de administración de Alphabet.

205 Eric Schmidt, Jared Cohen, *The New Digital Age*, Knopf, Nueva York, 2013.

que las tesis defendidas por Schmidt eran bastante delirantes. Y decidió responder a las elucubraciones del que en la actualidad es presidente de Alphabet.

Entre muchas otras cosas, Assange revela en su libro cómo Google —y Facebook, Amazon, etc.— nos espía, y cómo estas empresas transmiten esa información a las agencias de inteligencia de los Estados Unidos. Y muestra también cómo el célebre buscador está estrechamente ligado, casi de forma estructural, al Departamento de Estado. Afirma también Assange que hoy las grandes empresas de la galaxia digital nos vigilan y nos controlan más que los propios Estados. Atención —nos dice—: cuando navegáis por Internet dejáis detrás de vosotros, como Pulgarcito, rastros de vuestra vida privada que algunas empresas privadas, especialmente Google, recogen y archivan secretamente. Algún día podrían servirse de ellos para utilizarlos contra vosotros.

Nos encontramos en Londres el 24 de octubre de 2014, en una pequeña sala de la embajada de Ecuador.[206]

El tema central de tu nuevo libro —Cuando Google encontró a WikiLeaks— *lo constituye un encuentro tuyo, en junio de 2011, con Eric Schmidt, presidente ejecutivo de Google. En ese texto dices: «Google es la compañía más influyente del mundo». ¿Qué entiendes por «más influyente»?*

Lo que intento decir es que el mundo está viviendo un cambio muy profundo, y que Google es la empresa de

206 Hemos de señalar que el texto de Julian Assange («What WikiLeaks Teaches us About how the US Operates») que hemos citado anteriormente, acaba de ser publicado como prólogo del libro *The WikiLeaks Files: The World According to US Empire*, Verso, Londres/Nueva York, 2015.

comunicación que más influencia tiene en lo esencial de ese cambio, y tal vez también sobre la velocidad de ese cambio. Podríamos preguntarnos también si Google no es la empresa más influyente en términos absolutos. De esto no estoy seguro. Hay varias megaempresas que podrían ocupar esa posición, la de ser la más influyente en términos absolutos. Pero al menos, de entre las empresas de comunicación, sí es desde luego la más influyente. Otras compañías pueden tener mucha influencia, como General Electric, o Raytheon, o Booz Allen Hamilton, o ExxonMobil, o Chevron, pero todas ellas tienen, más o menos, un modelo de negocio estabilizado y el tipo de influencia que ejercen no es tan evidente. Son muy grandes, sí, pero son estáticas. En cambio, Google está en evolución constante; duplicó su valor bursátil entre 2011 y 2015, pasando de 200.000 millones de dólares a 400.000 millones. Y su penetración en la sociedad global, en términos de interacción con los individuos, ha aumentado más que la de cualquier otra empresa de gran tamaño.

¿Más que las empresas financieras?

Sí, no hay duda.

Escribes que «el avance de la tecnología de la información, encarnada por Google, anuncia la muerte de la privacidad para la mayoría de las personas y reconduce el mundo hacia el autoritarismo». ¿No es esto demasiado pesimista?

No creo que se pueda mirar el mundo y decidir si uno quiere hechos optimistas o pesimistas. Los hechos son como son. Hay otros fenómenos que se están produciendo y podemos considerarlos como optimistas, pero no lo que Google está haciendo.

¿En qué te basas para afirmar que «las tecnologías de Silicon Valley son un instrumento al servicio de la política exterior de los Estados Unidos»?

En varios puntos que describo en el libro. En primer lugar, la larga historia de colaboración entre el complejo militar-industrial de las fuerzas armadas de los Estados Unidos y Silicon Valley. Cualquier persona que haya investigado sobre Silicon Valley sabe que eso es así. Noam Chomsky denunció con contundencia lo que ocurría en Silicon Valley en las décadas de los setenta y los ochenta.[207] De hecho, si miramos hacia atrás y pensamos en cuál era la percepción que se tenía de los ordenadores en esa época, eran unas máquinas enormes que los militares hacían funcionar y las ponían al servicio de las grandes empresas estadounidenses. La idea negativa que la gente se hacía del superpoder de los ordenadores está reflejada en películas como *Colossus*.[208] En todo caso, en esa época eran los militares los que pilotaban el desarrollo tecnológico del Estado: ayudando a llegar a la Luna, ayudando a construir armas atómicas, ayudando a diseñar misiles ICBM,[209] ayudando a acelerar la velocidad de los submarinos nucleares, ayudando al Servicio de Impuestos Internos a verificar la fiscalidad de cada persona...

---

207 «Noam Chomsky on Government, Silicon Valley and the Internet», entrevista con Noam Chomsky realizada el 15 de agosto de 2012 por Jegan Vincent de Paul (http://www. socialphy.com/posts/computers-technology/17119/Noam-Chomsky-on-Government-Silicon-Valley-and-the-Internet.html).

208 Joseph Sargent, *Colossus: The Forbin project,* 1970 (título en español: *Colossus, el proyecto prohibido*), película de ciencia ficción. Narra cómo el gobierno de los Estados Unidos cede la defensa del país a un superodenador que se conecta con el superordenador de los soviéticos, llamado Guardian, para formar juntos un hiperordenador que, consciente de su poder, toma el control del planeta.

209 Misil balístico intercontinental.

Todo eso cambió cuando Silicon Valley en los años noventa, empezó a desarrollar un mercado de consumo, a poner los avances de la tecnología informática al alcance del gran público. Fue entonces cuando se empezó a crear una «burbuja de percepción», una matriz de opinión que presentaba a las empresas de Silicon Valley como «amigas» de la gente, «amigas» del consumidor. Apple, Google, Amazon y más recientemente Facebook han estimulado ese aspecto positivo y se han beneficiado de ello. Y todo eso ha creado una ilusión que ha permitido obliterar la visión previa, negativa, que la mayoría de los académicos tenía en relación con Silicon Valley, un Sillicon Valey que colaboraba con los militares.

En segundo lugar, estas nuevas compañías, como Google, que describo en mi libro, establecieron una estrecha relación con el aparato de Estado en Washington, en particular con los responsables de la política exterior. Esa relación es una evidencia ahora. La tienen los más altos ejecutivos de Google: Eric Schmidt, Jared Cohen…[210] Ellos tienen ideas políticas semejantes y comparten una idéntica visión del mundo. A fin de cuentas, esta asociación tan estrecha y esta visión del mundo compartida entre Google y la Administración estadounidense están al servicio de los objetivos de la política exterior de los Estados Unidos.

En esa misma línea escribes que cuando Eric Schmidt visitó China, Corea del Norte y Birmania en 2013, era claro que

210 Jared Cohen es el director de Google Ideas, un laboratorio de ideas (*think tank*) apadrinado por Google con el objetivo de «identificar los desafíos globales y definir las soluciones tecnológicas que pueden darles una respuesta». Fue asesor de Condolezza Rice y de Hillary Clinton, secretarias de Estado respectivamente de George W. Bush y de Barack Obama.

estaba llevando a cabo una operación de diplomacia encubierta para Washington. ¿Qué pruebas tienes de ello?

Hablo basándome en mi experiencia. Pudimos demostrar que cuando había un flujo de información entre Eric Schmidt y yo, inmediatamente esa información llegaba a los niveles más elevados del Departamento de Estado. Y cuando Eric Schmidt me contactaba por medio de Lisa Shields,[211] las informaciones que él me transmitía le habían llegado antes del Departamento de Estado. Respecto a la diplomacia encubierta con Corea del Norte y con algunos países con los que Washington no quiere ser visto manteniendo comunicaciones de forma directa, no soy yo quien lo afirma, yo simplemente repito y reproduzco las afirmaciones de otras personas bien informadas. Pero yo, como acabo de decir, tuve la experiencia concreta del papel de Eric Schmidt como informador del Departamento de Estado. Otros expertos también supieron evaluar lo que Schmidt hizo como «agencia» del Departamento de Estado en Corea del Norte y en otros países.

Hace unos meses, Eric Schmidt estuvo en Cuba.[212] *¿Crees que también era para llevar a cabo una diplomacia encubierta?*

Sí, eso creo.[213]

---

211 Lisa Shields, compañera de Eric Schmidt y directora de Comunicaciones del Council on Foreign Relations (Consejo de Asuntos Exteriores), el laboratorio de ideas más importante de Washington, especializado en relaciones internacionales, vinculado a los demócratas del Departamento de Estado.

212 *Challenges,* 29 de junio de 2014.

213 Julian Assange no se engañaba: seis meses después de la visita de Eric Schmidt, La Habana y Washington anunciaban, el 17 de diciembre de 2014, que Cuba y los Estados Unidos iban a «normalizar» sus relaciones.

¿Cometiste un error cuando recibiste en 2011 a Eric Schmidt y a sus amigos cercanos a la Administración estadounidense? ¿Pecaste de ingenuo?

Yo estoy acostumbrado a reunirme con muchas personas de todo tipo, desde hace mucho tiempo. Por ejemplo, periodistas con antecedentes dudosos. Pero no tenía tiempo de evaluar cuáles eran las motivaciones de Eric Schmidt y sus amigos (Jared Cohen, Lisa Shields, Scott Malcomson)[214] para venir a verme. Preparé la cita de forma similar a como siempre lo había hecho. Obviamente tuve mucho cuidado en no revelar detalles de nuestras operaciones o los nombres de los miembros de mi equipo, ese tipo de precauciones habituales. Si lees cuidadosamente la transcripción de mi conversación con Schmidt, verás que intento desviar un poco algunas preguntas demasiado «curiosas». Por ejemplo, cuando me pregunta cómo WikiLeaks se protegía técnicamente a sí misma. En lugar de responder a eso, describo cómo WikiLeaks se protegía ¡en etapas anteriores! Pero hay mucho que uno puede aprender sobre una persona cuando conversas con ella durante un largo rato. La visita de Eric Schmidt y sus tres acompañantes del Departamento de Estado duró más de cinco horas. Es un tiempo suficientemente largo como para poder sacar una impresión relativamente precisa sobre la salud de alguien, su estado de ánimo, qué es lo que le interesa, de qué se ríe, etc. Y yo ahora, claro, sería un poco más cuidadoso si hubiera sabido que ese tipo de información, recogida sobre mí por Eric Schmidt, iba a ir directamen-

214 Scott Malcomson fue asesor de Susan Rice, demócrata, exsecretaria de Estado adjunta para asuntos africanos, luego asesor del Conseil on Foreign Relations, y director de Comunicación en el International Crisis Group, una ONG especializada en conflictos y considerada próxima a la OTAN.

te hacia el Departamento de Estado. Pero, dicho esto, yo también recogí una excelente información sobre él, y eso me reveló quién era realmente Schmidt, y creo que los lectores también lo perciben. Si se analiza cuidadosamente lo que él y las tres personas que lo acompañaban me preguntaron, de qué se reían, la diferencia entre una risa verdadera y una risa falsa, se pueden sacar algunas conclusiones. Por ejemplo, está muy claro que Eric Schmidt ve a China como enemigo. Porque cuando yo hice bromas sobre cómo con WikiLeaks, habíamos engañado a la seguridad china, la risa de Schmidt fue más fuerte y espontánea, mientras que en otros momentos su risa sonaba falsa.

¿Te decepcionaste al ver la versión manipulada de esta conversación que daba Schmidt en su libro?

Me sentí más decepcionado por el libro de Schmidt como libro. Eso sí me decepcionó. Pero también fue muy interesante descubrir las pretensiones del libro. Yo también había grabado nuestra conversación, nuestro encuentro. Por tanto, sé exactamente lo que yo le había dicho a Schmidt y lo puedo comparar con lo que él reprodujo. Así pude ver lo que él estaba intentando hacer. Pude vislumbrar el objetivo de Schmidt cuando analicé qué partes de la conversación había conservado, cuáles había ocultado y cuáles había distorsionado. Su propósito no era atacarme a mí, aunque dijo algunas cosas hirientes. Lo que él intentaba era posicionar a Google como el «visionario geopolítico» que necesitaban los Estados Unidos, para que las autoridades de Washington acudieran a él y escucharan a Google.

Dices que muchos ciudadanos critican el espionaje y el control ejercidos por el Estado, pero sin embargo notas que son muy pocos los ciudadanos que critican la vigilancia ejercida por las empresas privadas. ¿Es tan peligrosa esta como la de los Estados?

¿Estás presuponiendo que hay una diferencia entre el Estado y las grandes empresas privadas?

[risas].

Te hago la pregunta. Tengo mi propia opinión. [risas].

Esta división entre Estados y grandes empresas privadas está desapareciendo en la mayor parte de los países de Occidente. Pero la complicidad es más clara en los Estados Unidos, donde por ejemplo, el 80 % del presupuesto de las agencias de seguridad nacional va a la industria privada. Incluso la agencia de inteligencia más secreta de los Estados Unidos, la NSA, que forma parte del núcleo más protegido del Estado, destina el 80 % de su presupuesto a las industrias del sector privado. Por lo tanto, es interesante preguntarse por qué ha habido más investigaciones sobre el espionaje del Gobierno que sobre el espionaje de las empresas privadas.

Creo que están ocurriendo dos cosas. En primer lugar, una ley general: cuando aumenta el grado de abstracción de un problema disminuye el número de personas que pueden entender esa abstracción. Por ejemplo, cuando el Gobierno estadounidense contrata a la empresa militar privada Blackwater[215] para que sus mercenarios operen en Oriente Próximo, ¿cuánta atención se presta al número de merce-

215 Blackwater USA ha cambiado de nombre varias veces y ahora se llama Academi. Es una empresa militar considerada el ejército privado más potente del planeta. Ha intervenido en Irak y Afganistán.

narios que intervienen en Irak o en Afganistán, comparado con lo que se publica sobre el número de militares de las fuerzas armadas en estos mismos escenarios de operaciones? ¿Cuánta atención se les da a los mercenarios de Blackwater cuando matan a alguien o cuando cometen un delito, comparado con la cobertura mediática cuando el «error» lo comete un militar? Y sin embargo, en ambos casos, el Gobierno estadounidense es el amo que da las instrucciones y financia las operaciones. Se le da un nombre diferente, y darle a algo un nombre diferente es suficientemente eficaz para disimular la realidad.

Y en segundo lugar, especialmente en los Estados Unidos, está el aspecto ideológico. Por un lado tenemos a la izquierda estadounidense. Casi toda esa izquierda liberal está en el seno del Partido Demócrata, en un sistema clientelista y por lo tanto, no está ejerciendo un examen adecuado de lo que está sucediendo con los excesos del Gobierno, especialmente con la privatización generalizada. Y, por otro lado, tenemos la parte liberal del Partido Republicano que dice que solo el Gobierno es el problema, nunca el sector privado. Sin embargo, el sector privado es quien dirige al Gobierno. Y algunas grandes empresas, como Google o Goldman Sachs, con su enorme tamaño y sus monopolios, están dirigiendo los servicios centrales del Estado como si fueran el propio Gobierno. Algunas de estas empresas privadas tienen una cifra de negocios anual superior al PIB de Nueva Zelanda o de otros países.

Ecuador, por ejemplo.

En efecto, de Ecuador. Si comparamos la empresa petrolera Chevron, que tiene una facturación de unos 300.000

millones de dólares al año y Ecuador, que tiene un PIB de unos 95.000 millones de dólares al año, la diferencia es abismal. Sabemos que hay un conflicto entre estas dos entidades.[216] Chevron intenta presentar a Ecuador como un «Estado poderoso» que utiliza la fuerza coercitiva para poder reducir e intimidar a una empresa privada. Pero si consideramos su poder financiero, no cabe duda de que Chevron es la entidad con más recursos de las dos. No es comparable. Chevron es tan grande que ha podido asociarse, además, al poder de los Estados Unidos, que también posee la habilidad de usar la fuerza coercitiva, no de manera directa, pero sí de forma indirecta, para tratar de intimidar hábilmente a Ecuador, movilizando, si es necesario, a la llamada sociedad civil.

¿No crees en el concepto de «sociedad civil»?

En el concepto sí, pero no en su práctica. La mayoría de las organizaciones de la llamada sociedad civil están financiadas para convertirse en agentes del Estado o de las empresas más poderosas. En mi libro doy bastantes ejemplos de esto, no para probar este punto, sino para estudiar lo que hace Google. La New America Foundation, por ejemplo, en Washington, ¿quién la financia? La respuesta es: Eric Schmidt personalmente y Google como compañía, y el Departamento de Estado, y Radio Free Asia, y varias entidades más, pero las que he mencionado son las principales patrocinadoras. Y su directora general, Anne-Marie Slaughter, trabajó anteriormente como asesora muy cercana a Hillary Clinton en el Departamento de Estado, donde sigue trabajando. Y es profesora en Princeton al mismo tiempo. Por lo tanto, aquí los tenemos a todos juntos:

216 Ignacio Ramonet, «L'Équateur et les 'mains sales' de Chevron», *Mémoires des luttes*, París, 2 de diciembre de 2013.

Eric Schmidt a título personal, Google como compañía, el Departamento de Estado como parte del Ejecutivo de los Estados Unidos. Igual ocurre con Radio Free Asia, y con el mundo académico representado en parte en la New Foundation, por Anne-Marie Slaughter.

Eric Schmidt es miembro del Consejo de Administración de muchas de estas fundaciones, junto con directivos de Facebook. Aunque —desde lejos— parece que Google y Facebook son competidores, en realidad a nivel social no se oponen entre sí, cooperan en fundaciones y también trabajan con el Estado, como en el caso de su participación en común en la New America Foundation. En el libro entro más en detalle con esta fundación porque es la más significativa desde el punto de vista político. Es como el hogar político de Eric Schmidt en Washington. Aunque él y varios ejecutivos de Google están involucrados también en otras fundaciones que pretenden encarnar la sociedad civil.

Dices que «detrás de la fachada de la democracia lo que hay, en realidad, es un poderoso deseo de controlar a los ciudadanos». ¿En qué te basas para afirmar esto?

¿Tiene que ver tu pregunta con esta falsa sociedad civil?

Sí, es la idea. Lo que llamamos «democracia representativa», en realidad escondería, según afirmas, un gran deseo de controlar a la gente.

Ya veo. Seguramente conoces la famosa afirmación de Noam Chomsky: «Los medios de comunicación son a la democracia lo que la propaganda es a la dictadura».

Sí, instrumentos de manipulación.

Elementos indispensables del sistema de control.

A ese respecto, háblame de Total Information Awareness. No te pido que la describas, lo haces en el libro, pero ¿crees que ese proyecto ha sido abandonado realmente?

¿Total Information Awareness? No, no, en absoluto. Disponemos de documentos que WikiLeaks no ha publicado todavía sobre el nacimiento de Total Information Awareness (TIA). Y mi conclusión, después de estudiar a fondo su evolución, es que, inmediatamente después de los atentados del 11 de septiembre de 2001, el complejo de los servicios de inteligencia estadounidense quiso obtener más poder. Aprovechar el choque emocional para conseguir muchas cosas que habían querido hacer desde hacía mucho tiempo, aunque estos servicios ya eran muy poderosos. No es que no hubiera vigilancia masiva antes del 11 de septiembre, sí la había. La Agencia Nacional de Seguridad (NSA) era ya como «la gran bestia» en Washington y ya recopilaba una enorme masa de información. Pero inmediatamente después del 11 de septiembre, el Ejército pensó que podía apoderarse de esa parte del pastel y quitarle la suya a la NSA. Por lo tanto, hicieron esa propuesta de Total Information Awareness, con algo llamado Moad (Mother Of All Databases, la madre de todas las bases de datos), que incluía toda la información que se había reunido en los Estados Unidos: la de la CIA, la de los satélites y la de las demás agencias de inteligencia. Y este proyecto se aprobó inicialmente. Pero la NSA vio esta intromisión del Ejército como una amenaza para su propio poder institucional. Por lo tanto, la NSA luchó contra Total Information Aware-

ness. Y no ganó inicialmente. Se estableció una especie de cibercomando supremo que no estaba dirigido por la NSA. Y la oficina de la TIA tampoco estaba dirigida por la NSA. Entonces, la NSA se unió con los demócratas, con los principales responsables demócratas, y empezaron a atacar ese proyecto. Una vez que lo debilitaron bajo el pretexto de que de algún modo, constituía una amenaza para las libertades civiles, empezó a digerir los trozos, las piezas de la TIA y a integrarlos en el seno de la NSA. Finalmente, la NSA absorbió la mayor parte de los elementos del proyecto Total Information Awareness. O sea, el proyecto como tal ha desaparecido, pero todos sus objetivos siguen vigentes y forman parte ahora de las misiones de la NSA.

A tus lectores les dices: «¡Aprendan cómo funciona el mundo!». Pero ¿dónde pueden aprender eso?

En primer lugar, comprando y leyendo mi libro.

[risas].

¿Y después?

La revolución de las nuevas tecnologías de la comunicación ha conectado a todas las sociedades unas con otras. Eso significa que conectó a todos los espías de una sociedad con los de otra sociedad, incluyendo a los principales espías, los de la NSA, y eso reforzó los aspectos negativos de la globalización. Por ejemplo, la competencia económica superagresiva, las transferencias financieras a la velocidad de la luz. Eso significa que los grupos dominantes, ya poderosos, pueden ahora multiplicar su poder gracias a Internet y

extenderlo a todos los países cuyas sociedades se están fusionando también gracias a Internet. Pero por otro lado este proceso, esta misma revolución tecnológica, ha permitido a muchas personas, en todas partes del mundo, educarse unas a otras mediante la transferencia lateral de la información. Y eso nos permite, en principio, informarnos mejor y comprender cómo funciona realmente el mundo.

¿Es el aspecto positivo del que hablábamos al principio?

Sí. La NSA y las organizaciones de espionaje semejantes a ella, como Google y otras empresas cuyo negocio es recoger información privada, han estado sacando información de las personas menos poderosas y archivándola para utilizarla en su provecho. Y esto ha aumentado su poder en gran medida. Aumentó el poder de aquellos que ya tenían mucho poder. Es el aspecto negativo.

Por otro lado, esa transferencia lateral de información aumentó el conocimiento y por lo tanto, el poder de millones de personas. Y surgieron unas cuantas organizaciones, no muchas, como WikiLeaks, que se especializan en recoger datos secretos de esas organizaciones superpoderosas para ponerlos a disposición de todo el mundo, para reequilibrar la falta de igualdad en materia de poder.

En cierto modo, no he respondido a tu pregunta, pero ahora hay muchas formas de aprender. Y los últimos cinco años han sido la época de mayor educación política que haya habido nunca, no para todos los países, pero si se mira esta educación que se está produciendo al mismo tiempo en todo el mundo, eso no había ocurrido nunca antes.

¿Crees realmente que Internet ha conseguido poner fin a la asimetría de la información?

Sí, pero, como lo acabo de explicar, las grandes empresas privadas y el Estado están intentando controlar este fenómeno recogiendo todavía más información.

Dices que «no es el Estado quien debe saberlo todo sobre los ciudadanos, sino los ciudadanos quienes deben saberlo todo sobre el Estado».

Sí, así debe ser. ¿A quién le importa la transparencia? A nadie realmente. La gente no nace con el tema de la transparencia en sus corazones. No piensan en la transparencia a la hora de la muerte.

Seguro.

La gente nace con deseos de justicia y antes de morir, quieren haber sido tratados con justicia. Lo mismo ocurre con el respeto a la vida privada. Transparencia y respeto a la vida privada son solo importantes porque son mecanismos que dan o quitan poder.

Afirmas que WikiLeaks contribuyó a hacer caer dos dictaduras: en Túnez y en Egipto. ¿Estás convencido de ello?

Muchas personas están convencidas de ello.

¿Está demostrado?

Los ministros de Ben Ali[217] admiten que la divulgación de unos cables con información explosiva por parte de

217 Zine El-Abidine Ben Ali, presidente de Túnez desde el 7 de noviembre de 1987 hasta el 14 de enero de 2011.

WikiLeaks fue lo que quebró la espina dorsal del sistema del presidente tunecino. Es evidente que estas divulgaciones jugaron un papel importante. Llegaron en el momento propicio y en un contexto de gran descontento social. Pero en realidad lo que hizo caer a Ben Ali fue el propio Ben Ali.

La dictadura misma, claro.

Sí.

Quisiera ir más allá. Dices que cuando se produjeron las Primaveras Árabes y las revueltas de jóvenes a través del mundo, desde Los Indignados de España hasta los manifestantes de Occupy Wall Street, «Internet se convirtió en un demo, un pueblo que comparte cultura, valores y aspiraciones, en un lugar en el que tiene lugar la historia». ¿No es excesivo decir que Internet es un «pueblo»?

Antes de 2005, Internet era un lugar muy apático. Pero luego, en parte gracias a WikiLeaks, se produjo un cambio muy grande.

Sin embargo, ¿no crees que es excesivo decir que «Internet es un demo»?

Es excesivo decir que Internet, en su totalidad lo es. Pero hay millones de personas en Internet —ignoro su número exacto— que se perciben a sí mismas como parte de ese demo. En cambio, hay otros millones de personas que utilizan Internet y no se conciben a sí mismas como parte de ese demo de Internet. Pero eso no impide que haya

millones de personas, repito, que sí se perciben a sí mismas como parte de él. Incluso conozco a personas a las que les pregunté: «¿De dónde sois?». Y hubo quien me contestó: «Soy de Internet».

Generación Internet.

Es extraño. Pero lo dicen en serio, no en broma. Sienten genuinamente que Internet es el lugar donde su cultura personal ha emergido.

¿Sigues pensando que compartir la información es una manera de liberar al mundo?

No hay otra esperanza. Nunca hubo ninguna otra esperanza. Esta fue siempre la lucha. Que las personas reciban información. Si retrocedemos al tiempo de los griegos, a los debates durante la Ilustración, a los enfrentamientos en China, a las guerras de independencia en América Latina o a las luchas poscoloniales, el primer paso siempre fue comprender la situación, comprender qué es posible y qué no es posible hacer. Incluso si nos apartamos de las cuestiones que tienen que ver con la distribución de recursos y el desequilibrio de los poderes —porque a veces pienso que las izquierdas se centran exclusivamente en estas cuestiones—, si miramos simplemente de qué es capaz el ser humano cuando está en sus mejores condiciones, y qué es capaz de hacer la civilización cuando está también en su mejor momento, cualquier cultura, cualquier civilización… Está claro que no se puede hacer un plan para hacer algo a no ser que se piense en ese plan. No se puede saber si un plan de acción es válido o no es válido a no ser que se

analice en detalle y se entienda la situación. A no ser que se comprenda cómo se comportan las instituciones humanas, y también a no ser que se comprenda cómo funcionan los seres humanos.

Los seres humanos siempre se han visto limitados por la falta de conocimiento. Imaginemos que mañana todo el mundo se queda sordo, mudo y ciego, que nadie puede comunicar ni transmitir sus conocimientos, ni tampoco aprender del pasado ni de los archivos escritos, ni transmitir sus conocimientos a sus hijos ni al futuro. Imaginemos esa situación extrema. Entonces las personas serían como conejos o como piedras. Pero también podemos imaginar otro escenario, donde la adquisición de conocimientos sería mucho más importante, y la educación mucho mejor que ahora, y la comunicación de mayor calidad y más honesta que ahora.

Pues bien, en este momento nos hallamos entre estos dos escenarios: entre la posición elevada y la de no ser más que simples piedras. Hace unos cinco mil años tal vez estábamos en un nivel muy bajo, ahora hemos subido un poco, pero aún nos queda mucho camino por recorrer para alcanzar, gracias a una educación y una información adecuadas, un nivel humano realmente superior.

Hablabas antes de transparencia. Un exministro socialista de Relaciones Exteriores francés, Hubert Védrine, dijo, criticando a WikiLeaks: «La transparencia absoluta es el totalitarismo». También se acusó a WikiLeaks de «violar la vida privada de los Estados». ¿Piensas que debe haber límites a la difusión de informaciones ocultas sobre los Estados?

Cuando los responsables políticos en los gobiernos se quejan del «exceso de transparencia», me da risa. Detrás de

esas acusaciones hay algo que es como decir: yo creo que las personas no deberían robarse unas a otras. Uno puede creer esto o no creerlo. Pero en realidad no importa, porque no somos perfectos, no somos dioses, y los Estados tampoco lo son. En la práctica, sabemos que los Estados no pueden regularse a sí mismos para evitar volverse «malos». En consecuencia, los Estados deben ser regulados por otras instancias, por personas que están dentro de ese Estado y por personas fuera del aparato de ese Estado. Esto es una evidencia.

Una institución que se regula a sí misma, que no tiene regulación externa, está condenada a cometer excesos o a la corrupción. Por eso, en términos prácticos, algunas instituciones del Estado, como la policía que investiga a las mafias, deben actuar de forma profesional para convencer a los ciudadanos de que sus investigaciones son fiables. Sin duda, WikiLeaks actúa de forma profesional y verifica que la identidad de nuestras fuentes no se vea comprometida o la identidad de nuestro equipo, de nuestro personal, nunca sea revelada. Y nunca lo ha sido. Pero mantener nuestros secretos no es la responsabilidad de toda la sociedad. De forma similar, no es porque la policía o las agencias de inteligencia actúen de forma incompetente que los editores de prensa o los ciudadanos deben censurarse unos a otros.

Dices que WikiLeaks le dio al mundo «una lección de periodismo», y que a los medios «habría que destruirlos todos» y sustituirlos. ¿No eres aquí también, un poco excesivo?

Yo he trabajado en los medios de comunicación como periodista, como editor, en competencia con otras publicaciones y como consumidor o lector, como todo el mundo.

Pero también tuve la experiencia de algo que poca gente ha experimentado, incluidos muy pocos periodistas, que es padecer a los medios de comunicación como sujeto. Los medios hablan de mí, y por lo tanto he desarrollado una percepción muy aguda respecto a su falta de profesionalidad, he comprobado que tienen muchos prejuicios y que están al servicio del poder dominante al que rinden cuentas. Aunque entre los periodistas que trabajan para los medios dominantes los hay muy buenos, las limitaciones institucionales son muy severas y casi inevitables. Esencialmente, el poder los corrompe.

Y cuando una organización mediática se convierte en influyente, incluso simplemente porque está haciendo bien su trabajo, se convierte en poderosa y como consecuencia, invita a otras personas a que trabajen para ella, y a su vez estas personas son invitadas por otros grupos sociales poderosos y acaban por encontrarse todos entre gente del mismo nivel social, del mismo nivel económico, para intercambiar información. Y este proceso es sencillamente un proceso de seducción social y de captación al que la mayoría de los seres humanos no se puede resistir. Resultado: todo grupo mediático que tiene influencia y que la ha ejercido durante muchos años ya no es capaz de dar la información de una forma honesta.

¿Qué relación tienes con Edward Snowden actualmente? Si no es un secreto…

No es un secreto el hecho de que WikiLeaks, yo y otras personas de WikiLeaks hemos conseguido sacar a Edward Snowden de Hong Kong para llevarlo a un lugar seguro. Tiene asilo en Rusia y ahora ha creado una organización

para defender las fuentes de los periodistas, que se llama Courage Foundation.[218] En cuanto a cómo nos comunicamos, de eso no puedo hablar. Pero es interesante el motivo por el que no puedo entrar en ello: es porque hay un Gran Jurado en los Estados Unidos investigando el caso de Snowden y los agentes del FBI vinculados a ese Gran Jurado estuvieron haciendo preguntas respecto al papel que yo, Sarah Harrison[219] y otros miembros de WikiLeaks tuvimos en el caso de Edward Snowden. Estamos muy orgullosos y muy contentos de que Snowden esté en un lugar seguro. Su familia ahora se ha reunido con él en Rusia. Y tiene libertad de movimiento en el país más grande del planeta. Posee documentación para viajar. Todavía tiene que tener mucho cuidado a la hora de salir fuera de Rusia, por los intentos de los Estados Unidos de capturarlo. Pero está bien. Y esto es un incentivo muy importante para que lanzadores de alertas como él den un paso al frente y hagan lo mismo.

Compartes con Snowden y con Manning el hecho de ser, a la vez, uno de los hombres más perseguidos por los Estados Unidos, y también el de ser considerado un héroe de nuestro tiempo[220] *por mucha gente.*

Sí. Ninguna buena acción queda impune. [risas].

---

218 http://www.couragefound.org.

219 Periodista británica especializada en investigaciones judiciales y asesora jurídica de Julian Assange.

220 Geoffrey de Lagasnerie, *L'Art de la révolte. Snowden, Assange, Manning,* Fayard, París, 2015.

¿Estás dispuesto a negociar con los Estados Unidos para poner fin a tu situación?

Respecto a los Estados Unidos hemos intentado negociar y mis abogados en Washington han negociado. El Departamento de Justicia estadounidense se niega a hablar con mis representantes. Y la última actualización por parte del Departamento de Justicia es que la investigación sobre mí sigue su curso, pero se niegan a decírmelo, se lo comunican al tribunal, pero no quieren hablar con nuestros abogados ni conmigo. Y el Gobierno de Ecuador, a nivel estatal, ha intentado hablar con el gobierno estadounidense respecto a esta cuestión y ahí también el Gobierno de los Estados Unidos se niega a entablar conversaciones.

En junio de 2014 anunciaste públicamente que pronto saldrías de la embajada de Ecuador.

No lo anuncié yo, fueron los medios de comunicación quienes lo anunciaron.

¡Ah! Otra prueba de las mentiras de los medios [risas]. *¿Cuándo piensas salir de aquí?*

Tengo confianza. La situación legal es absolutamente clara. Tenemos varios procesos en curso, hemos interpuesto una docena de demandas diferentes en distintas jurisdicciones que están avanzando. Sobre la mitad de ellas estamos a la ofensiva. Por ejemplo, presentamos una demanda penal contra las operaciones de inteligencia dirigidas a nosotros en Suecia, otra contra las operaciones militares de los Estados Unidos con igual fin en Alemania, otra en Dinamarca

contra la cooperación ilegal entre la inteligencia danesa y el FBI. He presentado también un recurso en Suecia y esperamos un resultado positivo.

Legalmente la situación está muy clara desde hace tiempo. Por otra parte a medida que avanza el tiempo, los Estados Unidos y el Reino Unido empiezan a tomar cierta distancia con respecto al tema WikiLeaks. Ahora, por ejemplo, están muy ocupados con la organización Estado Islámico. En el Reino Unido, además, están las elecciones del año que viene.[221] Y en Suecia hay un nuevo gobierno.

Socialdemócrata.[222]

Sí, pero no hay que olvidar que fue un gobierno socialdemócrata el que tomó la decisión de colaborar con la CIA en 2001.[223] En Suecia no hay mucha diferencia entre centroderecha y centroizquierda. La realidad es que, en Estocolmo, están actualmente en un periodo de transición. Y durante un periodo de transición la presión sobre el sistema judicial no es tan elevada porque el nuevo gobierno se está formando. En el Reino Unido tenemos varios grupos que están de mi parte, y esto tuvo como resultado un cambio en la ley. Hay que recordar que llevo aquí cuatro años bajo

221 Se trata de las elecciones legislativas del 7 de mayo de 2015. El Partido Conservador de David Cameron obtuvo la mayoría absoluta de la Cámara de los Comunes con 330 escaños de un total de 650.

222 Tras las elecciones del 14 de septiembre de 2014 en Suecia, se formó un nuevo gobierno el 14 de octubre de 2014, que es el resultado de una coalición formada por socialdemócratas y verdes, bajo la dirección del primer ministro Stefan Löfven (socialdemócrata).

223 En 2001, Suecia se vio salpicada por el escándalo de la tortura de dos ciudadanos egipcios en un vuelo secreto de la CIA que partió de El Cairo rumbo a Suecia en la época gobernada por una coalición dirigida por el primer ministro socialdemócrata Göran Persson.

vigilancia, sin pruebas. Y tampoco hay pruebas contra mí en los Estados Unidos, ni en Suecia. Esto resulta increíble. Yo mismo no llego a creer que esto pueda pasar, pero, sin embargo, es lo que me pasa a mí. Llevo detenido cuatro años sin pruebas e intentan extraditarme sin pruebas. Pero al menos ha habido un reconocimiento, por parte del Tribunal Supremo del Reino Unido, de que esto ha sido un abuso que no se podía evitar según la ley anterior. En consecuencia, el Parlamento ha modificado la ley. Y ahora ya no es posible una extradición sin pruebas en el Reino Unido.

¿Y tu situación está arreglada ahora?

No, hay un problema: esa nueva ley, evidentemente, no es retroactiva. Esa cláusula de no retroactividad se introdujo en la nueva ley después de que un artículo en el *London Independent* afirmara que, si se aprobaba la nueva ley tal y como estaba redactada, Assange quedaría libre. Probablemente no es legal, porque esa cláusula se ha introducido únicamente para causar perjuicio a una persona en concreto.

¿Una ley para una única persona?

Bueno, hicieron trampa, no pusieron mi nombre, pero describen mis circunstancias exactas.

[risas].

La llamarán la «Enmienda Assange», me imagino…

Mis abogados bromean. Dicen que es «la excepción Julian a la ley Assange». [risas]. Pero tengo confianza. Soy optimista.

II

ENTREVISTA CON NOAM CHOMSKY[224]

«El enemigo principal de cualquier gobierno
es su propio pueblo».

Noam Chomsky, considerado uno de los intelectuales más importantes de nuestro tiempo, nació en 1928 en Filadelfia, Estados Unidos. Es profesor emérito en el prestigioso Massachussets Institute of Technology (MIT). Sus trabajos en lingüística han transformado esta disciplina y han creado escuela en todo el mundo. Al mismo tiempo, Noam Chomsky reflexiona sobre la manera de construir una sociedad más justa, más autónoma y menos violenta. Ha desarrollado, por tanto, una intensa actividad crítica propia del intelectual comprometido, esencialmente en dos campos: la crítica del imperialismo en su expresión contemporánea y la crítica de los medios de comunicación como instrumentos de domesticación ideológica.

Con respecto al imperialismo, Chomsky cree que su deber como estadounidense es denunciar las guerras de su propio país. Sencillamente, porque para él es necesario

224 Versión abreviada de la entrevista con Noam Chomsky realizada para la televisión pública argentina, en Buenos Aires, el 13 de marzo de 2015, difundida íntegramente el sábado 21 de marzo de 2015.

comenzar siempre por criticar los actos del gobierno sobre el que se puede actuar, es decir, *en primer lugar*, el suyo.

En la entrevista, Chomsky habla ampliamente de esta cuestión, especialmente sobre la América Latina contemporánea y sobre las presiones ejercidas por Washington respecto a Venezuela y al anterior presidente, Hugo Chávez. También comenta la rivalidad actual con China.

En cuanto a los medios de comunicación y su ideología, una parte de la obra de Chomsky está consagrada al análisis de los mecanismos ideológicos de dominación y a los impactos de los poderes simbólicos en las sociedades occidentales. En su principal ensayo sobre estos temas, *Manufacturing Consent. The Political Economy of the Mass Media*,[225] que escribió junto a Edward S. Herman, profesor de la Wharton School de la Universidad de Pensilvania, aporta respuestas argumentadas a las siguientes preguntas: ¿Cómo se establece un «discurso de propaganda» en un Estado democrático? ¿Cómo se fabrica al «enemigo»? ¿Quién define los criterios de una «guerra justa»? ¿Por medio de qué procedimientos retóricos se hace que el pueblo acepte lo que va contra sus propios intereses? ¿Qué papel juegan los poderes públicos, las agencias de presión (*lobbies*), las grandes empresas privadas, la publicidad y las comunicaciones de masas en la construcción del consenso social?

En este sentido, en una entrevista con Daniel Mermet, Chomsky ha recordado que, en su opinión, la comunicación es el instrumento ordinario de gobierno de los regímenes democráticos. La comunicación sería a estos regímenes lo que la propaganda es a las dictaduras. Para poder controlar a sus poblaciones —dice Chomsky—, los propios regí-

225 Pantheon Books, Nueva York, 1988.

menes totalitarios tuvieron que recurrir a mecanismos de la comunicación publicitaria, perfeccionada en los Estados Unidos desde 1918.

Sin embargo —señala—, hay grandes diferencias entre el sistema de propaganda de un Estado totalitario y la manera de proceder en las sociedades democráticas. Exagerando un poco, en los países totalitarios el Estado decide la línea a seguir y todo el mundo tiene que conformarse con ello. Las sociedades democráticas actúan de otra manera. Nunca se enuncia la «línea» como tal, se sobreentiende. De alguna manera, se procede al «lavado de cerebro, en libertad. (…) En el fondo, es mucho más eficaz que los sistemas totalitarios».[226]

A la pregunta de si estimaba que su análisis sobre la «construcción del consenso» había envejecido tras el auge de Internet, la respuesta de Chomsky fue muy clara: «Nuestro análisis de base no ha cambiado. Es cierto que Internet ofrece oportunidades que antes no existían y en lugar de ir a la biblioteca ahora se puede acudir a Internet. Además, se puede publicar la información más fácilmente y existe la opción de diferentes distribuidores. Pero al final, el sistema no ha cambiado mucho».[227]

En lo que se refiere a la sociedad de vigilancia, Chomsky está en la misma onda que Julian Assange y Edward Snowden; en su opinión, las empresas privadas que dominan Internet nos vigilan tanto o más que las agencias de inteli-

---

226 Daniel Mermet, «Entretien avec Noam Chomsky», *Le Monde Diplomatique*, agosto de 2007. Ver también *Chomsky & Cie*, documental de Olivier Azam y Daniel Mermet, 2008.

227 Noam Chomsky, «Why Internet Hasn't Freed our mind. Propaganda Continues to Dominate», entrevista realizada por Seungyoon Lee, *Alternet*, 21 de mayo de 2015.

gencia del Estado: «Google y los demás gigantes de Internet ejercen una gran vigilancia para obtener nuestros datos personales, nuestras costumbres, nuestras interacciones, etc. Así pueden moldear la manera de presentar la información; y estas empresas nos vigilan mucho más que la NSA».[228]

Se suele decir que leer a Chomsky es un acto de autodefensa intelectual. Es verdad. Porque sabe hacer inteligentes a sus lectores, les abre los ojos y les hace tomar conciencia de la manipulación de la que son víctimas, muchas veces desde hace décadas.

La siguiente entrevista se hizo en Buenos Aires, Argentina, el 13 de marzo de 2015. Nos reunimos con Chomsky en ocasión del Encuentro Internacional «Por la emancipación y la igualdad»,[229] que reunió a personalidades procedentes de los Estados Unidos, América Latina y Europa.[230]

Noam, el 25 de noviembre de 2014 estuvo usted en Londres y visitó a Julian Assange en la embajada de Ecuador. Edward Snowden, por su parte, nos ha revelado la existencia de un enorme sistema secreto de vigilancia, ha puesto al descubierto el poder actual de los Estados en materia de espionaje a los ciudadanos. Assange y WikiLeaks por una parte, y por otra los lanzadores de alertas como Snowden, en los últimos tiempos nos han mostrado una nueva forma de hacer información, utili-

228 *Ibid.*

229 Organizado conjuntamente por el Ministerio de Cultura y el secretario de Estado de Coordinación Estratégica del Pensamiento Nacional, Ricardo Forster, el encuentro se celebró del 12 al 14 de marzo de 2015.

230 Entre ellos Martina Anderson, Leonardo Boff, Piedad Córdoba, Nidia Díaz, Íñigo Errejón, Álvaro García Linera, Marisa Matías, René Ramírez, Gabriela Ribadeneira, Emir Sader, Paco Ignacio Taibo II, Konstantino Tsoukalas, Camila Vallejo y Gianni Vattimo.

zando Internet. ¿Piensa usted que se va a desarrollar este nuevo género de periodismo en un futuro próximo, favoreciendo de esta forma la emancipación de los ciudadanos?

Igual que en la mayoría de las preguntas, la respuesta pertenece a los ciudadanos, a su acción. Sin ninguna duda, todos los sistemas de poder harán lo que puedan para impedirlo. Assange está refugiado en la embajada de Ecuador en Londres y el Reino Unido está gastando mucho dinero para que no se escape. Como sabe, las condiciones de vida de Assange son peores que si estuviera en prisión, pues en una cárcel puedes ver la luz del día, mientras que él no puede. Snowden está en Rusia y usted sabe lo que ocurrió con el avión de Evo Morales, el presidente de Bolivia, que volaba de Moscú hacia su país. Los países europeos —Francia, España y otros— interceptaron su vuelo por orden del Gran Amo en Washington. ¡Una cosa increíble![231] Finalmente, el avión tuvo que aterrizar en Austria. La policía inmediatamente subió para cerciorarse de que Snowden no estaba escondido en ningún sitio. Estas son, directamente, violaciones de protocolos diplomáticos internacionales, que muestran dos cosas: primero, el ensañamiento del Gobierno de Obama para castigar a Snowden; segundo, lo servil que es Europa con respecto al Gran Amo estadounidense.

Barack Obama va más allá en la represión que cualquier otro presidente estadounidense: él castiga a los lanzadores de alertas. En los Estados Unidos hay una ley de espionaje que se remonta a la Primera Guerra Mundial.

---

231 El 3 de julio de 2013, cuatro países europeos —Francia, Italia, España y Portugal— cerraron bruscamente su espacio aéreo para impedir el paso del avión presidencial de Evo Morales, presidente de Bolivia, cuando regresaba de Moscú, a causa de un rumor que hablaba de la presencia a bordo de Edward Snowden, refugiado en Moscú desde el 23 de junio y perseguido por los Estados Unidos por «espionaje».

Obama la ha usado para tratar de evitar la difusión pública de informaciones sobre la vigilancia generalizada reveladas por Snowden. El Gobierno va a hacer lo indecible para protegerse de su enemigo principal. Y el enemigo principal de cualquier gobierno es su propio pueblo. De la misma manera que las grandes empresas privadas van a tratar de proteger su control absoluto sobre muchos aspectos de la vida de la gente.

En lo que respecta a los lanzadores de alertas, su lucha por una información libre y transparente es una cosa casi natural. ¿Tendrán éxito? Eso depende de la gente. Si Snowden, Assange y otros hacen lo que hacen, lo hacen en calidad de ciudadanos. Están ayudando a la opinión pública a descubrir lo que hacen sus propios gobiernos. ¿Existe algo más noble para un ciudadano libre? ¡Y se le quiere castigar! Si los Estados Unidos pudieran echarles el guante, sería peor aún; hay otros (como Chelsea Manning) que ya han padecido el castigo. ¿Conseguirán estas persecuciones desanimar a los lanzadores de alertas? Esto dependerá de la respuesta de los ciudadanos.

Hay una crisis. Muchos periódicos están desapareciendo, muchos periodistas están perdiendo su empleo. ¿Piensa usted que sobrevivirá la prensa escrita? ¿Qué consecuencias podría tener esta desaparición?

No creo que sea inevitable. Hay algunas excepciones interesantes. Por ejemplo, en México. Creo que *La Jornada*[232] es ahora el segundo diario más difundido en el país; se lee mucho, aunque a los empresarios no les gusta nada, por lo que han retirado la publicidad; vive sin publicidad

232 *La Jornada* es un tabloide mexicano cuya línea editorial es de izquierda. Fue fundado en 1984 para hacer de contrapeso a los grandes periódicos dominantes: *Excelsior*, *El Universal* y *Reforma.*

de marcas, pero sí tiene publicidad del Gobierno, porque la ley mexicana exige que la «comunicación oficial» se reparta entre todos los diarios. *La Jornada* sobrevive, mucha gente lo lee; y aparentemente, por lo que yo he podido ver, es un diario de buena calidad y está sobreviviendo a la crisis. Y creo que no es algo imposible.

En la Declaración de los Derechos Humanos de la Organización de las Naciones Unidas (ONU), uno de los artículos, el 19, habla de la libertad de prensa.[233] Y dice que la libertad de prensa tiene dos aspectos: el derecho a generar una información libre del control gubernamental, pero también el derecho a recibir información y a tener la oportunidad de generar información libremente. Lo cual significa *sin concentración de capitales.* La prensa rica e independiente, del siglo XIX y principios del XX, sucumbió. Ha muerto por dos razones: una, la concentración de capitales que significaba la acumulación de capitales en la prensa comercial privada. Y dos, la dependencia de la publicidad. Cuando uno depende de la publicidad son los anunciantes los que tienen el poder en el periódico. Un diario moderno actual es un negocio y como cualquier otro negocio tiene que generar un producto destinado al mercado. El producto que fabrica un periódico son los lectores. Y su mercado son otras empresas que hacen publicidad. En la actualidad, un periódico vende publicidad a las empresas; lo mismo en televisión, pero esta no se paga cuando se enciende el televisor. La empresa canal de televisión vende sus telespectadores a los anunciantes. La parte creativa es la publicidad. En la

233 En efecto, el artículo 19 de la Declaración de los Derechos Humanos dice: «Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión».

industria de la televisión, la publicidad es el verdadero contenido. El resto es simplemente un relleno que la gente mira entre dos espacios publicitarios. Esa es la estructura básica de la televisión comercial.

En la jerga escrita de la prensa estadounidense hay un término: el *agujero* de las noticias. ¿De qué se trata? Primero se pone la publicidad, que es lo esencial y después se rellenan los agujeros que quedan, un poquito aquí y allá, con algo de noticias. Esa es la estructura natural de los medios comerciales.

Este tema ha sido una batalla durante siglos. Lo hemos visto en Argentina recientemente:[234] ¿acaso la libertad de prensa significa solamente la libertad de las empresas privadas de hacer lo que les da la gana? ¿O la libertad de prensa también tendría que comprender lo que dice la Declaración de las Naciones Unidas sobre los Derechos Humanos, o sea: el derecho de la gente a recibir información de *diversas fuentes*, y de tener la oportunidad de juntarse, generar y producir información a partir de estas?

Muchas veces nos preguntamos cómo ha podido transformarse la libertad de prensa en una tiranía de los propietarios de los medios de comunicación. Ha sido el resultado de una larga batalla comercial, que finalmente ha sido ganada por el sector privado. En los Estados Unidos hay una expresión que refleja esto: se habla de «Corporate libertarianism», pero no tiene nada de libertario, más bien se trata de la *tiranía de las empresas*. Así se debería llamar.

---

234 El gobierno argentino de Cristina Fernández llevó a votación, en 2009, una ley antitrust contra la excesiva concentración de la prensa. El poderoso grupo Clarín, que domina los medios de comunicación argentinos, cuestionó su legalidad, lo que provocó un largo pulso contra el poder. El Tribunal Constitucional acabó por dar la razón al Gobierno en 2013.

Su pregunta sobre los medios de comunicación impresos se sitúa en ese contexto. Podría haber medios impresos y con mucha vida, pero tiene que haber una ayuda pública. Y cuando hablo de ayuda, si el Gobierno es democrático, significa subvenciones públicas; significa que es el público el que participa, con sus impuestos, para garantizar un entorno mediático en el que el ciudadano pueda disponer de una información plural. Grupos de prensa independientes tendrían la oportunidad de elegir sus informaciones y ofrecer sus propios análisis, sus propias investigaciones, etc. Esa sería una versión necesaria de la libertad de prensa. No es imposible. Pero para esto, como para las demás formas de democratización, se necesita movilización ciudadana. Las empresas privadas van a hacer lo imposible para impedirlo. Eso se sabe bien en Argentina. Pero sucede en todos lados.

Hablemos de América Latina. En 1999 Hugo Chávez fue elegido presidente de Venezuela. Con posterioridad fueron elegidos varios presidentes progresistas: primero Lula en Brasil, luego en Bolivia Evo Morales, después en Ecuador Rafael Correa, en Argentina Néstor Kirchner, en Uruguay Tabaré Vázquez y Pepe Mujica. Esto se ha extendido por América Latina, que se ha separado un poco de los Estados Unidos. Yo quisiera preguntarle su opinión sobre estos gobiernos progresistas latinoamericanos y cuál piensa usted que es la razón de que los Estados Unidos haya podido llegar a esta situación de pérdida de influencia en América Latina.

Son acontecimientos de suma importancia en esta parte del mundo, todo lo que ha descrito usted tiene un alcance histórico. Si uno compara la América Latina de antes… Durante quinientos años, América Latina básicamente estuvo controlada por las potencias imperialistas occidenta-

les, sobre todo por los Estados Unidos en el siglo XX, pero antes hubo otros. Los pueblos originarios lationamericanos han sido controlados por una élite pequeña, generalmente blanca o casi blanca, muy rica, que dominaba a muchas personas pobres. Estas élites eran en cierta forma ajenas a su propio país: exportaban capital a Europa, por ejemplo, y enviaban a sus hijos a estudiar a los Estados Unidos. No les preocupaba su propio país. Y la interacción entre los países de América Latina era muy limitada. Cada país tenía su propia élite volcada hacia Occidente. Había ciertas diferencias, pero esta era en general la situación típica.

Y viene sucediendo desde hace quinientos años de una forma u otra.

Pero a partir de 1999 empezó a cambiar esta situación. Lo que usted ha descrito es un cambio muy significativo, es un punto de importancia histórica. Y los Estados Unidos son, por supuesto, la potencia que ejerce el mayor dominio en todo el mundo, pero ya no tiene el poder de destruir gobiernos y de imponer dictaduras militares cuando quieran. Si uno piensa, por ejemplo, en los últimos quince años, ha habido algunos golpes de Estado: un intento de golpe en Venezuela en 2002… bueno, funcionó, digamos durante apenas dos días. Los Estados Unidos apoyaron plenamente a los golpistas, pero no tuvo el poder de imponer a un nuevo gobierno. Hubo otro en Haití en 2004; los torturadores de Haití, Francia y los Estados Unidos organizaron el secuestro del presidente Aristide para enviarlo a África central. Fue exitoso, pero Haití es un país muy débil.

Hubo otro caso, el de Honduras, en 2009. Sí, sí, con Obama. Los militares se deshicieron del gobierno constitucional con una «excusa democrática». Y Washington no quiso calificarlo como un golpe de Estado. Pero los Estados

Unidos se encontraron aislados a escala internacional en su apoyo a ese golpe militar. Y ahora Honduras se encuentra en una situación desastrosa. La violación de los derechos humanos es allí una de las peores del mundo. Y en materia de emigración a los Estados Unidos —que es un tema importante— la mayoría de los inmigrantes proviene de Honduras, un país destruido por un golpe de Estado apoyado por Washington.

Y aunque algunos golpes de Estado han tenido éxito, las cosas ya no son como antes. América Latina ahora ha dado un paso hacia adelante para lograr cierto grado de independencia. Está en el buen camino. Organizaciones como Unasur,[235] Mercosur,[236] Celac[237] representan pasos importantes hacia la integración económica y política. La Celac es totalmente novedosa, porque los Estados Unidos y Canadá quedan excluidos, y esto nadie podría haberlo imaginado, era algo inconcebible años atrás. Este cambio se percibe también en otros ámbitos. Por ejemplo, la peor forma de tortura del mundo es cuando se arresta a alguien en secreto y se le envía clandestinamente a una dictadura militar aliada para que allí lo torturen con total impunidad. Los Estados Unidos lo vienen haciendo desde hace años (desde los atentados del 11 de septiembre de 2001).[238] En un informe reciente figura la lista de los países que han colaborado con Washington en esta siniestra actividad. Ahí están, por supuesto, los de Oriente Próximo: Assad en Siria, Mubarak en Egipto y Gadafi en Libia, ¿no? Y también la mayoría de los países europeos: Inglaterra, Suecia, Francia…

---

235 Unión de Naciones Suramericanas.

236 Mercado Común del Sur.

237 Comunidad de Estados Latinoamericanos y Caribeños.

238 Giulietto Chiesa, «L'archipel des prisons secrètes de la CIA», *Le Monde Diplomatique,* agosto de 2006.

Sin embargo, hubo una región en el mundo en la que no participó ningún país: América Latina. Y esto es muy importante. Cuando América Latina estaba bajo el control de los Estados Unidos era un centro global de tortura. Ahora, los países latinoamericanos se han negado a participar en estas atrocidades ideadas por los Estados Unidos. Esto es un cambio muy significativo, muy importante. América Latina está también en primera fila de la resistencia contra la globalización neoliberal. También ha habido otros éxitos, aunque todavía queda mucho camino por recorrer.

Usted conoció personalmente al presidente Hugo Chávez. Y él elogió algunos de sus libros. ¿Qué recuerdo tiene de él?

Tengo que confesarle que cuando el presidente Chávez mostró mi libro *Hegemonía o supervivencia*[239] en la Organización de las Naciones Unidas (ONU), las ventas se dispararon en Amazon. Dicho esto, conocí muy poco a Chávez; un encuentro con él en el palacio presidencial. Estuve en Caracas un día con un amigo y hablamos con Chávez sobre todo de cómo llegó al poder, cómo reaccionaron los Estados Unidos y otras cosas de esa naturaleza.

Chávez hizo un esfuerzo muy importante para tratar de introducir cambios sustanciales en las relaciones de Venezuela con el mundo. Uno de sus primeros éxitos fue lograr que la Organización de Países Exportadores de Petróleo (OPEP) redujese la producción para que los precios del barril aumentaran. Según lo que él me dijo, ese fue el momento en que los Estados Unidos se volvieron definitivamente contra él. Chávez hizo bien otras cosas: procuró petróleo a bajo precio a Cuba y a otros países pobres; reali-

239 *Hegemonía o supervivencia*, Ediciones B, 2005.

zó esfuerzos para mejorar el sistema de sanidad, reducir la pobreza; lanzó las misiones, que significaban un gran esfuerzo presupuestario en favor de los más necesitados, etcétera.

En esto obtuvo cierto éxito, pero se enfrentó a graves dificultades, en particular la incompetencia, la corrupción, la manera de combatir las huelgas, etc. El resultado final es un contexto difícil para Venezuela internamente. Y el problema más grave —que no se ha superado— y que es un problema de América Latina en general, es que todos estos países dependen de un modelo no sostenible de desarrollo económico, basado en la exportación de productos primarios. Un país no puede desarrollarse —Argentina y Brasil lo saben bien— sin una economía diversificada que pueda desarrollar una verdadera industria compleja. Si la actividad económica se limita a exportar productos agrícolas o mineros no es un modelo sostenible.

Si usted analiza los países que se han desarrollado, empezando por Inglaterra, los Estados Unidos y otros, todos, originalmente, empezaron exportando productos básicos. Por ejemplo, los Estados Unidos se desarrollaron porque tenían un casi monopolio en uno de los productos básicos más importantes del siglo XIX: el algodón, cultivado por esclavos encerrados en plantaciones, en campamentos que hubieran impresionado a los mismos nazis si estos los hubieran podido ver. Y así lograron los Estados Unidos aumentar la productividad del algodón más rápidamente que la industria, y eso que no tenía innovación técnica, excepto el látigo que usaban para torturar a los esclavos. Con el uso intensivo del látigo y de otros métodos espantosos, la producción de algodón se incrementó rápidamente, con lo cual los dueños de los esclavos se enriquecieron, por

supuesto, pero paralelamente se desarrollaron las fábricas textiles.

Si usted piensa, por ejemplo, en el noreste de los Estados Unidos, era una zona fabril donde estaban las principales fábricas de algodón, las fábricas textiles. Lo mismo sucedía en Inglaterra. Los ingleses importaban el algodón de los Estados Unidos y desarrollaron sus primeras fábricas textiles, lo cual también permitió la expansión del sistema financiero, pues hacían falta créditos y otras operaciones financieras. Y todo eso a partir del cultivo del algodón. Un sistema comercial, un sistema industrial, un sistema financiero. Ahora bien, los Estados Unidos, como otros países desarrollados, no respetaron lo que se llama hoy una «economía abierta». Se violaban los principios que hoy se proclaman, ya que había altos aranceles sobre las importaciones y otros mecanismos proteccionistas. Y eso siguió así hasta el año 1945, cuando los Estados Unidos pudieron desarrollar la producción industrial masiva de acero y de otros productos. Así es como se han desarrollado.

Si un país se autolimita a la exportación de productos primarios está abocado a la catástrofe. Y eso es lo que pasa en Venezuela. Su economía sigue dependiendo terriblemente de la exportación de petróleo. Es un modelo insostenible. Como es insostenible (en Brasil o en Argentina) una economía basada únicamente en la exportación de soja o de otros productos agrícolas. Hay que seguir un modelo de desarrollo similar al que han practicado Inglaterra, los Estados Unidos y algunos países europeos. Por ejemplo, Francia. El 20 % de la riqueza de Francia es producto del sufrimiento de los haitianos, que sigue hoy, lamentablemente. La historia del desarrollo en otros países coloniales repite el mismo modelo. Venezuela no ha superado este escollo. Y tiene

otros problemas internos graves que, por supuesto, Estados Unidos intenta exacerbar.

El 9 de marzo de 2015, Barack Obama firmó una orden ejecutiva decretando el estado de emergencia en los Estados Unidos por «la amenaza inusitada y extraordinaria» que representaría Venezuela para la seguridad nacional de su país.[240] *¿Qué piensa usted de esta declaración?*

Tenemos que ser cuidadosos y distinguir dos partes en esa declaración. Por un lado, hay un hecho real: las sanciones impuestas a siete funcionarios de Venezuela. La otra parte es un aspecto más bien técnico, la forma en que se formulan las leyes estadounidenses. Cuando un presidente impone una sanción debe invocar una fórmula ridícula que pretenda que haya «una amenaza para la seguridad nacional o para la existencia de los Estados Unidos». Es un aspecto técnico del derecho. Es tan ridículo que, de hecho, nadie lo había destacado. Pero esta vez algunas personas sí lo señalaron, porque apunta a América Latina. En la declaración habitual casi nunca se menciona toda esta retórica, y esta es la novena vez que Obama invoca una «amenaza para la seguridad nacional y para la supervivencia de los Estados Unidos», porque es el único mecanismo a su alcance que le permite imponer sanciones.

O sea, que lo que cuenta son las sanciones. El resto es una formalidad absurda; es una retórica obsoleta de la que podríamos prescindir, pero que, en todo caso, no significa nada. Aunque a veces sí. Por ejemplo, en 1985, el presi-

240 El 9 de marzo de 2015, el presidente Barack Obama firmó un decreto acusando a Venezuela de constituir «una amenaza para la seguridad de los Estados Unidos» e impuso sanciones a siete altos funcionarios venezolanos acusados de «violación de los derechos humanos».

dente Ronald Reagan invocó la misma ley diciendo: «Nicaragua es una amenaza para la seguridad nacional y para la supervivencia de los Estados Unidos». Pero en ese caso no era falso, porque ocurría en un momento en que el Tribunal Internacional de Justicia (TIJ) había ordenado a los Estados Unidos que pusieran fin a sus ataques contra la Nicaragua sandinista mediante los llamados contras. Washington no lo tomó en cuenta. Por su parte, el Consejo de Seguridad de las Naciones Unidas también adoptó, en ese momento, una resolución que pedía a «todos los Estados», que respetaran el derecho internacional. No mencionó a nadie en particular, pero todo el mundo sabía que se estaba refiriendo a los Estados Unidos.

El TIJ había pedido a los Estados Unidos que pusieran fin a sus actos de terrorismo internacional contra Nicaragua y que pagara compensaciones económicas importantes a Managua en concepto de reparaciones. Pero la reacción del Congreso estadounidense fue aumentar la ayuda a la oposiicón armada antisandinista. Es decir, la Administración de Reagan opuso su método a la resolución del TIJ. En ese contexto, Reagan se calzó sus botas de *cowboy* y declaró que Nicaragua era una «amenaza para la seguridad de los Estados Unidos». Recordará usted que, en aquel mismo momento, Reagan pronunció un célebre discurso diciendo que «los tanques de Nicaragua están a solo dos días de camino de cualquier ciudad de Texas». Y que había una «amenaza inminente». Bueno, según Reagan, aquella «amenaza», aunque absurda, era una realidad. Pero ahora lo de Obama es una fórmula retórica para dar a la declaración un carácter dramático adicional y tratar de socavar al gobierno de Venezuela. Algo que Washington hace casi siempre en este tipo de situaciones.

El 17 de diciembre de 2014, el presidente Barack Obama y Raúl Castro anunciaron la normalización de las relaciones entre Cuba y los Estados Unidos. Obama, en esa declaración, reconoció que cincuenta años de política estadounidense, de presiones, con bloqueo económico incluido, no habían producido ningún resultado, y que había que cambiar de política. ¿Qué piensa usted de esta normalización? Y ¿cómo ve usted la evolución de las relaciones entre La Habana y Washington?

Una pequeña corrección. No se trata de «normalización». Es un paso hacia lo que podría ser una normalización. Pero el embargo, las restricciones, la prohibición de viajar libremente de un país a otro, etc., no han desaparecido. Es un primer paso hacia la normalización y es sumamente interesante ver cuál es la retórica actual de Obama. Lo que dijo es que cincuenta años de esfuerzos «para llevar la democracia, la libertad y los derechos humanos a Cuba» han fracasado. Y que otros países, desgraciadamente, no apoyaron el esfuerzo de los Estados Unidos, lo que llevó a Washington a buscar otras formas de continuar sus esfuerzos por «imponer la democracia, la libertad y los derechos humanos». Más o menos esto es lo que dijo.

Quienes han leído *1984*, de George Orwell, saben que cuando un gobierno dice algo hay que traducirlo a un lenguaje más claro, que en general significa lo contrario. Lo que dijo Obama significa lo siguiente: «Durante cincuenta años hemos hecho contra Cuba un terrorismo de gran escala, una lucha económica sin piedad que ha acabado por aislar… a los Estados Unidos. En medio siglo no hemos conseguido derrocar al gobierno de Cuba. Y ¿qué tal si buscamos otra vía?». Esa es la traducción de su discurso, lo que realmente quiso decir.

Y vale la pena recordar que la mayoría de estas cuestiones se ocultan en los debates en los Estados Unidos y en Europa. Efectivamente, los Estados Unidos hicieron una campaña grave de terrorismo contra Cuba bajo la presidencia de John F. Kennedy, un terrorismo sin cuartel. Decenas de intentos de asesinar a Fidel Castro, ataques contra instalaciones petroquímicas, bombardeos de hoteles en los que sabían que había rusos alojados, ganado abatido, etc. Una campaña muy dura que duró muchos años.

Es más, después de que los Estados Unidos terminaran su terrorismo directo, se produjo el apoyo a los grupos terroristas con base en Miami en 1990. Además la guerra económica, que fue iniciada por Eisenhower, tomó realmente impulso durante la era Kennedy y se intensificó después. El pretexto de la guerra económica no era «establecer la democracia» ni «la introducción de derechos humanos», sino castigar a Cuba por ser un aliado del gran Satán que era la Unión Soviética.

Cuando colapsó la Unión Soviética en 1991, ¿qué pasó con el embargo? Se intensificó. Bill Clinton sobrepasó a George Bush padre endureciendo el bloqueo. Algo sorpredente por parte de un senador liberal de Nueva Jersey. Y más tarde se intensificó el esfuerzo por estrangular y destruir la economía cubana. Todo eso no tenía nada que ver ni con la democracia ni con los derechos humanos. Ni siquiera es una broma. Basta con ver en los archivos estadounidenses su apoyo a las dictaduras violentas y terroristas en América Latina. Washington no solamente las apoyó, sino que las impuso. Como en el caso de Argentina, donde los Estados Unidos fueron el más firme apoyo de la dictadura argentina (desde 1976 hasta 1983). Cuando el gobierno de Guatemala estaba cometiendo un verdadero genocidio (1982-1983),

Reagan quiso apoyarlo. Pero el Congreso le fijó algunos límites. Por eso dijo: «¿Qué tal si lo hacemos en Argentina? ¡Transformemos a los militares argentinos en neonazis para que hagan lo que nosotros queremos!». Desgraciadamente para él, Argentina pasó a ser una democracia después y ahí es donde los Estados Unidos perdieron el apoyo de Buenos Aires. Pero ya antes, desde principios de los años sesenta, se había desplegado sobre América Latina una gigantesca ola de represión: en Brasil, en Chile, en Uruguay, en América Central… Los Estados Unidos formaban y entrenaban directamente a los oficiales golpistas. Igual que hacen hoy. Por ejemplo, ya lo he dicho, Obama es el único dirigente que apoyó el golpe de Estado en Honduras [28 de junio de 2009], que derribó al gobierno constitucional [de Manuel Zelaya].

Hay que dejar a un lado las bellas palabras sobre la «democracia y los derechos humanos» que sirvieron de argumento para derrocar al presidente Zelaya. Palabras hipócritas, ya que desde hace tiempo todo el esfuerzo de Washington se dirigía a destruir ese gobierno democrático. Y sabemos por qué. Una de las cosas buenas de los Estados Unidos es que, en muchos sentidos, es una sociedad libre, y muchos informes y deliberaciones gubernamentales acaban siendo publicados. De manera que, al cabo de un tiempo, se puede saber exactamente lo que ocurrió y qué decisiones se tomaron al más alto nivel.

¿Piensa usted, como algunos analistas, que China será el gran rival estratégico de los Estados Unidos en el siglo XXI? ¿Qué consecuencias puede tener esto para el mundo en general y para el destino de los Estados Unidos?

China se desarrolla de una manera muy eficiente. Es algo que empezó en el año 1949, cuando se independizó. Hay una expresión para eso en el discurso estadounidense; se dice: «la pérdida de China». Es muy interesante: «la pérdida de China». No se puede perder algo que nunca se ha poseído. Pero en los Estados Unidos damos por sentado que nosotros somos los dueños del mundo y si algún país se aleja de nuestro lado, lo hemos «perdido».

China es hoy un productor *offshore* de las fábricas estadounidenses. Las principales empresas estadounidenses producen en China, importan de China. O sea, que las principales empresas de los Estados Unidos importan bienes baratos de China y obtienen ganancias extraordinarias. Una empresa estadounidense puede disponer allí de una mano de obra sumisa, muy barata, donde el Estado controla muy directamente a los trabajadores. No hay que preocuparse por la contaminación tampoco: es una forma muy inteligente de ganar dinero. Los vínculos comerciales, financieros e industriales entre los dos países son por tanto muy fuertes. Al mismo tiempo, China tiene las ambiciones normales de una superpotencia. Por ejemplo, China, si se fija usted en el mapa, está rodeada al este por una serie de protectorados estadounidenses que controlan sus aguas territoriales. Eso a China no le gusta. Los chinos se quieren expandir *offshore* por sus propias aguas. Entonces aparece un conflicto potencial bastante grave entre China, por un lado, y los Estados Unidos y Japón por el otro.

Y ese conflicto concierne al conjunto del Pacífico Occidental. Es una región donde Japón, durante su época imperial, tenía todas sus fuerzas. Y siguen controlando una buena parte, lo cual a China no le gusta.

En este momento, los cazas japoneses y chinos pasan continuamente sobre islas que no tienen ningún interés. Y ese estado de cosas en algún momento podría desembocar en una guerra. Lo mismo sucede entre los Estados Unidos y China. La política exterior de Obama mira hacia Asia; por eso envía fuerzas militares a Australia y hace construir una enorme base militar en una isla cercana a China. Nadie dice que es una base militar, pero seguramente lo es. Los Estados Unidos poseen, a pocos kilómetros de China, la base militar de Okinawa, cuya población se opone enérgicamente a ella. Pero los Estados Unidos quieren mantener bases en esa zona. Y se están construyendo otras nuevas, como he dicho, ante la mirada enojada de China, que ve todo esto como una amenaza. Y hay una confrontación potencial no solamente con los Estados Unidos, sino también con los países vecinos como Filipinas, Vietnam y Japón. Es un problema de tensiones. De manera subyacente hay también una tremenda interacción económica. Este será sin duda un tema importantísimo en los asuntos internacionales del futuro.

No obstante, se ha hablado mucho de la nueva potencia china en el siglo XXI. Creo que se exagera tremendamente. El crecimiento de China ha sido fuerte durante muchos años, pero sigue siendo un país sumamente pobre. Si se fija usted, por ejemplo, en el índice de desarrollo humano de la ONU, creo que China está en la posición noventa y no se mueve de ahí. Tiene graves problemas internos, movilizaciones de trabajadores que están rompiendo sus cadenas. Cada vez hay más huelgas, protestas, problemas ecológicos. Se habla de polución, pero es mucho peor: hay destrucción de los recursos agrícolas, ya muy limitados; se enfrenta a extraordinarios problemas que los Estados Unidos y Europa no tienen. Y sigue habiendo, repito, una enorme pobreza.

China no está a punto de transformarse en un poder hegemónico global.

Por otra parte, la presión de los Estados Unidos y Japón sobre China desde el Este está empujando a China hacia Asia Central. Uno de los desarrollos más importantes de los asuntos mundiales de los últimos tiempos es el establecimiento de lo que se llama la Organización de Cooperación de Shanghái (OCS), con base en China, pero que incluye a Rusia, a los Estados centrales asiáticos y a India e Irán como observadores. Se está desplazando también hacia Turquía y tal vez va a seguir expandiéndose hacia Europa, con lo cual se reconstituiría algo así como la ruta de la seda, que salía de China e iba hacia Europa.

A Washington no le gusta. Los Estados Unidos han pedido ser observadores en el seno de la OCS, pero se les ha negado. De hecho, la OCS ha pedido que se saquen todas las bases militares estadounidenses de Asia Central. Asia tiene grandes recursos; la confrontación actual de los Estados Unidos con Rusia está empujando al Kremlin a tener relaciones más estrechas con China, siendo China el poder dominante. Pero es un desarrollo natural. La parte oriental de Rusia tiene grandes recursos: minerales, petróleo, etc. Y eso podría permitir acercar aún más a China y Rusia. Uno puede ver una suerte de sistema eurasiano, con vínculos más estrechos. Por ejemplo, hoy se puede tomar un tren de alta velocidad desde China hasta Kazajistán. Esto forma parte del desarrollo que observamos y que es muy importante. Algunos estrategas han querido ver en esto una especie de OTAN cuyo cuartel general se encontraría en China. Es posible. Sea lo que sea, usted tiene razón: hay riesgos. Y potencialmente son peligrosos.

CONTENIDO

EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES
DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL
MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI –
EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES
DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL
MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI –
EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES
DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL
MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI –
EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES
DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL
MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI –
EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES
DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL
MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI –
EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES
DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL
MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI –
EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES
DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL
MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI –
EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES
DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL
MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI –
EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES
DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL
MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI –
EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES
DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL
MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI –
EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES
DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL
MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI –
EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES
DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL
MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI –
EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES
DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL
MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI –
EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES
DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL
MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI –
EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES
DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL MINCI – EDICIONES DEL

Ignacio Ramonet ★ El imperio de la vigilancia

Ediciones del Minci – Ediciones del Minci – Ediciones del Minci

Ya Michel Foucault en el siglo XX había previsto la mutación de las sociedades disciplinarias (que disponían del cuerpo y de su tiempo dentro de un espacio cerrado, bajo la mirada perpetua de un vigilante invisible) en unas sociedades de control mucho más sofisticadas.

La vigilancia como estrategia e instrumento del poder, desde el panóptico de Jeremy Bentham y a través de una prodigiosa revolución tecnológica, se erigiría en manos de los poderes, tanto estatales como fácticos, en el Big Brother cibernético capaz de una vigilancia total, aun en espacios abiertos y tiempos ilimitados. Es este nuevo régimen de panoptismo informático emergente en el siglo XXI el que Ignacio Ramonet, otrora alumno de Foucault, con su cabalidad, su perspicacia y su diafanidad características, retrata a través de su acelerada evolución durante las pasadas décadas, revelando minuciosamente las conexiones entre el imperio político-económico y el imperio de la vigilancia, el cual pretende garantizar una gobernanza universal y absoluta, a costa de la vida privada y los derechos individuales tan defendidos contradictoriamente por el liberalismo. El imperio de la vigilancia actual echa por tierra todo el culto de la vida privada y de la libertad individual preconizado por los grandes ideólogos del liberalismo histórico. Es la paradoja, o la hipocresía, de los actuales regímenes que a la sombra de unos grandes principios cada vez más confusos, invocando la libertad y la seguridad de los individuos, los convierten en los nuevos reos de una Big Data que incesantemente los ausculta y los registra.

ISBN: 978-980-227-465-9

9 789802 274659

Gobierno Bolivariano de Venezuela | Ministerio del Poder Popular para la Comunicación e Información

ediciones MinCI