

Reg Whitaker

El fin de la privacidad

Cómo la vigilancia total
se está convirtiendo
en realidad

Título original: *The End of Privacy*

Publicado en inglés, en 1999, por The New Press, Nueva York

Traducción de Luis Prat Clarós

Cubierta de Mario Eskenazi

Quedan rigurosamente prohibidas, sin la autorización escrita de los titulares del *copyright*, bajo las sanciones establecidas en las leyes, la reproducción total o parcial de esta obra por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares de ella mediante alquiler o préstamo públicos.

© 1999 by Reg Whitaker

© 1999 de la traducción, Luis Prat Clarós

© 1999 de todas las ediciones en castellano.

Ediciones Paidós Ibérica, S. A.,

Mariano Cubí, 92 - 08021 Barcelona

y Editorial Paidós, SAICF

Defensa, 599 - Buenos Aires

<http://www.paidos.com>.

ISBN: 84-493-0772-4

Depósito legal: B-42.253 / 1999

Impreso en A & M, S.L.

08130 Sta. Perpètua de Mogoda (Barcelona)

Impreso en España - Printed in Spain

Sumario

Introducción	9
1. El siglo de los servicios de inteligencia	15
2. El panóptico	45
3. El ciberespacio: la biblioteca de Babel	63
4. «La noche tiene mil ojos»: nuevas tecnologías de vigilancia	101
5. Las torres oscuras: bases de datos y alienación	151
6. El panóptico participatorio	171
7. El consultorio del Gran Hermano: el panóptico internacional	195
Índice analítico y de nombres	229

Introducción

Se dice a menudo, en el cambio de siglo, que vivimos en una nueva «economía de la información», que la «información es poder», y que la llave para el éxito nacional en la competencia global consiste en estar «en el umbral de la información»; se nos satura de celebraciones y de advertencias sobre una «revolución de la información» que se estaría expandiendo por todo el mundo: es prácticamente imposible, para cualquiera que esté al corriente de los medios de comunicación social, desconocer las «nuevas tecnologías de la información», a las que se considera responsables de reestructurar nuestro entorno político, económico, social y cultural.

Hay mucha exageración y alarmismo sobre las nuevas tecnologías y sus implicaciones, como en la mayoría de las especulaciones del fin del milenio sobre la vida en el siglo XXI. Aunque las predicciones drásticas y apresuradas del futuro no pueden ser dignas de

confianza, nos encontramos ante nuevas tecnologías y nuevos medios de comunicación que tienen profundas repercusiones, y sobre cuyas espectaculares consecuencias sólo podemos hacer conjeturas más o menos consistentes.

En tanto que científico especializado en el ámbito político, estoy especialmente interesado en la cuestión del poder: cómo se ejerce y por quién. Este libro se centra básicamente en el impacto de las nuevas tecnologías de la información sobre el poder político. Me siento especialmente interesado por un conjunto de teorías que observan la *vigilancia* como un mecanismo de poder. Marx analizó incisivamente las relaciones entre el poder económico y el poder político en la era del capitalismo, pero dejó sin cuestionar los mecanismos específicos, o tecnologías, del poder. Otra línea de pensamiento, ejemplificada en el trabajo reciente del filósofo francés Michel Foucault, ha resaltado la vigilancia y el uso estratégico de la información como instrumentos de control social. La metáfora del «Panopticon», que examino en el capítulo 2, es especialmente apropiada. En nuestra época, las líneas divisorias entre el Estado y la sociedad, o entre el sector público y la esfera privada, se diluyen cada vez más, y se dice que el Estado está en retirada. El concepto de panopticismo tiene la ventaja singular de no privilegiar el poder formal del Estado respecto a su ejercicio informal, al margen de las estructuras estatales. Este último poder es el que constituye el tema central de este libro.

Empiezo, en el capítulo 1, con una discusión sobre el papel de la información en el crecimiento del Estado a lo largo del siglo xx. Los servicios de inteligencia, es decir, la adquisición intencional de información secreta, han sido un instrumento importante del poder estatal tanto en tiempos de guerra como de paz. A raíz de ello, se ha desarrollado una de las metáforas centrales del poder en este siglo: el Estado orwelliano, en el que el control totalitario se basa en el monopolio de la información. Incluso las democracias liberales han intentado imitar algunas características de esta estructura del poder. Sin embargo, el modelo orwelliano es una guía radicalmente errónea para las estructuras del poder en el próximo siglo. Las nuevas tecnologías de la información nos desafían a reconstruir las nociones fundamentales del poder. El Estado se ha descentralizado y el poder es cada vez más disperso y difuminado. Esto no quiere decir que deje sentir su peso menos duramente sobre la gente, sino que sus orígenes

son ahora menos identificables, y sus efectos se perciben y experimentan de modo muy distinto.

En el capítulo 3, examinamos la naturaleza de las nuevas tecnologías de la información y algunas de sus consecuencias sociales. Existen fundadas razones para creer que tales tecnologías tienen la capacidad de cambiar drásticamente la concepción que tenemos de nosotros mismos y, en consecuencia, de modificar profundamente los conceptos de comunidad y de ciudadanía. Estos cambios pueden ser descritos como el advenimiento de la sociedad-red. Para poner de manifiesto esta evolución he prestado atención a menudo a la cultura popular, ya que, según creo, ha sido especialmente sensible a tales cambios y sugere sobre su impacto humano.

La capacidad técnica de la vigilancia, en la actualidad y en el futuro inmediato, ha superado ampliamente la de los Estados totalitarios del pasado reciente. En el capítulo 4 repaso algunas de las nuevas tecnologías de vigilancia, desarrolladas y empleadas en una miríada de modos de control social y en numerosos contextos cotidianos. Tales tecnologías son alarmantes en la medida en que pueden hacer transparente las vidas de la gente corriente.

En el capítulo siguiente prosigo con algunas consecuencias perturbadoras de las bases de datos y del poder que confiere a las empresas y los Estados la posesión de información detallada sobre los ciudadanos —a veces denominada «datavigilancia»—. La sociedad de la información se caracteriza como una nueva forma de alienación: los datos sobre perfiles sociales (*data profiles*) están ampliamente fuera de nuestro alcance, pero pueden oprimir y eclipsar nuestras vidas. Las empresas y las instituciones gubernamentales funcionan bajo el principio de gestión del riesgo, por lo que los datos sobre perfiles identifican a la gente como un buen o mal riesgo. Aquellos que quedan clasificados en la categoría de riesgo pueden llegar a ser excluidos de una plena participación en la economía y en la sociedad.

El capítulo 6 plantea un asunto espinoso: ¿por qué hay relativamente tan poca protesta social contra la invasión de nuestra intimidad por las nuevas tecnologías de la vigilancia y por el poder de la *vigilancia de datos*? Una respuesta posible a este interrogante es que las nuevas formas del poder panóptico son vistas a menudo bajo la perspectiva de las diversas recompensas que ofrecen, y no como agentes de penalización. Su adaptabilidad, por otro lado, puede fo-

mentar la fragmentación del público en una multitud de identidades «de consumo», en lugar de una ciudadanía democrática común.

El último capítulo examina el futuro, y se pregunta qué tipo de política puede desarrollarse a partir de la expansión internacional de las nuevas tecnologías de la información y de la constitución de la sociedad-red. Un modelo plausible es el del «feudalismo virtual». Rechazo este modelo, ya que no consigue explicar los numerosos efectos negativos del nuevo orden global, y desatiende la capacidad de las fuerzas democráticas para constituir redes de resistencia. También sugiero que la inestabilidad inherente al nuevo orden global impondrá un retorno limitado a los Estados en tanto que reguladores y garantizadores de los acuerdos establecidos.

Esta discusión lleva al libro a completar un círculo entero. Empezamos con el papel de los servicios de inteligencia, y concluimos con la colaboración entre los distintos servicios nacionales de seguridad e inteligencia para supervisar el nuevo orden internacional. Uno de los mayores efectos de la nueva vigilancia ha consistido en minimizar la pertinencia del modelo orwelliano del poder estatal centralizado: la introducción de las nuevas tecnologías de la información ha provocado el despido del Gran Hermano.* Irónicamente, la inestabilidad inherente al nuevo orden puede provocar el requerimiento, una vez más, de los servicios del Gran Hermano, aunque esta vez sólo sea como consultor periférico. El poder en un mundo reticulado será disperso y difuminado, pero continuará jugando un papel importante en el modo en que el mundo se organiza y se sostiene a sí mismo. Y, desde luego, según cómo se ejerza este poder, tendremos un mundo humano o inhumano. Tal alternativa dependerá en gran medida de la voluntad y de la determinación de las organizaciones y grupos democráticos que surjan de la nueva sociedad civil global con el propósito de inspeccionar, criticar, protestar y controlar los dispositivos del poder estatal, corporativo y empresarial.

No ofrezco ningún programa de acción para la oposición política, ya que sin duda sería presuntuoso por mi parte, así como prematuro. Lo que he intentado en este libro es trazar un esbozo de los parámetros cambiantes del poder bajo el impacto de una evolución tecnológica sostenida, y sugerir algunas de sus consecuencias.

* Gran Hermano (*Big Brother*): el brazo omnipotente del gobierno; término extraído de la novela 1984, de Georges Orwell. (*N. del t.*)

Una última aclaración respecto a lo que este libro no trata. El título remite al «fin de la intimidad». Las nuevas tecnologías de vigilancia hacen cada vez más transparentes a las personas, y reducen sin cesar los espacios privados en los que la gente, tradicionalmente, se retraía para refugiarse y para dedicarse a sí misma. Existen razones suficientes para preocuparse, y hay académicos, abogados y activistas que han desarrollado una línea de pensamiento sobre la protección de la intimidad mediante regulaciones y prevenciones legales. No analizo las diversas aproximaciones a la protección de la intimidad, ya que los distintos sistemas legales y las diversas culturas políticas de los países occidentales convertirían tal discusión en un complicado ejercicio de política comparada y jurisprudencia, para el que no hay espacio en este libro. Además, la difusión de las nuevas tecnologías de la información y de la vigilancia está transformando rápidamente la naturaleza de los desafíos a la protección de la intimidad, y en este libro me ha interesado más describir la naturaleza de estos desafíos que proponer acciones políticas y públicas específicas. Sólo pretendo exponer la magnitud de estos desafíos, que, sin lugar a dudas, es impresionante.

Quisiera agradecer la inestimable ayuda de las becas concedidas por el Izaak Walton Killam Trust y por el Consejo de Investigación en Ciencias Sociales y Humanidades de Canadá, así como el constante apoyo que me ha aportado mi propia institución: la Universidad de York.



1. El siglo de los servicios de inteligencia

A pesar de todo lo ocurrido a lo largo del último siglo, ple-
tórico de asombrosos descubrimientos científicos y técnicos, así
como de igualmente asombrosas brutalidades y atrocidades, el
siglo xx también ha sido el siglo de la inteligencia, una dimen-
sión especialmente intrigante sobre la que vamos a centrar nues-
tra atención. No nos referimos a la inteligencia, desde luego, sino
a los servicios de inteligencia: la adquisición intencional y sis-
temática de información, así como su clasificación, recuperación,
análisis, interpretación y protección. No es necesario mantener
oculta la temática que planteamos: estamos hablando de *espio-
naje*.

El espionaje es sin duda tan antiguo como la misma historia. Se-
gún el Antiguo Testamento: «Dios habló a Moisés y le dijo: "Envía
algunos hombres a espiar las tierras de Canaán, ya que voy a ofre-

cerlas a los hijos de Israel...».¹ Un antiguo consejero de la CIA, carente del imprimátur de Dios, ha descrito el espionaje como «la segunda profesión más antigua del mundo, y tan honorable como la primera».² Los secretos han existido desde siempre, y la gente siempre ha intentado desvelarlos. El espionaje —con sus máscaras repulsivas y sin embargo fascinantes, con sus engaños, traiciones y fidelidades— siempre ha tenido cierto atractivo, así como detractores. También conlleva privilegios, ya que los secretos robados han aportado a menudo poder y beneficios a sus nuevos propietarios.

Sin embargo, sólo en el siglo xx el espionaje se ha convertido en una actividad burocrática, organizada y sistemática, con sus tecnologías específicas, su base exclusiva de conocimientos científicos, y su propio papel, casi autónomo, en política nacional e internacional. Winston Churchill, por ejemplo, ha descrito la Segunda Guerra Mundial, el mayor conflicto bélico de la historia, como una «guerra de magos». Los «magos» de Churchill eran matemáticos, y otros científicos y catedráticos, entre los cuales estaban los inventores del concepto de ordenador, y todos ellos fueron reunidos en un local secreto de la Inglaterra rural llamado Bletchley Park, desde donde descifraron los códigos de comunicación usados por los militares alemanes. De este modo, Churchill y el búnker a sus órdenes en las calles de Londres pudieron saber qué iban a hacer los militares nazis, y cuándo lo llevarían a cabo. En Washington, otros «magos» descifraron los códigos japoneses, gracias a lo cual, en palabras del historiador militar John Keegan, en Midway («la batalla naval más importante de la [guerra]») «el conocimiento de las intenciones japonesas permitió a los norteamericanos situar su escueta flota transportadora de modo estratégico, con lo cual consiguieron vencer a las fuerzas enemigas, considerablemente más numerosas».³ Los servicios de inteligencia no hicieron ganar la guerra a los aliados, pero les ayudaron en gran medida, del mismo modo que los deficientes servicios de inteligencia del Eje aceleraron su derrota.

Con el Proyecto Manhattan y la trascendencia de las explosiones atómicas en Hiroshima y Nagasaki, en 1945, la importancia de los

1. Números 13.1-2.

2. Michael J. Barnett, citado en el frontispicio de Phillip Knightley, *The Second Oldest Profession: The Spy as Patriot, Bureaucrat, Fantast and Whore*, Londres, Pan Books, 1987.

3. John Keegan, *The Second World War*, Londres, Penguin, 1989, pág. 501.

servicios de inteligencia aumentó de forma espectacular, puesto que Norteamérica era la única en poseer el poder secreto de la fisión nuclear. La Unión Soviética dedicó amplios recursos científicos y materiales para alcanzar tales objetivos, pero también recurrió ampliamente al espionaje. En 1951, en el apogeo de la temprana Guerra Fría, mientras los norteamericanos luchaban contra los comunistas en Corea y el senador Joe McCarthy cazaba a los comunistas norteamericanos, el juez Irving Kaufman condenó a Julius y Ethel Rosenberg a morir en la silla eléctrica por «poner en manos de los rusos la bomba atómica». Su espionaje, según explicó el juez a los abogados defensores, «ya ha causado, en mi opinión, la agresión comunista en Corea, con un balance de víctimas que ya supera las 50.000, y quién sabe cuántos millones más de gente inocente pagarán el precio de su traición. Sin lugar a dudas, mediante su deslealtad, han alterado realmente el curso de la historia en perjuicio de nuestra patria».⁴ A pesar de las protestas internacionales, los Rosenberg, tal y como era de esperar, fueron ejecutados, dejando huérfanos a sus dos jóvenes hijos. Las contiendas entre los servicios de inteligencia ya habían alcanzado un cierto paroxismo.

Los Estados y la pasión por el saber

Es imposible separar el estatus contemporáneo de los servicios de inteligencia de dos características esenciales del siglo XX: por un lado, los impresionantes adelantos del conocimiento científico y de sus aplicaciones prácticas, especialmente en una tecnología militar cada vez más letal; por otro lado, un sistema internacional basado en los Estados-nación soberanos, el más poderoso de los cuales ha evolucionado hasta convertirse en una superpotencia militar. Tales Estados, al defender celosamente sus prerrogativas (o pretensiones) de agentes soberanos y autónomos, basaron la protección de su seguridad nacional en la fuerza militar, ya fuese por cuenta propia o mediante alianzas. La ciencia permitía fabricar un armamento que aumentaba considerablemente esta fuerza militar y, en consecuencia, la seguridad nacional, por lo que la adquisición de conocimiento se

4. Citado en Ronald Radosh y Joyce Milton, *The Rosenberg File: A Search for the Truth*, Nueva York, Holt Rinehart & Winston, 1983, pág. 284.

convirtió en una actividad estatal clave en más de un sentido. Los científicos, respaldados por las infraestructuras de investigación proporcionadas por el Estado, aprendieron los secretos de la naturaleza y aplicaron este conocimiento al desarrollo secreto de tecnología. Los Estados también consagraban sus recursos a la adquisición del conocimiento acumulado por otros Estados, ya fuese mediante intercambios voluntarios cuando era posible (o a través de las alianzas), o mediante una agresiva y entrometida recolección (espionaje), cuando era necesario.

Se ha señalado a menudo la perversión que todo ello conlleva para el libre desarrollo de la ciencia: los resultados de la investigación científica se transforman, mediante la alquimia de la Guerra Fría y de la actividad bélica en general, en secretos nacionales, almacenados en arsenales de la muerte estrechamente vigilados. La investigación y fabricación de las armas nucleares puso especialmente en evidencia esta perversión. El doctor Robert Oppenheimer, el máximo responsable de los aspectos científicos del Proyecto Manhattan, se debatió con los dilemas éticos planteados por el uso del poder que él mismo había ayudado a desencadenar, y, posteriormente, cuestionó el avance de la investigación en torno a la bomba de hidrógeno: en 1954, su autorización en materia reservada fue revocada. Pero los escrúpulos de Oppenheimer fueron mucho más contenidos que los de muchos otros científicos. Otros investigadores de la energía atómica, como Klaus Fuchs, Alan Nunn May y Bruno Pontecorvo, tomaron su propia iniciativa y pasaron información a la Unión Soviética, tanto antes como después de la Alianza en el periodo de guerra, por lo que plantearon otro tipo de dilemas éticos. El doctor Albert Einstein, cuyas tempranas innovaciones teóricas en la ciencia física fueron fundamentales para el desarrollo de la investigación nuclear, abogó en vano por la paz y la colaboración entre las naciones.

La ciencia había sido movilizadada con la pretensión de restablecer la seguridad en la guerra de todos contra todos, pero su uso sólo aumentó la inseguridad. Los servicios de inteligencia, cada vez más tecnificados, ofrecían la posibilidad de hurgar cada vez más agresivamente en los secretos más celosamente guardados del otro bando, al mismo tiempo que prometían, seductora pero engañosamente, proteger nuestros propios secretos. Una vez establecidos en esta carrera, los Estados se embarcaron en un círculo vicioso en el que per-

según una mayor seguridad pero sólo obtenían mayor inseguridad. En un siglo caracterizado por una verdadera eclosión de nuevas tecnologías de la comunicación, cualquier adelanto técnico exigía nuevas invenciones técnicas que permitiesen interceptar y leer lo que pretendía comunicarse: tras el teléfono y el telégrafo, vino la interceptación de las líneas telefónicas y telegráficas; tras la comunicación radiotelefónica, se hizo necesario desarrollar nuevas técnicas capaces de recoger las señales del «éter». Aunque las comunicaciones dirigidas a destinatarios autorizados sólo se codificaban para desconcertar a los posibles fisgones, así nació la ciencia de la encriptación. Los misiles sólo fueron el inicio de la tecnología espacial, y esta última permitió poner en órbita satélites de espionaje con el objetivo de descifrar las capacidades de los misiles enemigos, e identificar así sus bases de lanzamiento para ataques preventivos, pero también podían utilizarse para lanzar armas de destrucción masiva desde el espacio. Finalmente, la tecnología de la «Guerra de las Galaxias» garantizaba la seguridad ante cualquier ataque mediante una «bóveda» antimisiles de defensa virtual, situada en la estratosfera y controlada informáticamente. Afortunadamente para todos, el colapso de la Unión Soviética y el final de la Guerra Fría ralentizaron esta escalada desenfrenada.

La estrecha conexión entre ciencia, tecnología, poder militar y los servicios de inteligencia se ha resumido a menudo en la máxima «saber es poder», lo cual es erróneo en diversos sentidos. A lo largo de este siglo el poder ignorante ha aplastado numerosas veces al conocimiento desprovisto de poder, y los mismos investigadores se han visto a menudo oprimidos por los frutos de su propia labor intelectual. A pesar de todo, el dicho se ha hecho tan popular que parece caracterizar al siglo xx.

Podemos, sin embargo, corregir esta máxima para expresar con más precisión los matices de la era tecnológica: si los servicios de inteligencia, en tanto que organización estatal o actividad corporativa, difieren de la inteligencia en tanto que capacidad mental, también el «conocimiento» difiere de la «información». El conocimiento, en un sentido filosófico o religioso, tiene poco o nada que ver con la información, y el uso del conocimiento científico para aumentar el poder mediante el desarrollo tecnológico tampoco remite al conocimiento en su sentido clásico. Los servicios de inteligencia se centran en la adquisición intencional de información, es decir, en fragmentos de

conocimiento «útil», pero no en el conocimiento en sí mismo. El conocimiento se transforma en información, y ésta en «datos». Los datos, según la ciencia informática, remiten a la representación (sobre todo cuantitativa) de información, de tal modo que pueda ser procesada. Más generalmente, los datos son información organizada para su análisis científico o para su uso en la toma de decisiones y, sin duda, el control de este tipo de información puede dar lugar al auténtico poder.

La extraña pareja: el espía y el académico

Hay curiosos paralelismos entre el mundo del espionaje y el mundo académico: en algunos casos, ambos mundos colaboran de forma espectacular, como cuando el brillante matemático Alan Turing ayudó a romper los códigos alemanes en Bletchley.⁵ En Estados Unidos, los académicos de las universidades de la Liga Ivy colaboraron activamente con la Oficina de Servicios Estratégicos durante la guerra, así como con su sucesora, la CIA, en los primeros tiempos del periodo de paz.⁶ Se ha dicho a menudo que algunas de las mejores mentes de la Unión Soviética acabaron trabajando para la KGB o para las distintas agencias que la precedieron. No puede reducirse tal colaboración a una envidiosa atracción de los sosegados académicos por el misterioso mundo del espionaje, ya que tanto el mundo académico como los servicios de inteligencia comparten ambos, en cierto sentido, las mismas preocupaciones: la recopilación organizada y sistemática de información, así como su análisis e interpretación, con el objetivo de elaborar teorías que expliquen los hechos procesados. A lo largo de este siglo, tanto los servicios de inteligencia como las instituciones académicas se han especializado y compartimentado, y los diversos premios y recompensas a la investigación académica han promovido cada vez más lo cuantificable respecto a lo cualitativo, así como los datos/información respecto al conocimiento/saber. Tanto

5. Andrew Hodges, *Alan Turing: The Enigma*, Nueva York, Simon & Schuster, 1983.

6. Robin W. Winks, *Cloak & Gown: Scholars in the Secret War, 1939-1961*, Nueva York, William Morrow & Co., 1987; M. Katz, *Foreign Intelligence: Research and Analysis in the Office of Strategic Services, 1942-1945*, Cambridge, Massachusetts, Harvard University Press, 1989.

los analistas de los servicios de inteligencia como los académicos tienden a trabajar en contextos que estructuran e incluso limitan, en algunos casos, su capacidad para entender fenómenos cambiantes o disonantes de la realidad. Ambos pueden frustrarse a menudo al ver despreciados o ignorados sus consejos, tan razonados y fundados como poco conocidos, a favor de actuaciones que desafían abiertamente sus recomendaciones. El mundo de los servicios de inteligencia está repleto de «fracasos» flagrantes atribuibles a políticos obstinados, testarudos e ignorantes que no están dispuestos a escuchar lo que no les gusta, del mismo modo que en el ámbito público los políticos han rechazado tantas veces ideas académicas a favor de compromisos mediocres con el poder y la riqueza. Finalmente, tanto los espías como los académicos se encuentran a menudo en la situación incómoda, y peligrosa, de tener que decir la verdad al poder.

Tres distinciones fundamentales se mantienen, sin embargo, entre el espía y el académico. En primer lugar, la información que persiguen los servicios de inteligencia se mantiene deliberadamente en secreto, lo que conlleva una recopilación encubierta, por lo que los espías infringen generalmente la ley de los países en los que intervienen. Los investigadores académicos, por el contrario, trabajan por lo general con fuentes públicas de información. El espionaje se acerca así, regularmente, a la cara oscura de la naturaleza humana (mentiras, engaños, traiciones, etc.), lo cual puede constituir una patología de la vida académica, pero no es su rutina. En segundo lugar, los servicios de inteligencia remiten a un servicio creado, ordenado y utilizado por un único cliente, casi siempre el Estado, aunque recientemente también por distintas corporaciones o empresas privadas, mientras que los académicos intentan publicar sus descubrimientos con la máxima difusión posible. Si los científicos no consiguen llegar más allá de un pequeño grupo de iniciados, el problema proviene de sus complicadas temáticas así como de sus lenguajes especializados, pero no de coacciones exteriores. La tercera distinción es que los servicios de inteligencia se fundamentan en la hostilidad entre naciones, así como en una competencia que no sólo es endémica, sino potencialmente mortífera. La vida académica puede ser competitiva pero su ideal, al menos, se basa en la búsqueda pacífica y cooperativa del conocimiento.

Más allá de estas diferencias obvias, la afinidad que subyace entre ambas actividades es notable: su interés común en adquirir y acu-

mular información y datos en tanto que actividades esenciales para el control (de la naturaleza, de los individuos y de los Estados), ha forjado una relación que muchos consideran embarazosamente íntima. Esta relación ha sido especialmente beneficiosa para la tecnificación de los servicios de inteligencia, que han alcanzado unas capacidades cada vez más sofisticadas para percibir, escuchar y ver desde grandes distancias y a través de barreras defensivas primorosamente construidas —desde sonares submarinos hasta centros de escucha que exploran el éter, pasando por satélites de reconocimiento fotográfico en órbita por el espacio—. Tales adelantos, del mismo modo que el ordenador e Internet, son el resultado de un trabajo conjunto entre los servicios de inteligencia y la investigación científica bajo el auspicio militar. De hecho, la revolución de la información que se está extendiendo por todo el mundo a finales de este siglo debe su génesis, en gran medida, a esta extraña pareja del espía y el académico.

La jungla de los espejos

En el mundo hobbesiano de los servicios de inteligencia, la información se desdobra y ensombrece por su copia fantasmal, la contrainformación: los servicios de inteligencia se enfrentan a los servicios de contrainteligencia, y el espionaje se defiende del contraespionaje. Tal y como ha señalado Michel Howard en relación con los servicios de inteligencia militares:

Cualquier sorpresa se basa en su ocultación, y la «seguridad» es uno de los clásicos «principios de la guerra». Pero pocos comandantes inteligentes se han satisfecho nunca *escondiendo* simplemente sus intenciones o su fuerza, ya que si pretenden imponer su voluntad al enemigo (lo que constituye, en última instancia, el objetivo de cualquier operación militar) intentarán *engañarlo*, introduciendo información falsa en el bando enemigo para que actúe del modo más adecuado para facilitar sus planes [...] Deberá, por lo tanto, intentar acceder a las intenciones del comandante enemigo con el objetivo de evaluar su apreciación de las posiciones respectivas de cada bando, y entonces, mediante todos los recursos disponibles, hacerle creer una información que le llevará a actuar en conformidad con el plan de ataque realmente

previsto. No es suficiente persuadir al enemigo para que *piense* de un cierto modo, sino que es necesario persuadirle para que *haga* ciertos movimientos. El objetivo del engaño [...] consiste en alterar las acciones del adversario.⁷

Las confrontaciones entre servicios de inteligencia han dado lugar a algunos engaños espectaculares. Durante la Segunda Guerra Mundial, por ejemplo, los ingleses no sólo fueron capaces de interceptar todas las comunicaciones alemanas, sino que también consiguieron, mediante el ahora famoso sistema de «traición cómplice»,⁸ «convertir» virtualmente a todo espía alemán en un agente doble, algunas veces gracias a una red completa pero ficticia de comunicaciones. De este modo, lograron transmitir a los crédulos mandos del espionaje alemán sólo aquella información que el servicio de inteligencia inglés quería hacer llegar a los comandantes nazis. Hitler recibió así indicaciones totalmente fraudulentas sobre los planes aliados y sus intenciones, con resultados sorprendentes, como la movilización de toda la Wehrmacht a causa de tropas norteamericanas inexistentes en el Canal de la Mancha, en 1944.

Durante la larga Guerra Fría, ese «cuasiconflicto» al que Mary Kaldor apodó perspicazmente «Guerra Imaginaria»,⁹ la retorcida madeja de mentiras, contramentiras y contra-contramentiras que se estableció entre los mayores servicios de inteligencia del Este y del Oeste se hizo tan intrincada, que algunas mentes despejadas encargadas de desenredar sus mecanismos parecen haber perdido la cabeza por el camino. Así mismo acabó Jesus Angleton, el jefe de los servicios de contraespionaje de la CIA, cuya caza de dobles agentes soviéticos se volvió tan frenética, tan indisciplinada y tan totalizadora que la CIA tuvo finalmente que despedirlo, con la razonable asunción de que un topo soviético nunca sería tan perjudicial para la agencia y para la seguridad nacional como lo era la caza maníaca de topos llevada a cabo por Angleton.¹⁰ O la contrapartida inglesa de

7. Michel Howard, *Strategic Deception in the Second World War*, Londres, Pimlico, 1992, pág. ix.

8. J. C. Masterman, *The Double Cross System in the War of 1939 to 1945*, Yale University Press, 1972.

9. Mary Kaldor, *The Imaginary War: Understanding The East-West Conflict*, Oxford, Blackwell, 1990.

10. Tom Mangold, *Cold Warrior: James Jesus Angleton, the CIA Master Spy Hunter*, Londres, Simon & Schuster, 1991.

Angleton, Peter Wright, también despedido por propagar sospechas infundadas, y que se apodó orgulosamente a sí mismo, en sus memorias, «Cazador de espías».¹¹

¿Realmente era un desertor del otro lado del telón de acero, como aparentaba? ¿Se trataba de una trampa para propagar desinformación?... Una vez puestas en movimiento, las ruedas de la sospecha alimentaron una maquinaria infernal. Hay una metáfora muy elocuente que se ha usado a menudo para referirse a todo este complejo entramado: «la jungla de los espejos». La complejidad de esta espiral de sospechas y reflejos también puede ser señalada mediante los matices del término «desinformación»: desinformación no es lo mismo que información errónea o falsa, sino que remite a una información elaborada por expertos a partir de informaciones estratégicamente seleccionadas. La información genuina es el cebo que debe atraer a la presa para que se trague el anzuelo, pero éste debe esconderse cuidadosamente, y el cebo debe ser muy tentador, puesto que la presa es esencialmente recelosa y suspicaz. No se trata realmente de que cada contrincante desconozca las reglas no escritas del juego, sino que, por el contrario, cada uno de ellos posee sus propios cebos y sus propios anzuelos. Existe incluso la siniestra posibilidad de que, una vez el bando contrario se haya tragado el anzuelo y parezca atrapado, las apariencias se vuelvan engañosas: quizás, mientras uno intenta coger la presa, descubre que, en realidad, se ha cazado a sí mismo, mediante un engaño con una compleja y fatal vuelta de tuerca suplementaria.

En 1950, en la ciudad dividida de Berlín y en pleno auge de la Guerra Fría, el Oeste construyó un túnel bajo la zona comunista del Este para intervenir las comunicaciones soviéticas. El túnel se mantuvo operativo durante casi un año, a lo largo del cual se intervinieron más de medio millón de conversaciones, hasta que los soviéticos declararon públicamente haberlo descubierto y la operación se dio por terminada. Sin embargo, un agente soviético muy bien colocado en los servicios de inteligencia ingleses, George Blake, ya había advertido secretamente a la KGB sobre los planes del túnel antes incluso de que fuera construido. A pesar de ello, los soviéticos dejaron que el proyecto siguiera adelante con el fin de proteger y mantener a

11. Peter Wright, *Spycatcher: The Candid Autobiography of a Senior Intelligence Officer*. Toronto, Stoddard Publishing, 1987.

su traidor en las filas enemigas. Mientras el túnel estuvo operativo, la KGB transmitió sin duda mucha desinformación al Oeste para engañar y distraer, aunque también tuvo que dejar caer algunas migajas de información auténtica para poder convencer a los servicios de inteligencia occidentales de que la operación funcionaba correctamente. Según la mirada retrospectiva de diversos analistas occidentales, la cosecha fue abundante. Tal y como parece que ocurrió, la KGB no avisó al servicio de inteligencia paralelo y militar, la GRU (el verdadero objetivo de la operación desde el principio), de la existencia del túnel, ya fuera por una rivalidad entre agencias o a causa de una utilización errónea de la regla acerca de la «información que es necesario hacer saber». Incluso ahora, cuando al menos algunos de los dossiers de la CIA y de la KGB se han puesto a disposición de los investigadores, y cuando algunos participantes de ambos lados están dispuestos a recordar con más o menos libertad, se mantiene una ambigüedad irreductible sobre quién salió realmente victorioso de todo este turbio asunto, si es que puede hablarse de victoria.¹²

Una vez embarcados en este mundo de espejos, no hay escapatoria a la claustrofobia ni al sentimiento de traición, tan humano y necesariamente involucrado en la duplicación de mundos y personas de los servicios de inteligencia. La historia del espionaje está mancillada con los nombres de los grandes traidores: Kim Philby, Guy Burgess, Donald Maclean, John Cairncross, Georges Blake, Aldrich Ames. Hombres que vivieron una doble vida, sirviendo aparentemente a sus patrias respectivas pero sirviendo de hecho, clandestinamente, a los enemigos de su país. Hombres capaces de vender a sus amigos y a sus compañeros y, en algunos casos, de entregar a agentes u otras personas cuyas vidas dependían de su confianza, abandonándolos a su suerte: encarcelamiento, torturas o a la muerte. Sin duda asuntos escabrosos, aunque hayan generado una literatura que los convierte en fascinantes, como en las famosas obras de John Le Carré.

Parte de esta fascinación, más allá de la vinculada al lado oscuro de la naturaleza humana, deriva de las representaciones en espejo

12. David E. Murphy, Sergei A. Kondrashev y Georges Baley, *Battlefield Berlin: CIA vs. KGB in the Cold War*, New Haven, Yale University Press, 1997. Dos de los autores de este testimonio fueron destacados antagonistas de la guerra entre servicios de inteligencia en Berlín.

que he descrito más arriba. Nuestros traidores son los héroes del bando contrario, y viceversa. Siempre ha habido una cierta ambigüedad en el modo en que los desertores de los servicios de inteligencia del otro lado del telón de acero eran bienvenidos al mundo occidental. Por un lado, representaban victorias respecto del enemigo, especialmente si se mantenían en sus puestos como agentes dobles, haciendo estragos en los servicios de inteligencia rivales. Además, al escoger valientemente la libertad en lugar del totalitarismo, ponían en evidencia la superioridad moral de nuestra forma de vida. Sin embargo, siempre quedaba un cierto residuo de sospecha hacia aquellos que, en última instancia, habían *traicionado* a su país. También los topos occidentales para la URSS, al menos durante el periodo en que aún prevalecían los motivos ideológicos, reivindicaban una fidelidad superior a la de su país. Pero en los últimos años de la Guerra Fría, la avaricia y otros motivos innobles reemplazaron a la devoción hacia un ideal. Aunque tales ideales puedan parecer perversos para gente de otra ideología, no era lo mismo ser traicionado por Kim Philby, que se consideraba un soldado y entregaba toda su vida a la causa de la revolución del proletariado, que ser traicionado por Aldrich Ames, que recibió 1.8 millones de dólares de los tratan-tes rusos y se le prometió una suntuosa *dacha* rural para su jubilación. Pero la explotación de la debilidad humana, y desde luego el uso del chantaje como arma, especialmente cuando se basa en ese viejo recurso que es el sexo, siempre ha estado muy cerca de las raíces del espionaje, y también ha proporcionado a los relatos de espionaje algunos aspectos de esa depravada atmósfera de mezquindad y corrupción que siempre ha atraído tanto al lector de novelas policíacas. El espionaje es, repitémoslo, la «segunda profesión más antigua del mundo» y, en consecuencia, el marco ideal para los relatos que discurren con fascinación por el sexo, el engaño y la muerte, al tiempo que exponen oportunas lecciones morales.

La automatización de los servicios de inteligencia

Los elevados costes del espionaje, compartidos por todos las bandos y en todas partes, han contribuido sin duda a consolidar, a lo largo de la segunda mitad de este siglo, la tendencia a sustituir el trabajo humano de los espías para los servicios de inteligencia por

un trabajo automático. La interceptación de señales y comunicaciones, cuyas bases tecnológicas siguen evolucionando a un ritmo exponencial, ha dotado a la escucha humana de unas extensiones deslumbrantes. La mayoría de las comunicaciones auditivas pueden ser interceptadas por una serie de bases terrestres de escucha conectadas a una red local. Durante la Guerra Fría, los servicios de inteligencia occidentales dirigieron sus interceptaciones comunicativas al bloque del Este. Cuando el avión comercial coreano KAL-007 fue atacado y derribado en territorio soviético, en 1983, el gobierno norteamericano pudo proporcionar inmediatamente a los medios de comunicación una transcripción completa de la conversación entre el piloto soviético que lanzó los disparos fatales y la torre de control terrestre con la que estableció comunicación.¹³ Este tipo de interceptación es una rutina de los servicios de inteligencia, aunque su divulgación pública sea excepcional.

Durante el primer periodo de la Guerra Fría, el reconocimiento aéreo proporcionó imágenes de las instalaciones militares soviéticas de inestimable valor, pero se trataba de una técnica muy vulnerable a las represalias, tal y como ocurrió con el embarazoso derribo del avión norteamericano U-2, y la posterior captura de su piloto, el espía Francis Gary Powers, en 1960.¹⁴ El advenimiento de la era espacial, a finales de la década de los cincuenta, permitió disponer de vehículos más seguros para los «ojos celestes». Al principio, los satélites de espionaje, en órbita alrededor de la Tierra, producían imágenes que tenían que ser obtenidas y recuperadas, pero los modelos más recientes transmiten imágenes digitales en tiempo real. Las imágenes de alta resolución pueden distinguir objetos a ras del suelo tan pequeños como un pie, e incluso menos, y, además de su relativa invulnerabilidad a las medidas preventivas, una de las mayores ventajas de los satélites espías es su capacidad para obtener diferentes clases de imágenes, utilizando diferentes porciones del espectro electromagnético. La fotografía infrarroja y la infrarroja térmica, por ejemplo, pueden detectar elementos invisibles para el ojo humano. Las radiaciones térmicas señalan la presencia de instalaciones enterradas bajo tierra al detectar las diferencias térmicas en la superficie

13. Seymour M. Hersh, *«The Target is Destroyed»: What Really Happened to Flight 007 and What America Knew About It*, Nueva York, Random House, 1986.

14. Michel R. Beschloss, *Mayday: Eisenhower, Khrushchev and the U-2 Affair*, Nueva York, Harper & Row, 1986.

terrestre y, junto a las infrarrojas, pueden «ver» en la oscuridad. Las imágenes capturadas mediante radar pueden, por su parte, atravesar las barreras de nubes. En todos los casos, el tratamiento informático posterior puede analizar las imágenes y separar los datos importantes de los elementos irrelevantes.¹⁵ Los mayores inconvenientes del reconocimiento por satélite remiten a los elevados riesgos involucrados en el lanzamiento del satélite, cargado de material muy valioso (incluso actualmente prosiguen los despegues malogrados), así como a la inflexibilidad y limitación de las zonas-objetivo a causa de las órbitas prefijadas. Al finalizar la Guerra Fría, los servicios de inteligencia norteamericanos se encontraron con una inversión excesiva en satélites de espionaje orientados al bloque soviético, pero a principios del próximo siglo XXI, los servicios de inteligencia ya dispondrán de una nueva generación de satélites, mucho más pequeños y manejables, que podrán proveer ininterrumpidamente imágenes de cualquier conflicto local y específico en todo el mundo.¹⁶ En el periodo posterior a la Guerra Fría ha habido importantes presiones para que la poderosa capacidad de captación de imágenes de estos satélites sea puesta a disposición de los científicos y de la investigación sobre el entorno y el medio ambiente,¹⁷ así como para la explotación comercial, aspecto sobre el que volveremos en un capítulo posterior.

El almacenamiento técnico de información llevado a cabo por los servicios de inteligencia se extiende aún más lejos: monitores sensibles a los seísmos pueden registrar la más ligera contorsión de la corteza terrestre, y ofrecer con todo detalle la magnitud exacta de las pruebas subterráneas con armamento nuclear; la trayectoria de los submarinos es registrada a través de las profundidades silenciosas de los océanos. Todo este complejo hardware está al servicio de la cada vez mayor capacidad para almacenar datos, recuperarlos y procesarlos, del mismo modo que el desarrollo de un software extraordinariamente intrincado, capaz de separar las «señales» del «ruido»: por ejemplo, ciertas palabras clave o contraseñas basa-

15. William E. Burrows, *Deep Black: Space Espionage and National Security*, Nueva York, Random House, 1986.

16. Walter Pincus, «Smaller Spy Satellites May Give U.S. Stealth Capability Over Trouble Spots», *Washington Post*, 1 de febrero de 1998.

17. Jeffrey T. Richelson, «Scientist in Black», *Scientific American*, febrero de 1998, págs. 48-55.

das en el reconocimiento de la voz permiten recoger, selectivamente, pequeñas muestras de información útil de voluminosos e ilimitados almacenes que son, de hecho, sistemas de comunicaciones espaciales, circulando por el vacío interestelar y repletos de escombros informativos, pero cuya función remite a una central electrónica de escucha y captación furtiva; el software de lo que se llama inteligencia artificial (IA), por su parte, permite localizar movimientos de «blanqueo» financiero de entre la totalidad de las transacciones económicas que se efectúan en cualquier momento a una escala internacional, distinguiendo entre patrones normales y anormales en los flujos financieros.

Aunque la automatización de los servicios de inteligencia es mucho menos económica que su tradicional funcionamiento humano y exige grandes cantidades de capital, se ha ido consolidado lenta pero inexorablemente con relación al modelo tradicional. Además de ofrecer unas ventajas tecnológicas en constante expansión, la sustitución de los espías por máquinas también tiene otras ventajas: las máquinas no mienten, ni engañan, ni hacen trampas deliberada e intencionalmente, ni se emborrachan y desvelan todos sus secretos, ni se meten en situaciones comprometidas como compartir el lecho con parejas casi desconocidas. Cuando los secretos son obtenidos mediante exploraciones aéreas, marítimas y terrestres, en sustitución de las complicidades humanas basadas en traiciones, existen menos riesgos de provocar enredos políticos y, sin lugar a dudas, tanto la URSS como Estados Unidos descubrieron, gradualmente, que el panóptico extraterrestre de satélites de espionaje que exploraba incansablemente las capacidades nucleares del otro bando fue, de hecho, un factor de estabilidad en la confrontación entre ambas superpotencias. Al proclamar ambos bandos intenciones defensivas y pacíficas, el espionaje no hacía más que confirmar lo manifestado, o al menos hacía menos probable que cualquiera de las dos partes organizase en secreto un primer asalto. Sin embargo, si el propio servicio de inteligencia pasaba por alto unos topes humanos tan bien colocados, hubiese podido estallar un escándalo público de insondables pero catastróficas consecuencias: los Rosenberg fueron ejecutados por ayudar intencionalmente a la otra superpotencia a adquirir la capacidad nuclear que le permitía equilibrar la balanza del terror, evitando quizás una tercera guerra mundial. Mientras tanto, los satélites en órbita alrededor de la Tierra eran considerados los responsables del cli-

ma de confianza que desembocó, finalmente, en los acuerdos de reducción de armamento entre ambas superpotencias.

En el mundo de los servicios de inteligencia, se ha comparado a menudo los méritos de las HUMINT (fuentes humanas de inteligencia) respecto a las TECHNINT (inteligencia proporcionada por medios técnicos). A pesar de que esta última es excelente en aspectos como el despliegue de tropas o las comunicaciones entre oficiales, la tecnología actual tiene límites evidentes, y sin duda no será nunca capaz de penetrar en la mente de las personas con mayor responsabilidad para captar sus motivos e intenciones. Es especialmente revelador el hecho de que los servicios de inteligencia norteamericanos, a pesar de contar con el mayor y más sofisticado sistema de vigilancia tecnológica penetrando en todo el territorio comunista, fueron incapaces de anticipar el colapso del comunismo, la desintegración del bloque soviético y la disolución de la misma Unión Soviética. Por más inteligentes que sean las máquinas que usen en el futuro los servicios de inteligencia, siempre habrá personas que las programen, las dirijan y, en última instancia, empleen o desatiendan los resultados o servicios que permiten, según el caso de que se trate. El día en que las máquinas sustituyan totalmente a los humanos se mantiene estrictamente en el campo de la ciencia-ficción. Sin embargo, no cabe ninguna duda de que los servicios de inteligencia han incrementado notablemente el desarrollo de las tecnologías de la comunicación y de la información, y de que esta evolución ha transformado a su vez los servicios de inteligencia. En este sentido, la cuestión acerca de los méritos comparativos entre hombres y máquinas es una falsa alternativa: ambos han crecido juntos.

Vigilancia político-policial internacional

Los servicios de inteligencia se consideran prestigiosos o infames por actividades muy distintas a la simple recopilación de información con recursos encubiertos. Los norteamericanos, con toda su influencia a escala mundial, se dedicaron a una especie de actividad policial internacional encubierta: sus intervenciones en varios países del Tercer Mundo tomaron rumbos muy variados, desde desestabilizaciones planificadas clandestinamente, hasta asesinatos y golpes de Estado. Las habilidades y recursos especializados de los servicios

de inteligencia (sus métodos de propaganda y desinformación, de manipulación política y de colaboración militar con grupos rebeldes) se proponían conseguir cambios reales en diversos países, y no sólo recoger y acumular información reservada. Un caso clásico fue el de Guatemala, en 1954, cuando la CIA orquestó una especie de golpe de Estado mediante un engaño, un acontecimiento fabricado por los medios de comunicación que provocó la huida aterrorizada del presidente, y empujó al país a décadas de represión con regímenes militares. Aunque no todas sus acciones encubiertas tuvieron éxito (si «éxito» puede considerarse un término adecuado para estos casos), la CIA obtuvo la reputación de entrometerse en todos los rincones del mundo, sin duda una reputación muy desproporcionada con respecto a la verdadera capacidad dañina de esta agencia.

Las superpotencias se dejan tentar fácilmente por la posibilidad de emprender acciones encubiertas que mejoren sus intereses en política internacional. Por ello han desplegado y mantenido meticulosamente toda una red de agentes, contactos y otras fuentes humanas, con el objetivo de recopilar y acumular información reservada, lo cual ya constituye el primer paso para su uso posterior en posibles intervenciones que pretendan cambiar realmente el curso de los acontecimientos en otros países. Los expertos en organización y análisis de datos dentro de los servicios de inteligencia no siempre están de acuerdo con las decisiones que toman sus gobiernos, pero éstos suelen preferir resultados rápidos y concretos antes que proseguir con el análisis. Lo que siempre ha atraído más de las intervenciones de los servicios de inteligencia, en oposición a otras formas de actuar más directas y abiertas, es el hecho de que puedan efectuarse en secreto: si se fracasa, el Estado que la organiza puede evitar la deshonra de una derrota humillante. Así debía ser en teoría, pero en la práctica tanto la CIA como el gobierno norteamericano aprendieron, a su pesar, que los fracasos siempre conseguían de algún modo hacerse públicos. Pero ni las críticas, ni las controversias, ni siquiera el final de la Guerra Fría, nada ha conseguido eliminar la tentación de usar operaciones encubiertas al servicio de la política internacional, aunque las recriminaciones del Congreso y de los medios de comunicación, en la década de los setenta, consiguieron una prohibición formal del asesinato de líderes políticos extranjeros (magnicidios o atentados) en tanto que herramienta policial de la política exterior norteamericana.

La tecnología cada vez más sofisticada de los servicios de inteligencia también ha jugado un papel importante en la función policial norteamericana a escala internacional. Tras la Guerra Fría, el control de la proliferación de armamento de destrucción masiva dependía de la capacidad de los servicios de inteligencia norteamericanos (de su red de vigilancia tecnológica desplegada por mar, tierra, aire y en el espacio) para alertar a la «comunidad internacional» del desarrollo de armas nucleares, químicas o biológicas en los Estados considerados peligrosos, así como para controlar el cumplimiento de los acuerdos sobre armamento en los países que ya poseen algunas de estas armas, y, por último, para vigilar los movimientos de aquellos agentes no estatales considerados como un peligro real o potencial. Sin duda, las inspecciones e intervenciones humanas pueden ser necesarias para el cumplimiento de ciertas leyes, como pone en evidencia la guerra de desgaste entre Estados Unidos, las Naciones Unidas y el Iraq de Saddam Hussein, pero esta evidencia se predica sobre la base de una exploración internacional, con alta tecnología, de cada rincón y escondrijo del mundo.

Vigilancia político-policial nacional

La vigilancia político-policial a escala internacional sólo remite a un uso (o mal uso) de los servicios de inteligencia. Para millones de personas, ha sido mucho más importante su utilización para la seguridad interna: la represión de la disidencia y de los disidentes; el control de las clases turbulentas y peligrosas; la conformidad política compulsiva, y la penetrante y omnipresente vigilancia y regulación de la vida cotidiana. Por un lado, tenemos al Estado policial y totalitario, pero lo que existe del otro lado, no es una auténtica sociedad «libre», sino un Estado democrático y liberal que contiene elementos autoritarios y antiliberales. La seguridad nacional, o la *inseguridad* nacional, para ser más precisos, es una ansiedad que aflige a los Estados de todo el espectro político: gobiernos de todo tipo han recurrido a los servicios de inteligencia para establecer una vigilancia político-policial nacional y, en un momento u otro, también han empleado el secreto o la policía política para reprimir lo que consideraban un riesgo subversivo o revolucionario. La incidencia e intensidad de la represión han variado mucho, desde luego, y no

puede equipararse la caza de brujas de McCarthy en Estados Unidos, por más desagradable que fuese, con las terribles depredaciones del régimen estalinista de la misma época, del mismo modo que sería inapropiado igualar las esporádicas transgresiones del FBI en la época de J. Edgar Hoover con la rutinaria y sistemática intromisión de la Stasi en la Alemania del Este. Pero más allá de estas diferencias, que pueden apreciarse fácilmente en la vigilancia político-policial de los servicios de inteligencia del régimen gubernamental, lo que más llama la atención es la universalidad de este fenómeno a lo largo del siglo xx. Al estar disponibles diversos instrumentos de vigilancia y control, ningún Estado se ha resistido a la tentación de usarlos, y la mayoría ha intentado mejorarlos aún más. Los Estados con muchos enemigos internos y externos, reales o potenciales, han usado generalmente tales instrumentos de forma descuidada y brutal, mientras que los Estados con un mayor consenso nacional han tendido a refrenar su uso, empleándolos con mayor discreción y habilidad en aquellos momentos considerados de inseguridad nacional o estatal. Esta relativa discreción, sin embargo, sólo ha servido para encubrir los efectos negativos de la vigilancia político-policial secreta en la práctica de la democracia liberal.

La inseguridad internacional provoca generalmente miedo respecto a la seguridad nacional y al enemigo interior, ya que las patologías del contraespionaje, descritas más arriba, están íntimamente vinculadas a la percepción del enemigo interior en tanto que una insidiosa extensión del enemigo exterior: el quintacolumnista, el espía, el saboteador, el terrorista o el subversivo, dirigidos por el enemigo exterior, son imágenes que deben su aspecto amenazador y fascinante a la indistinción entre Interior y Exterior, entre Nosotros y Ellos. La típica imagen de la Guerra Fría de los «rojos debajo de la cama» refleja indeleblemente esta ansiedad. La xenofobia, la ideología y el pánico sexual y cultural se refuerzan entre ellos.

En los años anteriores a la Primera Guerra Mundial, con el horizonte nublado por grandes conflictos de poder, Inglaterra se vio invadida por el pánico al espionaje, alimentado por la prensa popular y por una nueva hornada de escritores que se estaban inventando, de hecho, la novela moderna de espionaje. Los malos de estas novelas eran agentes alemanes que intentaban minar el poder y la seguridad británicos; los héroes eran patriotas ingleses alertas al «vándalo alemán». El público inglés se sensibilizó al peligro del enemigo inte-

rior, definido por aquel entonces en términos claramente étnicos, y empezaron a circular espeluznantes reportajes de la bellaquería germana.¹⁸ El Estado británico, más influenciado por tales reportajes fantasiosos que por alguna evidencia concreta, concluyó que «existe un extenso sistema de espionaje alemán en nuestro país, y [...] no tenemos ninguna organización que pueda controlar ni determinar con precisión su extensión y sus objetivos».¹⁹ En consecuencia, Whitehall aprovechó la ocasión para crear el servicio secreto inglés, del que emergieron los servicios interior y exterior de inteligencia: MI6 y MI5. La línea divisoria entre realidad y fantasía en el mundo de los servicios de inteligencia fue borrosa desde el principio y, en cierto sentido, sigue siéndolo en la actualidad. No hace falta ni decirlo: en Alemania, por la misma época, se desarrollaron fobias similares al espionaje, con los roles invertidos pero resultados muy parecidos.

Al terminarse la guerra y desaparecer el «vándalo alemán», al menos por el momento, los jóvenes servicios de inteligencia dirigieron su atención a otro tipo de enemigo interior, más definido por la ideología que por rasgos étnicos. La revolución bolchevique de 1917 extendió un fantasma que obsesionaría los servicios de inteligencia occidentales durante la mayor parte de este siglo: el agente comunista, cuyos objetivos revolucionarios nacionales (suficientemente malos en sí mismos) se vinculaban de forma directa a la amenaza internacional de la Unión Soviética, lo cual doblaba los riesgos. Por su parte, los bolcheviques fueron pioneros en el uso indiscriminado de la policía secreta como arma principal para la consolidación y el mantenimiento del poder estatal, con un alarmante coste humano saldado en purgas, arrestos, torturas, gulags y asesinatos masivos. La Checa (comisión para combatir la contrarrevolución y el espionaje), que se convertiría posteriormente en la KGB, fundó lo que se ha llamado «Estado en tanto que servicio de contrainteligencia»,²⁰ en el cual no hay ninguna distinción entre la seguridad interna y las operaciones exteriores del servicio de inteligencia. El bolchevismo no tenía, sin embargo, el monopolio de las formas más policiales del

18. David Stafford, *The Silent Game: The Real World of Imaginary Spies*, Toronto, Lester & Orpen Dennys, 1988.

19. Christopher Andrew, *Secret Service: The Making of the British Intelligence Community*, Londres, Sceptre, 1986, pág. 100.

20. John J. Dziak, *Chekistry: A History of the KGB*, Lexington, Massachusetts, D.C. Heath & Co., 1988.

Estado, tal y como puso en evidencia la victoria nazi en Alemania, en 1933, con la Gestapo como brazo armado. Después del *Görterdämmerung* nazi de 1945, Alemania del Este combinó las tradiciones de la Checa y de la Gestapo en la Stasi, hasta finales de la década de los ochenta, con unos mecanismos de vigilancia que penetraban en cualquier rincón y escondrijo de la sociedad civil, convirtiéndose en informadores a amigos contra amigos, incluso a maridos contra sus mujeres.²¹ Quizás la Gestapo tuviese un coeficiente de brutalidad más elevado, pero en cuanto a la eficacia de la atención al detalle y de la minuciosidad, la Stasi fue superior: el porcentaje de habitantes por cada agente de la Gestapo era alrededor de 10.000; hacia finales de la década de los ochenta, la Stasi había alcanzado el notable porcentaje de 200. Sin embargo, ambos sistemas fueron incapaces de sobrevivir.

Por más repulsivo que sea el rostro de la represión totalitaria, no deberíamos ser ciegos a ciertas prácticas similares en las democracias liberales occidentales —ellas mismas Estados de inseguridad— aunque no hayan alcanzado nunca algo parecido a lo ocurrido en las pesadillas del Estado policial nazi o comunista. Las creencias comunes a todos los regímenes en cuestiones de seguridad interna pueden resumirse del siguiente modo: un enemigo exterior está empleando una quinta columna de agentes cuya fidelidad remite al Estado adversario, por lo que usarán armas como el espionaje, el terrorismo, el sabotaje, y toda clase de actividades encubiertas y dirigidas desde el extranjero, para beneficiar los intereses del enemigo y, en definitiva, la subversión, es decir, la socavación clandestina y desde dentro de la integridad y de la voluntad de la nación y de sus valores. Para combatir tales amenazas, el enemigo interior debe ser identificado y aislado, de modo que pueda evitarse su influencia (el objetivo ideal sería la extirpación inmediata, pero como mínimo deberá ser vigilada de cerca y contenida). Todo ello exige el desarrollo y el mantenimiento de una extensa y estrecha vigilancia a grupos e individuos sospechosos, así como la elaboración de largos informes y dossiers sobre actividades políticas sospechosas y sobre activistas (tales informes son acumulativos y pueden ser entrecruzados y comparados con otras bases de datos relativas a ciudadanos y asociaciones civi-

21. Timothy Garton Ash, *The File: A Personal History*, Nueva York, Random House, 1997.

les). El modo más efectivo de elaborar dichos informes es mediante las redes nacionales desplegadas por los servicios de inteligencia (agentes y fuentes de información), de forma parecida a las ya desarrolladas en el exterior por los mismos servicios; pueden emplearse métodos de vigilancia tanto humanos como tecnológicos, según los requerimientos específicos. Además, lo que debe identificarse es el riesgo, y no los hechos criminales en tanto que tales. Los mecanismos de seguridad operan al margen de las reglas del sistema legal e, idealmente, no deberían estar sujetos al control judicial, aunque, en caso de plantearse un juicio inevitable, debería poder delimitarse estrictamente. Tal inmunidad se basa en la premisa de que los servicios de seguridad deben proteger la identidad de sus informadores, su *modus operandi* y el contenido de sus archivos de cualquier divulgación pública, incluso respecto a otros sectores administrativos del Estado. De este modo, el dispositivo de seguridad se atribuye más o menos las funciones de un Estado secreto dentro del Estado. Los criterios específicos para establecer dónde radica el riesgo varían según el régimen y la época, pero siempre y en todas partes se trata de criterios claramente políticos que establecen líneas divisorias entre expresiones, opiniones o asociaciones legítimas o ilegítimas, conformes o peligrosas; más encubiertamente, también pueden señalar «debilidades» que hacen a una persona vulnerable al chantaje o a la manipulación de agentes hostiles, aunque generalmente tales «debilidades» también reflejan prejuicios políticos acerca de los rasgos del comportamiento, como la condena de la homosexualidad, la desaprobación de ciertos estilos de vida u otros aspectos del mismo orden.

Existen ciertas similitudes estructurales entre el FBI de Hoover y la KGB de Beria, por más diferentes que fueran en la práctica ambos regímenes políticos y su policía secreta. No se trata de establecer ecuaciones morales, lo cual sería inherentemente inapropiado, sino de constatar cómo regímenes tan radicalmente distintos en sus principios y su organización comparten, sin embargo, ciertas pautas estructurales que, al menos superficialmente, son muy similares. Las personas contra las que arremete el FBI pueden experimentar problemas en su carrera o verse incluso privados de su trabajo, así como verse incluidos en alguna lista negra; muy ocasionalmente, pueden terminar en la cárcel o atrapados en litigios judiciales. Las víctimas de la policía secreta soviética podían terminar mucho más fácil-

mente en el gulag e incluso muertas pero. tanto de un lado como de otro, los seres humanos se convierten en casos, archivos, abstractos perfiles de sí mismos más o menos caricaturizados, como unos dibujos animados burocráticos que destacan ciertos atributos, o supuestos atributos, y los exageran: *X se asoció una vez con Y, que se asoció con reconocidos trotskistas (comunistas); infectado por el trotskismo (comunismo); la actitud de X deberá ser reinterpretada como la de un (contra) revolucionario subversivo*. Cuando la máscara de los archivos empieza a sustituir a la persona real en el mundo real, las palabras y los actos que en circunstancias normales parecerían inocentes adquieren las más siniestras connotaciones y, además, pueden tener consecuencias reales para otras personas reales, más brutales en ciertos regímenes que en otros, pero en todos los casos basadas en la información recogida en los archivos de la policía secreta.

Los servicios de inteligencia del Estado liberal

Para apreciar mejor cómo ha funcionado y sigue funcionando este proceso en las democracias liberales, podemos abordar los mecanismos de seguridad basados en la ocultación de información. Inicialmente instaurados de forma manifiesta en tanto que medidas de contraespionaje, su propósito era reducir el riesgo que implica para el gobierno la contratación de funcionarios, que siempre pueden traicionar la confianza depositada en ellos. Pero los mecanismos de seguridad basados en la ocultación siempre y en todas partes han gozado de su propia vida y de su propio ímpetu, imponiendo complejas clasificaciones de seguridad de toda la información gubernamental interna y reservada y, por lo tanto, de los mismos funcionarios según su grado de acceso a dicha información clasificada. Tales mecanismos siempre han provocado el desarrollo de una burocracia-dentro-de-la-burocracia, cuyo objetivo es administrar los procesos de ocultación y protección de datos, con su propio saber hacer especializado y con técnicas específicas. Así mismo, se hizo necesario establecer una amplia gama de sanciones para todos aquellos que ponen en peligro esta información reservada, lo que conlleva, en las democracias liberales, la instauración de diversos procedimientos administrativos y judiciales. Sin embargo, a causa de la naturaleza de la evidencia o

de las pruebas (basadas en el riesgo y no en la culpabilidad), y a causa también del imperativo de los servicios de seguridad de proteger sus fuentes y métodos, los juicios consiguientes, privados de gran parte de la información y de los criterios que interpretan la evidencia, siempre resultan limitados y fraudulentos.

Un hecho que llama particularmente la atención en estos mecanismos de seguridad es que, a pesar de usar una tecnología considerada racional y objetiva para la identificación del riesgo, comparándose incluso con los chequeos médicos que actúan preventivamente para evitar, por ejemplo, el desarrollo de un virus, en la práctica, tales mecanismos de seguridad son radicalmente opuestos a los procedimientos científicos para identificar el riesgo. Desarrollados con el propósito de proteger al Estado de las ideologías hostiles, los criterios de ocultación son ellos mismos inevitablemente ideológicos. De ahí las devastadoras consecuencias del maccarthismo, que suponían una generalización del riesgo y, en consecuencia, de su identificación a lo largo de la Guerra Fría. Más alarmante aún ha sido la ampliación de tales criterios para incluir conductas consideradas indecorosas o detestables por las convenciones al uso: los criterios de «seguridad» se han usado para llevar a cabo purgas de homosexuales y lesbianas. Por si no fuera suficiente delimitar tales medidas de seguridad al cuerpo de funcionarios, los mecanismos se aplicaron también a todos los peticionarios de permisos de inmigración, residencia y nacionalidad, así como a los que pretendían obtener la condición de refugiados.

Dos hechos pueden ayudarnos a explicar la persistencia y la tenacidad de los mecanismos de seguridad, mecanismos que han sobrevivido fácilmente al fin de la Guerra Fría. En primer lugar, la protección de la información se considera necesaria sea cual sea la situación internacional. Los Estados contemporáneos tenían que encontrar métodos para adaptarse a las condiciones de una democracia de masas. En tiempos más remotos, los Estados podían recurrir a una elite reducida y compacta para contratar a sus empleados públicos en función de la confianza personal. En sociedades con una clara clase dominante, como Inglaterra, la tradición de recurrir a las clases altas educadas en Oxbridge para formar una clase administrativa de elite aún perduró bastante a lo largo de este siglo. Sin embargo, después del espantoso desamparo al que se vieron sometidas tanto la nación como las clases altas por el apodado anillo de espías de Cambridge

(Philby, Burgess, Maclean, Blunt y Cairncross), convertidos a la causa de la revolución proletaria, se hizo evidente que el antiguo método de reclutamiento ya no era el más adecuado: en 1950 se estableció la necesidad de poseer una «reconocida veteranía» para acceder a puestos importantes en el cuerpo de funcionarios. En la era de la democracia de masas, cada vez era más apremiante encontrar alternativas a los anticuados métodos de contratación basados en la confianza familiar o amistosa. Como era de esperar, la opción finalmente escogida consistió en una especie de mecanismo administrativo basado en categorías generales y universales que cualquier estudiante de la burocracia weberiana hubiese previsto. A pesar de todo, es difícil imaginar que se hubiese podido trazar un sistema más acorde con las idiosincrasias individuales, o más tolerante con las desviaciones de la norma política, para gestionar las inmensas e impersonales burocracias administrativas de las vastas democracias de masas.

En segundo lugar, la necesidad de establecer mecanismos de seguridad basados en la ocultación no surgió de la nada: el espionaje existía realmente: los Estados se espían entre ellos y tratan de protegerse del espionaje de sus rivales, razón por la cual nació el Estado de inseguridad nacional, con sus informes secretos y con sus bancos de datos que almacenan las creencias y las ideologías políticas de sus ciudadanos. El desarrollo de la vigilancia político-policial está íntimamente vinculado a los requerimientos del contraespionaje en los servicios de inteligencia.

Aunque no todas las víctimas de la protección contra espías y agentes subversivos eran inocentes, la acusación de «caza de brujas» lanzada contra el frenesí de los servicios de seguridad contiene una gran dosis de verdad. Muchas de las víctimas sólo eran culpables de hallarse en el bando erróneo de las cambiantes modas políticas, o de haber sostenido alguna vez opiniones que se convertían posteriormente en impopulares, o simplemente de haberse asociado o relacionado con gente inadecuada. Pero para los expertos en protección y ocultación de datos, la «inocencia» quedaba fuera de lugar, puesto que lo que estaba en juego era uno de los mayores desafíos del siglo xx: la identificación del riesgo estatal, y la consecuente necesidad de separar peligrosidad y seguridad a partir de toda la información almacenada por diversos métodos, de modo que se tuviera un Estado a salvo de riesgos innecesarios. Evidentemente, podían

cometerse errores, ciertas informaciones sobre particulares podían ser falsas, y la inocencia podía confundirse a veces con cualquier otra cosa, pero lo importante no era la culpabilidad legal de un individuo, sino simplemente el riesgo que implicaba desde un punto de vista estatal. Si existía alguna duda respecto a la confianza de una persona, se resolvía siempre en beneficio del Estado: un puesto de funcionario, una entrada de inmigración o una adquisición de nacionalidad se consideraban privilegios y no derechos, aunque, de todos modos, no había mucho o ningún interés en las personas en tanto que tales. Las personas eran *enrevesadas*, insondables en su complejidad e idiosincrasia para los burócratas encargados de tratar con una cantidad enorme de casos a partir de categorías universales. Los informes eran por lo tanto *limpios*, sencillos y útiles para los propósitos específicos que se les requería. A partir de sus fuentes de información, las fuerzas de seguridad recogían datos que, en muchos casos, por imperativos de seguridad, no podían ser confirmados mediante testimonios cruzados, por lo que dichos datos eran interpretados con criterios relativamente simples: si los sujetos parecían peligrosos, entonces *eran* peligrosos, por definición.

Owen Lattimore fue un prestigioso académico chino que ejerció la docencia en la universidad Johns Hopkins. En 1950, el senador Joe McCarthy le acusó de ser el principal espía soviético en Norteamérica. Esta grotesca acusación, respaldada en secreto por el FBI de Hoover, aceleró lo que Lattimore calificó posteriormente de «prueba por difamación», culminando en un caso de perjurio, aunque finalmente fuera liberado por falta total de pruebas. Al rememorar su propia historia, Lattimore señaló que el FBI y otros servicios del gobierno y del Congreso norteamericanos habían elaborado un informe sobre él que remitía a «un hombre que pudo haber existido».²² Esta afirmación expresa la esencia de las creaciones del Estado nacional de inseguridad: un mundo de datos que ensombrece, imita y caricaturiza el mundo real. En las democracias occidentales, en algún momento a mediados de este siglo, los perfiles de datos de las personas que hubiesen podido existir empezaron a eclipsar a las personas que existían realmente, una situación ya conocida en los

22. Owen Lattimore, *Ordeal by Slander*, Boston, Little Brown, 1950. Para un estudio más reciente de este caso, basado en documentos desclasificados del FBI, véase Robert P. Newman, *Owen Lattimore and the «Loss» of China*, Berkeley, University of California Press, 1992.

Estados totalitarios y policiales desde hacía algún tiempo. Los pioneros en el desarrollo de estos procesos fueron los servicios públicos y estatales pero, tal y como veremos más adelante, el sector privado ha intensificado este proceso, llevándolo mucho más lejos y transformando sutilmente su significación.

La ciudad de cristal: el Estado totalitario y los servicios de inteligencia

El siglo xx ha estado obsesionado por ideales utópicos que se convertían luego en pesadillas distópicas. La utopía revolucionaria conllevaba que la humanidad volviese a hacerse de nuevo a sí misma, trasladando un ideal democrático a la realidad material, y realizando una transformación ideológica de la sociedad, de la economía y de la cultura. La utopía contrarrevolucionaria, por su parte, conllevaba una purificación racial y el triunfo de la voluntad del *Volk*. La realidad de ambos proyectos ha consistido en el Estado totalitario, el estalinismo y el *Führer-prinzip*, el gulag y Auschwitz. Ahora, al terminarse este siglo, cuando vivimos entre las ruinas de revoluciones fracasadas y de ideales agriados, cuando los grandes relatos que inspiraron y aterrorizaron a las generaciones precedentes han perdido su gancho y balbucean en la incoherencia, el relato de la utopía que se convierte en distopía ya no provoca más que aislados encogimientos de hombros o suspiros tediosos, aunque, a pesar de todo, sigue alimentando profundamente nuestra comprensión de las relaciones entre el poder y el saber.

El Estado totalitario ha existido con formas concretas, en tanto que terrible realidad para aquellos que quedaron enterrados bajo su incansable maquinaria represiva. No obstante, existe más memorablemente en tanto que ideal, o pesadilla, es decir, en tanto que Estado totalitario ideal del que las realizaciones materiales efectivas sólo participan imperfectamente, del mismo modo que las formas geométricas platónicas se sitúan más allá de todas las formas geométricas reales, aunque éstas contengan algo de aquéllas. La Alemania nazi real era una realización imperfecta, a veces caótica, del Estado imaginado por Adolf Hitler, pero es la *idea* de tal maquinaria de la muerte lo que aún sigue poseyéndonos después del fin del régimen nazi y de sus líderes. La Rusia estalinista fue en la práctica un con-

glomerado de contradicciones, muchas de las cuales aún deben ser desenredadas por los historiadores, pero el *concepto* de un Estado inspirado por la idea de la revolución del proletariado —convertido en un monstruoso culto a la personalidad sin ningún tipo de respeto a la ley ni a los derechos humanos— continúa alimentando la imaginación, incluso después de que tal Estado se haya finalmente colapsado bajo el peso de su propia muerte.

Quizás esta disyuntiva entre ideal y realidad explique por qué ha sido en la imaginación literaria del mundo occidental donde el Estado totalitario se ha planteado más vívidamente. La obra *1984*, de Georges Orwell, es una exposición paradigmática de la distopía totalitaria, cuya estructura básica (un futuro totalitario en el que un Estado policial dirigido por un partido único refuerza su poder a costa de la humanidad de sus súbditos) ha provocado numerosas imitaciones en la cultura popular. La obra de Orwell, publicada al principio de la Guerra Fría, fue bienvenida por los medios de comunicación conservadores en tanto que útil advertencia a la civilización occidental sobre el riesgo comunista.²³ El mismo Orwell tomó prestada la estructura básica de *1984* de una destacada, aunque menos conocida, novela distópica soviética: *Nosotros*, de Eugene Zamiatin,²⁴ escrita en 1920, cuando la revolución bolchevique aún estaba en sus albores y la toma del poder por Stalin aún quedaba lejos. La obra de Zamiatin es más desafiadora que la de Orwell porque escribe a través de la perspectiva subjetiva de un grupo de personas «concienciadas» por la colectivización, que no aprueban ni entienden el individualismo. Pero lo más interesante de ambos escritores es la arquitectura del totalitarismo que describen, así como lo hondo que pudo calar en sus lectores.

En ambas novelas, el poder está centralizado en el partido único estatal, que aplasta cruelmente cualquier disidencia sin permitir la menor oposición. En ambas el poder es, en última instancia, personificado: el Estado Unido de Zamiatin está presidido por el «Bienhechor», y la Oceania de Orwell por el «Gran Hermano». El poder se

23. Georges Orwell, *1984*, Londres, Martin Secker & Wargurg, 1949. [Existen varias traducciones castellanas.]

24. Impublicable en la misma URSS a causa de la censura, *Nosotros* circuló en forma de *protozamizdat*. Fue publicado en inglés en 1924, y reimpresso de nuevo en 1952, quizás como un saludo al éxito de *1984*; Eugene Zamiatin, *We*, traducido al inglés por Gregory Zilboorg, Nueva York, E. P. Dutton & Co., 1924 y 1952 (trad. cast.: *Nosotros*, Barcelona, Tusquets, 1991).

mantiene mediante la *vigilancia*, constante y precisa, de todos los ciudadanos o unidades del colectivo («números», en la obra de Zamiatin). Nada de lo que nadie pueda hacer en cualquier lugar escapa al siempre atento ojo del Gran Hermano o del Bienhechor, mientras que los mensajes del partido y del líder invaden constantemente los medios de comunicación de masas; la comunicación es, por consiguiente, monodireccional, jerárquica, dominante y reguladora. Se forma y disciplina incesantemente a los ciudadanos, aunque tal dirigismo queda en su mayor parte oculto por la inmensa fábrica rutinaria e invisible de la vida cotidiana. La obra de Zamiatin ilustra este aspecto de forma impresionante mediante la arquitectura de las viviendas y de los lugares de trabajo: la ciudad del futuro es una *ciudad de cristal*, que hace transparente la vida de todo el mundo a todos los demás, con la excepción, desde luego, del Bienhechor y de los guardianes del Estado Unido: la ciudad de cristal, pero se trata de un cristal monodireccional.

Los Estados totalitarios reales nunca consiguieron perfeccionar el control del pensamiento, y eran totalmente ineptos para llevar a cabo el difícil y cotidiano ejercicio del poder mediante el consenso. En lugar de conservar el terror en tanto que último resorte, como en la «habitación 101» de Orwell, en donde la resistencia de Winston Smith es finalmente aplastada mediante el terror, utilizaron el terror y la violencia como primer resorte y se mancharon de los pies a la cabeza con la sangre de sus víctimas. En vez de ser unos diabólicos y astutos ingenieros del consenso, sólo fueron unos verdugos torpes. Sin embargo, la imagen del Estado totalitario «ideal» se mantiene viva y convincentemente en nuestra imaginación, seguramente porque es una oscura parábola de lo que suponemos que es el poder. Es conveniente detenerse un poco más en esta parábola, en tanto que constituye un signo indicador del lugar en el que hemos estado a lo largo de este siglo.

La visión totalitaria es convincente porque representa el esqueleto arquitectónico del poder moderno. Hemos entendido y representado el poder como una amalgama de fuerza y de autoridad ejercidas jerárquicamente de arriba abajo, centrado espacialmente en un lugar en el que se concentra todo el dominio y el mando, y que tiene a las personas y a la sociedad civil como súbditos, pero también como instrumentos. En la medida en que los Estados democráticos liberales han imitado ciertos aspectos de esta visión totalitaria —al

establecer y reforzar la policía secreta y los servicios nacionales de inteligencia, a pesar del impedimento que pudiesen suponer las constricciones constitucionales y los derechos humanos; al intentar controlar, o por lo menos gestionar, información en interés de la seguridad del Estado; y al movilizar el saber en interés del poder—, también podemos ver aspectos de nosotros mismos en la visión totalitaria, y no sólo de nuestros enemigos. Para resguardar a la sociedad libre de sus antagonistas, J. Edgar Hoover aspiró a un poder cuasi-totalitario, de lo que deriva la peculiar mezcla de miedo y servil deferencia que inspiró a lo largo de su vida, sustituidos luego, cuando ya reposaba definitivamente en su tumba, por la repugnancia y la repulsa.

Esta horripilante representación del poder, con gran capacidad de espetar la imaginación política, ha obsesionado y dominado el siglo xx, *pero se trata de una representación casi sin lugar a dudas equivocada*. Ya no encaja con las realidades del mundo a finales del siglo xx: los profundos cambios tecnológicos, económicos y culturales (algunos, pero de ningún modo todos, pueden ser reunidos bajo el paraguas de la denominada revolución de la información) han convertido tal representación en radicalmente engañosa. Necesitamos nuevas representaciones del poder que reflejen más rigurosamente el mundo contemporáneo. En los siguientes capítulos, intentaré entender y explicar algunos de estos cambios, y señalar cómo pueden empezar a considerarse el principio de una representación más rigurosa del poder. En el sentido más general, y como simple apunte, lo que estoy describiendo es la transición desde el *Estado de vigilancia* a la *sociedad de vigilancia*. No se trata de una distinción meramente formal: la sociedad de vigilancia implica un entramado muy diferente del poder, y su impacto en la autoridad, en la cultura, en la sociedad y en la política es muy distinto al del poder centralizado que tenía el Estado de vigilancia de nuestro pasado inmediato.

2. El panóptico

En cualquier discusión sobre la capacidad y organización de los servicios de inteligencia, tanto en objetivos internos como externos, la vigilancia es un concepto clave. Pero, ¿qué implica exactamente la vigilancia?, y ¿para qué objetivos se ha empleado? Según Christopher Dandeker, uno de los teóricos más eminentes sobre la cuestión:

El ejercicio de la vigilancia conlleva una o más de las siguientes actividades: *a)* la recopilación y almacenamiento de información (presumiblemente útil) sobre personas y objetos; *b)* la supervisión de las actividades de personas o entidades mediante instrucciones, o mediante el diseño físico de los entornos naturales o artificiales. En este contexto, la arquitectura puede facilitar de modo importante la supervisión de las personas, como por ejemplo en las cárceles o en los diseños ur-

banísticos: c) la utilización de toda la información almacenada para controlar el comportamiento de las personas bajo supervisión y, en el caso de personas con obligaciones penales o de otro tipo, su obediencia respecto a las instrucciones emitidas.¹

El panóptico

La imagen del panóptico impregna todas las discusiones contemporáneas sobre la vigilancia. Tanto el término como la idea fueron introducidos en 1787 por el filósofo utilitarista inglés Jeremy Bentham.² El término ha sido retomado por el filósofo francés Michel Foucault en su obra tardía, hacia 1970,³ y sigue siendo un concepto de enorme influencia. En 1990, Oscar H. Gandy Jr. emprendió su monumental investigación sobre las implicaciones de las últimas tecnologías de la información para una «economía política de la información personal», y el título de su libro fue *The Panoptic Sort*.⁴

El panóptico fue de hecho propuesto por Bentham como un diseño arquitectónico para las prisiones. Se trata de una idea sencilla: una prisión construida de forma circular, cuyo perímetro periférico en cada uno de los niveles consiste en celdas individuales que albergan a un solo prisionero, totalmente aislado de los otros reos, a los que no puede ver ni escuchar. Todas las celdas son visibles a la observación del inspector, instalado en una oficina central desde la que puede controlar perfectamente a cada uno de los prisioneros. Mediante un sistema de aperturas y tubos de comunicación demasiado complicado para ser descrito aquí (y seguramente, en la práctica, para que pudiese construirse efectivamente) todos los prisioneros son conscientes del escrutinio potencial del inspector en cualquier

1. Christopher Dandeker, *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day*, Nueva York, St. Martin's Press, 1990, pág. 37.

2. Jeremy Bentham, *The Panopticon Writings*, editado por Miran Božovič, Londres, Verso, 1995 (trad. cast.: *El panóptico*, Madrid, Endymion, 1989).

3. Michel Foucault, *Surveiller et punir: naissance de la prison*, París, Gallimard, 1975. Trad. inglesa: *Discipline and Punish: The Birth of Prison*, Nueva York, Pantheon, 1978. Trad. cast.: *Vigilar y castigar: nacimiento de la prisión*, Madrid, Siglo XXI, 1998.

4. Oscar H. Gandy, Jr., *The Panoptic Sort: A Political Economy of Personal Information*, Boulder, Colorado, Westview Press, 1993.

momento del día o de la noche (la luz inunda las celdas de forma natural durante el día y artificialmente por la noche). Los reos reciben de vez en cuando instrucciones personalizadas del inspector a través de los «tubos de comunicación», que individualizan los mensajes de modo que ningún otro reo pueda escucharlos. Aunque el inspector pueda ver permanentemente a los prisioneros, éstos no pueden ver el rostro ni los ojos de aquél, ya que, mediante otro complicado sistema de linternas y aperturas, su figura es una silueta opaca que, a pesar de recordarles constantemente su presencia, se mantiene como una «figura completamente negra» cuyos rasgos son indescifrables.

El panóptico es una especie de teatro cuya representación consiste en «la ilusión de una vigilancia permanente: los prisioneros no están realmente bajo una vigilancia constante, simplemente piensan o imaginan que lo están».⁵ El objetivo es la *disciplina* o el *adiestramiento*: mientras los prisioneros temen que pueden ser constantemente observados y que se les puede aplicar castigos por cualquier transgresión, interiorizarán las reglas y, de este modo, las penas reales se harán superfluas. En otro sentido, todo el panóptico es en sí mismo un espectáculo teatral en beneficio del público, de personas invitadas para observar (Bentham creía firmemente en el valor ejemplar de la publicidad). La reeducación o reinserción de los presos es casi de interés secundario, puesto que el propósito fundamental consiste en una reforma moral de la sociedad mediante el edificante espectáculo de la disciplina controlada por la vigilancia. Bentham consideraba que el principio del panóptico podía ser aplicado a otras instituciones sociales, como los asilos, los hospitales, las escuelas y los lugares de trabajo.

Tal diseño no ha sido realizado nunca, ni durante la vida de Bentham ni desde entonces. Sin embargo, es una metáfora insuperable del poder de la vigilancia en el mundo contemporáneo. Para Foucault, la idea de Bentham consistía en una «tecnología política» que induce al sujeto a «un estado de conciencia y visibilidad permanente que aseguran el funcionamiento automático del poder».⁶ El Estado totalitario e imaginario de 1984 ha supuesto, para la imaginación política, la plasmación del esqueleto arquitectónico del poder del Estado. El panóptico imaginario también consigue plasmar el trabajo

5. Bentham, *op. cit.*, pág. 16.

6. Foucault, *op. cit.* págs. 207 y 201; las referencias remiten a la versión inglesa.

silencioso e invisible de las técnicas del poder interiorizado, ejercidas sin la presencia directa de coerciones.

Como era de esperar, Bentham no se consideraba un reaccionario en la reivindicación de su concepto. El hombre al que Marx describió como «un *archifilisteo*, ese insípido y pedante oráculo, azote aterciopelado de la inteligencia burguesa del siglo XIX»,⁷ apenas podía contener su entusiasmo en las primeras frases del prefacio de su *Panóptico*: «Se reforma la moral, se preserva la salud, se vigoriza la industria, se difunde la instrucción, los pilares públicos se ilustran y la economía se sostiene, realmente, sobre una base firme; el nudo gordiano de las leyes para los desamparados no se elimina, se libera, ¡y todo mediante una sencilla idea arquitectónica!». Bentham prosigue elaborando «la totalidad de las vías que se abren ante mí» en tanto que «un nuevo modo de incrementar el poder de la mente sobre las mentes ajenas, en una medida sin precedentes hasta ahora [...] Tal es el artefacto, tal es el trabajo que puede hacerse con él».⁸ Tal «artefacto» se basa en lo que realmente parece una idea sencilla de ingeniería arquitectónica, aunque de ningún modo es tan sencilla como Bentham reivindicó. La realización práctica de esta idea era de una inmensa complejidad como para poder encomendar a nadie el proyecto de construir realmente, y mantener, una prisión así, pero es la riqueza del concepto y su amplio eco en la modernidad lo que le ha dado su importancia y lo ha hecho perdurar. Bentham se consideraba a sí mismo un reformador práctico, armado con diseños y proyectos concretos. Irónicamente, este austero ingeniero social, auténtica materialización de las advertencias de Edmund Burke respecto a una próxima era de «sofistas, economistas y calculadores», consiguió con su panóptico, no un diseño práctico, sino una brillante metáfora del poder en las sociedades modernas.

7. Karl Marx. *Capital*. Londres. Lawrence & Wishpert, 1972, vol. 1, parte VII, cap. XXIV, apartado 5.

8. Bentham. *op. cit.*, pág. 31. El título completo de la obra da una ligera idea de la grandiosidad de las pretensiones que albergaba Bentham: *Panóptico, o Centro de Inspección; conteniendo la idea de un nuevo principio de construcción aplicable a cualquier tipo de establecimiento, en el que las personas de cualquier descripción se mantendrán bajo inspección; y en particular para establecimientos penitenciarios, prisiones, establecimientos industriales, puestos de trabajo, albergues para pobres, fábricas, sanatorios, lazaretos, hospitales y escuelas, con un plan de gestión adaptado al principio panóptico*.

El sentido mesiánico de la misión social del proyecto de Bentham es evidente por su insistencia en el culto y en la formación religiosa dentro de su penitenciaría y, de modo más sorprendente, por el paralelismo subyacente entre su panóptico y la idea de un Dios invisible, omnipresente y todopoderoso. El inspector *ve sin ser visto*: su presencia, que es también una ausencia, se sustenta únicamente en su mirada vigilante, mientras que los prisioneros están encarcelados tanto en sus celdas como en sus propios cuerpos. No pueden escapar a la mirada vigilante y omnipresente que parece situarse en un mundo incorporeal, aunque penetre en el mundo corporal hasta hacerlo transparente. Evidentemente, tal omnipresencia del inspector es sólo un artificio arquitectónico, un elaborado juego de manos, un simple truco. Hay realmente un inspector (Bentham, siempre práctico, discute incluso diversas posibilidades para albergar a su familia), pero desaparece en la «figura completamente oscura» que los prisioneros pueden ver. Es el inspector imaginario, este subproducto de la construcción arquitectónica, el que eclipsa la realidad mundana, de modo parecido a la relación entre la idea de Dios y la misión de la Iglesia en la tierra.

El paralelismo religioso va incluso más lejos: Dios es inaccesible pero omnipotente, tal y como lo presenta el Nuevo Testamento. Sin embargo, como el Dios del Antiguo Testamento, el inspector interviene estratégicamente para asegurarse de que su presencia es reconocida. Bentham, por ejemplo, sugiere que ciertas pequeñas infracciones cometidas por los prisioneros pueden ser aparentemente pasadas por alto durante algunos días, animándolos entonces a cometer mayores transgresiones. Finalmente, la Voz emitirá el listado de todas las infracciones cometidas, por lo que cada prisionero se hará consciente de que la impunidad es una simple ilusión y de que incluso el silencio por parte del inspector sólo significa que, por misteriosas razones, ha preferido diferir su intervención: tanto Dios como el inspector lo saben todo, pero ellos mismos son incognoscibles.

El panóptico sólo es, en el fondo, un juego de prestidigitación, una simple ilusión, pero, según Bentham, crea el contexto adecuado para que los sujetos no tengan otra alternativa que creer que toda apariencia es realidad. La clave está en la vigilancia. El panóptico es, como Oceana o el Estado Unido, una ciudad de cristal monodireccional, pero aquí radica el problema del que Bentham parece haber sido ingenuamente inconsciente: consideraba que la vigilancia con-

llevaría la obediencia sin necesidad de recurrir a coerciones, ya que los prisioneros se harían dóciles mediante un adiestramiento permanente que provocaría la interiorización de las reglas y, de este modo, el consenso acabaría sustituyendo a la mera coerción. Pero la obediencia sigue descansando, en última instancia, en la amenaza coercitiva. Además, los sujetos del panóptico están recluidos y bajo vigilancia porque, justamente, son prisioneros privados de su libertad civil y de sus decisiones personales. Todas las instituciones a las que Bentham creía posible aplicar el principio panóptico se basan similarmente en diversos grados de coerción.

Si el truco de prestidigitación de la vigilancia para lograr el consenso requiere una coerción real o amenazadora, ¿no hay acaso una paradoja en el mismo corazón del proyecto panóptico? El consenso perfecto sólo se obtiene mediante el perfeccionamiento previo de la coerción: ¿por qué se quedan los sujetos bajo la mirada vigilante del inspector? ¿Por qué, si no están encerrados coercitivamente, permiten al inspector ser una «figura completamente oscura», que lo sabe todo y se mantiene incognoscible? ¿Qué les impide romper el cristal monodireccional y encontrarse, como Dorotea y sus amigos, al inseguro y repulsivo pequeño hombre que manipula y se esconde tras el amenazador rostro público del Mago de Oz?

La religión ha intentado resolver este problema del cumplimiento de la moral al imponer un Dios que exige castigos y recompensas después de la muerte. Sin embargo, esta solución siempre ha sido un modo muy imperfecto de asegurarse la obediencia al código moral en la vida presente, especialmente cuando las recompensas materiales por ignorar o desviarse de los preceptos de la moral divina pueden conllevar un atractivo mucho más inmediato. Pero para la lógica del panopticism no hay sanciones en la «otra vida»: sólo existe el aquí y el ahora. La metáfora de Bentham muestra cómo la vigilancia puede exigir la obediencia, y ser por lo tanto un instrumento efectivo para el control social, pero sólo en la medida en que los sujetos vigilados no tienen otra opción que la de someterse ellos mismos a la mirada vigilante del inspector. La historia de la vigilancia en el mundo occidental a lo largo de los siglos XIX y XX confirma la lógica panóptica de Bentham al mismo tiempo que se desvía persistentemente de ella. Tal lógica es apremiante, y diversos analistas sociales y políticos han señalado toda la perspicacia que contiene e implica el diseño panóptico. Pero los sujetos sometidos al control panóptico se han resistido a menudo.

El panóptico ha sido, en consecuencia, cuestionado en tanto que concepto, del mismo modo que lo haremos en este libro.

Una breve historia de la vigilancia

En su innovador y fundamental trabajo sobre el nacimiento de la prisión, Foucault se interesó por el concepto de panopticismo en «la intensidad imaginativa que ha poseído durante al menos doscientos años»:

Pero el panóptico no debe ser entendido como un edificio de la fantasía: es el diagrama del mecanismo del poder reducido a su forma ideal: su funcionamiento, abstraído de cualquier obstáculo, resistencia o fricción, debe ser representado como un sistema puramente arquitectónico y óptico: se trata de hecho de la figura de la tecnología política que puede y debe ser separada de cualquier uso específico.⁹

Aunque Foucault trataba específicamente de las prisiones, así como de los asilos, en un libro anterior,¹⁰ señaló que el principio del panopticismo no debería ser delimitado a tales recintos, deliberadamente aislados y separados de la sociedad. La disciplina organizada en recintos cerrados, como cuarteles, escuelas o talleres, «es lo que Bentham soñaba transformar en una red de mecanismos que estaría en todas partes y constantemente alerta, cubriendo toda la sociedad sin interrupciones de espacio o tiempo». De este modo, Foucault percibió en los siglos XVIII y XIX un «desplazamiento desde la disciplina excepcional a la vigilancia generalizada [...] la ampliación gradual de los mecanismos disciplinarios [...] su expansión a través de todo el cuerpo social, la formación de lo que puede llamarse, en general, la sociedad disciplinaria».¹¹ La tecnología panóptica se expandió desde instituciones especializadas y recluidas hasta las autoridades administrativas que organizaban tales instituciones, para invadir finalmente los «aparatos estatales, cuya mayor, si no exclu-

9. Foucault, *op. cit.*, pág. 205.

10. Foucault, *Histoire de la folie à l'âge classique*, París, 10/18, 1961; trad. inglesa de Richard Howard, *Madness and Civilization*, Nueva York, Pantheon, 1965; trad. cast.: *Historia de la locura en la época clásica*, Madrid, Fondo de Cultura Económica, 1979.

11. Foucault, *Discipline and Punish*, pág. 209.

siva, función es la de asegurarse de que la disciplina reina sobre la sociedad como una [policía] global».

Se puede hablar de la formación de una sociedad disciplinaria en este movimiento que se extiende desde las disciplinas encerradas y aisladas, una especie de «cuarentena» social, hasta los mecanismos indefiniblemente generalizables del «panopticismo». No es que la modalidad disciplinaria del poder haya reemplazado a todas las demás, sino que se ha infiltrado en las otras, algunas veces socavándolas, pero haciendo de intermediaria entre ellas, conectándolas, extendiéndolas, y haciendo posible situar los efectos del poder en elementos más distantes y actuales. Asegura una distribución infinitesimal de las relaciones de poder.¹²

La fábrica panóptica

Tal y como ha puesto de manifiesto el teórico social británico Anthony Giddens, el desarrollo del Estado-nación moderno está unido al crecimiento de la vigilancia en tanto que mecanismo crucial del control administrativo.¹³ Pero la forma predominante del Estado moderno no sólo remite al Estado-nación, sino también al Estado *capitalista*. El capitalismo separa lo económico de lo político y crea los compartimentos distintos, aunque interrelacionados, del sector privado y del sector público. Si, como sugiere Foucault, los principios y mecanismos panópticos se expanden mediante la infiltración, los puestos de trabajo del capitalismo deberían ser un buen lugar para empezar a localizarlos.

El conocimiento es un recurso productivo, tal y como ponen claramente en evidencia los puestos de trabajo del capitalismo. Adam Smith hizo famoso el poder productivo de la división del trabajo al describir cómo una fábrica de alfileres superaba ampliamente la producción de un fabricante tradicional al dividir el proceso de fabricación en dieciocho operaciones distintas, de las que se encargaban diferentes trabajadores.¹⁴ Estas operaciones y estos trabajadores deben ser organizados y supervisados a partir de una base permanente. Tras la revolución in-

12. Foucault, *ibíd.*, pág. 216.

13. Anthony Giddens, *The Nation-State and Violence*. Berkeley, University of California Press, 1987.

14. Adam Smith, *The Wealth of Nations*, 1776; nueva edición: Nueva York, Random House, 1937, págs. 4-5 (trad. cast.: *La riqueza de las naciones*, Barcelona, Folio, 1997).

dustrial, y bajo la presión de las exigencias del mercado para aumentar la eficacia productiva y el beneficio económico en los procesos de producción, la fábrica se convirtió en un lugar fundamental para la innovación en métodos de vigilancia y disciplina. Al instaurarse la cadena de montaje, los trabajadores quedaban insertados en un flujo constante y mecanizado, siendo tan intercambiables como las piezas que montaban. Además, en la cadena de montaje cada acción del trabajador es registrada automáticamente en la continuidad del flujo productivo, así como cada desviación es señalada instantáneamente por la interrupción del proceso. Henri Ford, el gran empresario de las cadenas de montaje masivas, no quedaba satisfecho con la vigilancia y el control de los trabajadores que podía llevar a cabo en sus fábricas. Como es sabido, esperaba que la vida «privada» de sus trabajadores también estuviera conforme con sus expectativas de probidad moral, por lo que organizó una compañía de espías (llamada significativamente «Departamento sociológico») para que investigara el comportamiento de sus trabajadores en sus horas libres. Con el desafío de los sindicatos, la vigilancia capitalista de los lugares de trabajo adoptó unas funciones policiales más agresivas. La gestión empresarial desarrolló, para sus propios objetivos, algunas de las típicas capacidades de los servicios de seguridad e inteligencia de los modernos Estados de seguridad nacional, de modo que pudiese prevenir, en primer lugar, la infiltración de cualquier sindicalista en las fábricas, así como, en caso de que dicha infiltración se produjese, poder vigilar estrechamente las actividades sindicalistas, y contrarrestar y boicotear las huelgas.

El lugar de trabajo capitalista tiene su propio Bentham, el teórico de la fábrica panóptica: Frederick Winslow Taylor, a principios del siglo xx, desarrolló y promocionó la gestión «científica», no sólo como un plan de acción para la clase ejecutiva o directiva, sino también como una panacea para conseguir un funcionamiento más efectivo de todos los aspectos de la sociedad capitalista. Como Bentham, Taylor se consideraba a sí mismo esencialmente como un hombre práctico (inventó un proceso para la producción de acero a alta velocidad) y no como un soñador idealista, pero, como Bentham, es más recordado por su ideal teórico, el que de hecho lleva su nombre y remite a una ideología: el taylorismo.¹⁵ La esencia del taylorismo,

15. Reg Whitaker. «Scientific management as political ideology», *Studies in Political Economy*, n.º 2, 1979, págs. 75-108.

o gestión «científica», se basa en la aplicación del principio de la división del trabajo elaborado por Adam Smith para organizar de modo efectivo la producción en todos los procesos laborales de los trabajadores. Según Taylor, todo trabajo puede descomponerse en distintos movimientos, y se podría alcanzar una mayor eficacia mediante un análisis científico de tales movimientos que nos indicase «el mejor modo» de llevar a cabo cada trabajo. El estudio llevado a cabo por Taylor y sus discípulos sobre tales movimientos y sus consecuencias temporales llenó las fábricas de expertos en eficacia, armados con cronómetros y tablas de apuntes. La gestión empresarial, coronada por una aura de cientificismo, reclamaba ahora el monopolio del conocimiento útil sobre el proceso de producción, apropiándose de hecho del saber hacer del trabajador para convertirlo en una unidad cuyo funcionamiento sería controlado por una observación minuciosa y continua. En el puesto de trabajo panóptico, el inspector fue reemplazado por el experto en eficacia con resultados similares: una mirada ininterrumpida y vigilante controla a los sujetos; el observador que lo sabe todo pero que se mantiene incognoscible. Un sistema de compensación de la velocidad a la que circulaban las piezas, orientado a la medición precisa de la productividad, se encargaría de que se cumpliesen todos los movimientos y órdenes exigidos, sin necesidad de recurrir a un poder coercitivo manifiesto.

Así era por lo menos en teoría, ya que, al igual que con el panóptico de Bentham, el sistema de Taylor ha sido más memorable en tanto que concepto de la imaginación que como una realidad concreta, a lo que sin duda ha contribuido la resistencia de los trabajadores para servir meramente como aceleradores del trabajo mecanizado y aumentar los beneficios de los empresarios. Una vez más, el sueño panóptico vacila ante las limitaciones del poder coercitivo, subyacente pero necesario para que el sistema, aparentemente voluntarioso y obediente, funcione de hecho. Con el tiempo, las tempranas y prístinas teorías sobre la gestión «científica» fueron transformadas con el propósito de incluir las «relaciones humanas» en la gestión empresarial, lo que permitía métodos más conciliadores (los críticos dirían engañosos) para obtener el acuerdo consensual de los trabajadores y su participación en el proyecto empresarial. Sin embargo, aunque el taylorismo haya quedado enterrado, la gestión «científica» ha perdurado: el poder en los centros de trabajo no sólo

se basa en la posesión de capital y en la apropiación de la fuerza laboral del trabajador (condiciones estructurales), sino también en el funcionamiento operativo y cotidiano de la gestión empresarial mediante una cada vez mayor capacidad de vigilancia, así como en la concentración de conocimiento útil que permite la capacidad anterior. La resistencia de los trabajadores ha dificultado el ejercicio sin trabas de este poder, pero no ha conseguido invertirlo nunca.

La vigilancia en los centros laborales es especialmente efectiva porque es *reflexiva*: la «gestión» controla tanto a los trabajadores como a sí misma, y los estudios sobre la eficacia han tratado tanto de procesos administrativos y de supervisión como de los mecanismos productivos. Como veremos más adelante, la difusión de las nuevas tecnologías de la información en los lugares de trabajo no sólo ha aumentado notablemente el poder de la vigilancia disciplinaria *in situ*, sino que también ha intensificado la capacidad reflexiva de la gestión para controlar su propia actuación y tomar las medidas más apropiadas para mejorar su eficacia. Además, las nuevas tecnologías permiten incluso desplazar el lugar de trabajo y dispersar geográficamente a los trabajadores y gestores sin que disminuya la vigilancia supervisora de sus actividades: el panóptico descentralizado.

El Estado panóptico

La empresa capitalista, en resumen, ha sido y sigue siendo un lugar fundamental para el ejercicio de la vigilancia, así como para la innovación de las tecnologías y de los métodos de organización de dicha vigilancia. Al mismo tiempo, la historia del capitalismo ha sido, al menos hasta hace poco, la historia de capitalismo nacionales, en los que el Estado-nación actuaba como contenedor, con goteras, es cierto, pero contenedor a pesar de todo. El Estado-nación moderno conlleva una soberanía en tanto que monopolio del ejercicio legítimo de coerción sobre un territorio dado, generalmente, aunque no siempre, en correlación con la unidad de una lengua y de una cultura, y con una identidad nacional. Funcionalmente, el Estado-nación consiste en una unidad administrativa encargada de organizar el territorio nacional, estableciendo y manteniendo el orden mediante regulaciones y leyes, actuando como juez en los conflictos relativos a la distribución de recursos, redistribuyendo los recursos nacionales

mediante impuestos y gastos, y proveyendo la infraestructura social y económica a la empresa capitalista. Además, puesto que ningún Estado se ha convertido en una «isla» autosuficiente, los Estados también han tenido que establecer relaciones comerciales, diplomáticas y militares con otros Estados, lo que significa, en la práctica, la instauración de ejércitos permanentes y profesionales, así como la capacidad tecnológica y la voluntad de costear la guerra en la época actual.

Todo ello requiere conocimiento, y especialmente un conocimiento reflexivo, es decir, la capacidad cada vez mayor del Estado para supervisar todas sus actividades y a sí mismo. Para cobrar los impuestos a los ciudadanos, debe conocer la distribución de la renta y de la propiedad, pero también debe controlar sus propios medios de recaudar los ingresos. Antes de que emergiera el Estado moderno, los impuestos se recaudaban por encargo, una práctica que, además de conllevar una extensa corrupción y opresión, difuminó el poder y debilitó al Estado centralizado. La centralización de los impuestos requiere una base de datos centralizada: el Estado debe conocer todo lo que puede ser susceptible de pagar impuestos y a quién exigirlos. Al reunir y analizar toda esta información, el Estado también obtiene una evaluación de sí mismo, de su capacidad fiscal y de sus limitaciones. De modo similar, en el mantenimiento de la ley y del orden, el Estado reúne información confidencial sobre los ciudadanos, asociaciones, grupos y clases mediante diversos medios, y, a partir de esa información, hace intervenciones estratégicas en la sociedad civil así como en el mantenimiento cotidiano del orden. Mediante el mismo proceso, el Estado también controla su propia legitimidad y autoridad.

En todas estas actividades típicas del Estado, la vigilancia es un instrumento crucial e incluso, en un sentido muy amplio, es su instrumento más fundamental. Muchos de los aspectos específicos del Estado moderno se consideran fácilmente normales, perdiéndose aquello que tienen de único desde una perspectiva histórica más amplia. Por ejemplo, la elaboración rutinaria de estadísticas sobre cada aspecto de la sociedad, de la cultura y de la economía es una actividad intrínseca del Estado moderno, y sólo puede ser comparada con métodos muy rudimentarios y fragmentarios de épocas anteriores. Tales estadísticas permiten un grado de autoconciencia colectiva sin precedentes históricos. La sociedad se ha convertido en objeto de su propia reflexión, pero de un modo que refleja el mismo método es-

tadístico: las relaciones cuantitativas han sustituido a las cualitativas, así como las categorías, clases y otros conceptos objetivos han aplastado a los seres humanos. El objeto es siempre una elaboración del entendimiento para hacer comprensible el mundo social, con el objetivo de cambiarlo o de controlarlo. La información estadística es ideal para poner «sujetadores» a los sujetos. Las cualidades morales y personales de cada individuo no son mensurables, pero su actividad productiva, sus propiedades, su renta y patrimonio, sus relaciones contractuales, sus infracciones de la ley, todo ello es mensurable y ofrece una posibilidad de regulación. Pero la vida personal e íntima de los individuos (sus pensamientos y su motivación) no es calculable, por más que el comportamiento pueda ser vigilado y registrado. La vigilancia estadística nunca es un conocimiento en sí misma, al menos en un sentido filosófico, ya que la filosofía remite, literalmente, al amor por el conocimiento. Se trata de un conocimiento orientado al control, y se ha empleado básicamente al servicio del Estado, aunque, como veremos más adelante, quizás menos en el presente y en el futuro próximo que en el pasado inmediato.

Las ciencias sociales, llamadas ocasionalmente ciencias del «comportamiento», emergieron al mismo tiempo que el Estado en tanto que productor de conocimiento, lo cual no es ninguna casualidad, como tampoco es una mera coincidencia la dependencia de las ciencias sociales respecto a las estadísticas elaboradas por el Estado. Incluso la conceptualización de la «sociedad» por los sociólogos, de la «economía» por los economistas o del «gobierno» por los científicos del hecho político, han sido estructuradas por el tipo de estadísticas que los Estados requerían para sus intereses, así como por el modo en que los Estados organizaban la información. En consecuencia, para cerrar el círculo, los científicos sociales han ayudado, a su vez, a elaborar los perfiles e informes estadísticos del Estado, al enriquecer y desarrollar tales instrumentos científicos. Tal relación simbiótica —de la que la extraña pareja, o relación, entre el espía y el académico tratada en el capítulo anterior sería un subapartado— es un producto del conocimiento reflexivo hecho posible por la naturaleza del Estado moderno. Tampoco puede separarse de la voluntad de poder inherente a la capacidad, descrita más arriba, de ampliar y profundizar en la autoconciencia colectiva. Ya sea en tanto que proyectos políticos impulsados por el Estado, o en tanto que movimientos y escuelas interpretativas de las ciencias sociales, el conocimiento

ya no puede separarse analíticamente del control que dicho conocimiento promete y permite. Tal indistinción es independiente de que los propósitos concretos sean conservadores o reformistas: cambiar o mantener el orden social remiten del mismo modo a la manipulación, a la intervención y al control: ambas actividades requieren una base estadística.

Desde el punto de vista estatal, el desarrollo de un aparato administrativo racional, lo que Max Weber llamaba una burocracia moderna,¹⁶ es un asunto crucial. Los burócratas son nombrados y promocionados por sus méritos, y no a partir del parentesco o la recomendación; es el oficio y su función lo que detentan la mayor importancia, y no la persona y sus relaciones. La administración debe tener lugar en un contexto de reglas establecidas, con expectativas que tengan un grado razonable de predicción. La obediencia a las regulaciones y a las órdenes administrativas debe ser normal, rutinaria. Para que el sistema pueda mantenerse, la información es una pieza clave, ya que la habilidad del Estado administrativo para llevar a cabo su gestión se fundamenta, justamente, en un amplio conocimiento de la sociedad, y de dónde y cuándo se producen desviaciones de su funcionamiento regular.

En el interior de un Estado administrativo eficiente, el poder panóptico puede reproducirse en varios lugares para observar distintas categorías de personas. Las escuelas preparan a los individuos a lo largo de su infancia, adolescencia y juventud, entrenándolos para la disciplina de la oficina o de cualquier otro lugar de trabajo. La disciplina de los centros de trabajo sólo se aplica, evidentemente, a los empleados. Para los desempleados, «inempleables» o jubilados, el Estado ofrece programas de seguridad social o de bienestar que también consisten en elaborados sistemas de vigilancia que recogen información detallada de sus «clientes». En todos los casos existen poderosos incentivos (ingresos o beneficios) para permanecer voluntariamente bajo la vigilancia panóptica, así como paliativos para los que pretender escapar de ella. Si a pesar de las «zanahorias» y de los «azotes» uno pretendiese escaparse deliberadamente, hay muchas posibilidades de terminar sujeto a sanciones criminales, lo que quiere decir prisionero en el sentido más literal de Bentham.

16. Max Weber, *The Theory of Social and Economic Organizations*, Londres, W. Hodge, 1947.

Una vez más, nos encontramos ante el principio fundamental del panóptico en funcionamiento: el inspector, ahora convertido en burócrata, controla a los prisioneros, ahora la sociedad, totalmente transparente a su mirada vigilante. Pero, de nuevo, esta transparencia es monodireccional, ya que el Estado se mantiene celosamente escondido gracias al secreto administrativo. El Estado sólo aparece ante el sujeto en tanto que objeto impenetrable y separado, del mismo modo que la administración de la política, sin tener que rendir cuentas a los votantes democráticos. La coerción, desde luego, acecha en la sombra, en tanto que sanciones subyacentes destinadas a fomentar la obediencia al Estado, que tiene todos los instrumentos para ver y registrar cualquier infracción de las reglas. La diferencia entre el estado panóptico y el panóptico de Bentham sólo remite a distintos grados de complejidad: la sociedad es mucho más amplia y un fenómeno infinitamente más complicado que una cárcel, así como más escurridizo al saber y, en consecuencia, al control. Tampoco hay ningún burócrata que pueda ser comparado al inspector en tanto que tal: el volumen de la información procesada por el inmenso aparato de la vigilancia estatal es demasiado elevado como para remitir a cualquier individuo. Ésta es precisamente la razón por la cual la burocracia weberiana debe acompañar y respaldar a la vigilancia estatal: su organización jerárquica de las oficinas y de las funciones pretende facilitar la gestión racional y colectiva (así como policial) de la información. El inspector colectivo se transforma de este modo en una división funcional del trabajo para desarrollar esencialmente el mismo papel de vigilante, con exactamente los mismos objetivos: la interiorización de las reglas por los sujetos, su obediencia, sin recurrir, siempre que sea posible, a una coerción manifiesta.

El moderno Estado administrativo ha sido un gran innovador en técnicas y tecnologías de vigilancia, muchas de las cuales se han generado mediante su aparato militar,¹⁷ tal y como hemos planteado en el capítulo anterior en relación con los servicios de inteligencia. La vigilancia político-policial, con su evidente respaldo coercitivo por parte del Estado, sin duda más visible que en cualquier otra área, también remite a la vanguardia de tales innovaciones. Otras áreas administrativas del Estado han permitido el desarrollo de técnicas

17. El libro de Dandeker, *Surveillance, Power and Modernity*, es especialmente interesante para apreciar la contribución militar a la vigilancia tecnológica.

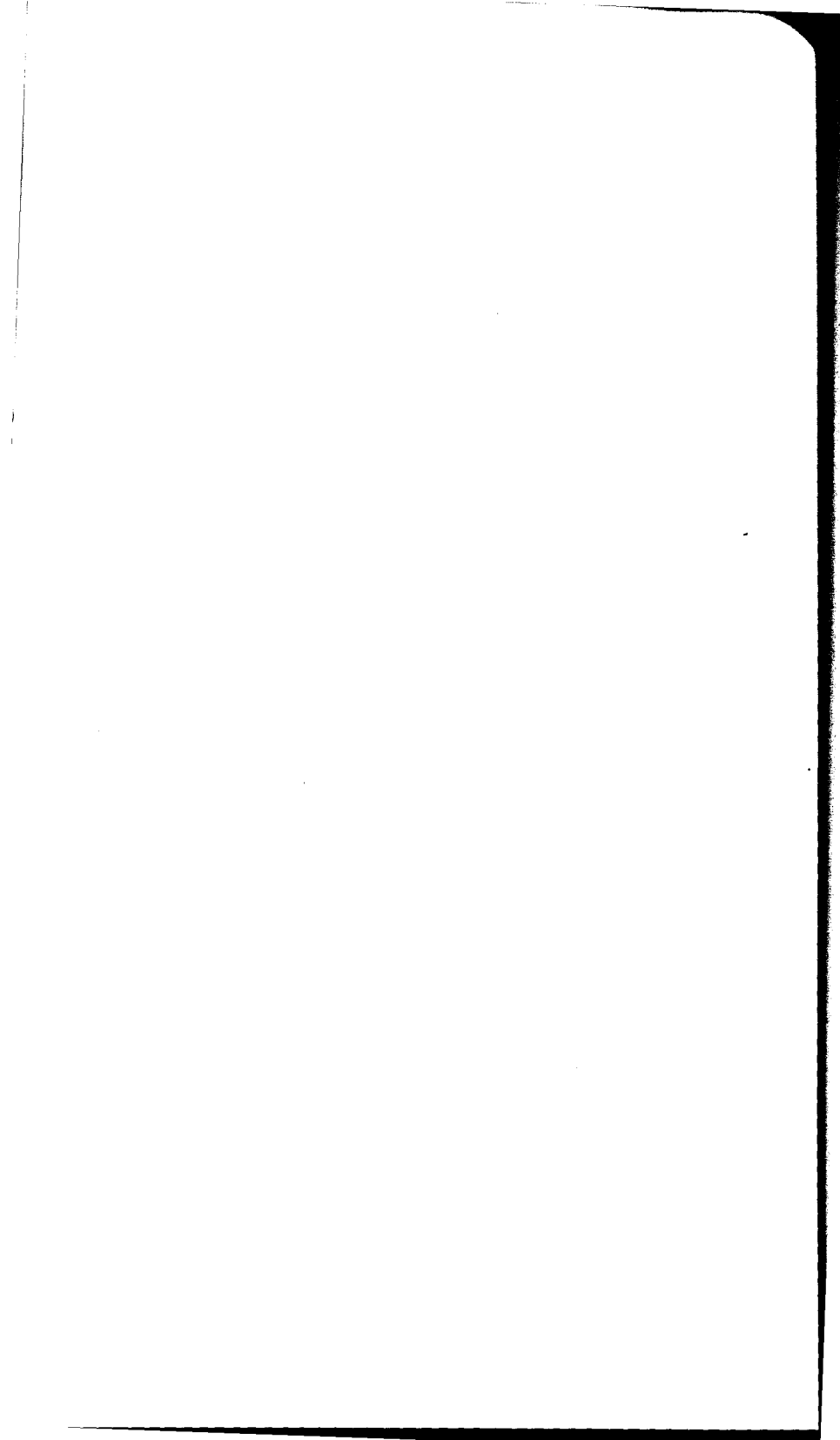
para recoger información específica, según sus intereses particulares, tales como la protección de la salud, un campo en el que los avanzados métodos de vigilancia relacionados con la salud y aplicados a vastas poblaciones se han originado en sectores administrativos del Estado.

El panóptico y su aversión al riesgo

La analogía panóptica no estaría completa sin referirnos a una última similitud fundamental. El panóptico de Bentham recurría a las sanciones punitivas para aquellos que infringían las reglas, pero ejercía de forma mucho más importante un control preventivo. El Estado administrativo, junto al sector privado y corporativo, va un paso más allá al establecer, para una categoría dada de personas, las probabilidades estadísticas de que infrinjan las reglas. Cuando el riesgo puede ser calculado confidencialmente, es posible excluir a los transgresores potenciales de cualquier oportunidad de desobediencia. Vastas compañías, públicas o privadas, emprenden constantemente análisis del riesgo y muestran abiertamente su aversión al mismo. Algunos observadores han llegado a hablar de la «sociedad del riesgo» contemporánea.¹⁸ Sin duda, las bases de datos y las redes y contextos informáticos relacionados con factores de riesgo (lo que se ha llamado «sistemas de comunicación con riesgo») son ellos mismos elementos panópticos fundamentales. El riesgo debe ser gestionado y contenido y, aunque la prevención conlleva más gastos, es socialmente menos perjudicial que los castigos y sanciones por hechos consumados. En consecuencia, el Estado panóptico se orienta cada vez más hacia el futuro y se concentra cada vez más en el poder de predicción de la información que acumula, del mismo modo que las empresas capitalistas del sector privado se orientan hacia la recuperación futura de sus inversiones. Tanto el Estado como las empresas se convierten así en rehenes de la incertidumbre, razón por la cual buscan y acumulan, con entusiasmo y avidez, tanta información como les sea posible, esperando reducir de este modo la incertidumbre que les acecha.

18. Richard V. Ericson y Kevin D. Haggerty, *Policing Risk Society*, Toronto, University of Toronto Press, 1997.

El apetito informativo que provoca tal aversión al riesgo parece extensible de forma indefinida. Con las nuevas tecnologías que permiten recoger, procesar, acumular y recuperar información, las tendencias panópticas de la sociedad moderna aumentan de forma desmesurada, tanto en sus posibilidades como en su eficacia. En los próximos capítulos nos centraremos en estas nuevas tecnologías y sus efectos.



3. El ciberespacio: la biblioteca de Babel¹

Diversas profecías de revolución han inundado la cultura capitalista de este fin de siglo, anunciando unas transformaciones tan profundas que apenas podemos discernir sus implicaciones. Pero esta vez el fantasma de la revolución no viene de abajo, sino de afuera, mediante un milagroso agente *deus ex machina*: la tecnología. Tras la revolución agrícola y la revolución industrial, ahora estamos sumergidos en la revolución informática: el ordenador está transformando la economía, la sociedad, la cultura e incluso a los mismos seres humanos.

Para ciertos profetas, los futurólogos digitales del capitalismo, esta revolución no es un fantasma, sino un faro que señala hacia un

1. Algunas partes de este capítulo han aparecido en «The Tower of InfoBabel: Cyberspace as Alternative Universe», en Leo Panitch (comp.), *Socialist Register 1996: Are There Alternatives?*, Londres, Merlin Press, 1996, págs. 173-188.

futuro más brillante, un futuro radicalmente distinto del presente, aunque *plus ça change, plus c'est la même chose*: el capitalismo será el motor de esta transformación, ya que es el que mueve los hilos del cambio tecnológico; el mismo capitalismo que sabe cómo usar la tecnología para fines prácticos y que ofrece el mercado adecuado para su difusión y circulación. Algunos capitalistas quedarán desca- rriados por la inmensa rueda del *laissez faire*, pero aquellos que aprendan a gobernar la tecnología serán recompensados con posiciones clave en los altos mandos del nuevo mundo.²

En contra de este chorro de sirenas revolucionarias conservadoras, existe un grupo de profetas izquierdistas, más pequeño, menos omnipresente en los medios de comunicación y en las nuevas plataformas electrónicas, pero con el mismo entusiasmo, que ven las semillas de una revolución social en las nuevas tecnologías: la democracia no emanará del cañón de una pistola, sino del ordenador personal y del módem, mientras que los Estados y las corporaciones del sector privado perderán el control del flujo informativo: el verdadero amo de Internet será la gente.³

Ambos bandos comparten al menos el principio de que la tecnología es ahora el motor autónomo de la historia. Es como si nos hubieran lanzado unos dados cósmicos y todos, nerviosos y ansiosos, estuviéramos esperando conocer los resultados. Existe un tercer bando, no muy identificable políticamente mediante las etiquetas tradicionales, que también comparte este determinismo tecnológico: los pesimistas, que consideran nefastos todos estos cambios y predicen la destrucción del empleo, el fin de los valores, la degradación de la sociedad y la atrofia cultural.⁴

2. Véase, por ejemplo, Nicholas Negroponte, *Being Digital*, Nueva York, Vintage Books, 1995. Un consultor canadiense, Don Tapscott, ofrece una visión ligeramente más equilibrada y prudente en *The Digital Economy: Promise and Peril in the Age of Networked Intelligence*, Nueva York, McGraw Hill, 1996.

3. Es realmente difícil encontrar una sola obra representativa de esta perspectiva. Quizás una de las más cercanas podría ser la de Howard Rheingold, *The Virtual Community: Homesteading on the Electronic Frontier*, Reading, Massachusetts, Addison-Wesley, 1993. La posición política de Rheingold remite a una especie de anarquismo norteamericano: es notable que haya tan pocos «antiguos izquierdistas», o marxistas, entusiasmados con la Red.

4. David E. Noble, *Progress Without People: New Technology, Unemployment, and the Message of Resistance*, Toronto, Between The Lines, 1995. Noble acepta orgullosamente el calificativo de «ludita», término derivado de los obreros destructores de máquinas textiles a principios del siglo xx.

Finalmente, hay un cuarto bando, también políticamente inclasificable, que rechaza el determinismo tecnológico de los otros, se burla del «infobombo», y argumenta que podemos hacer retroceder la gran rueda, o al menos detenerla en alguno de sus giros, si reconocemos la debilidad y el engaño de tales profecías.⁵ La revolución de la información es, desde esta perspectiva, un simple aumento cuantitativo de todos los mecanismos y hábitos actuales, y no un salto cualitativo en lo desconocido.

Dada esta carrera desenfrenada tras las últimas innovaciones que caracteriza este tipo de discusiones, sorprende realmente descubrir una imagen perfecta de la era de la información, forjada por un escritor argentino ajeno a cualquier interés sobre el presente o el futuro de la tecnología. Se trata de la excepcional visión que Jorge Luis Borges ofrece de la «Biblioteca de Babel»:⁶

El universo (que otros llaman la Biblioteca) se compone de un número indefinido, y tal vez infinito, de galerías hexagonales [...] Desde cualquier hexágono, se ven los pisos inferiores y superiores, interminablemente. La distribución de las galerías es invariable. Veinte anaqueles, a cinco largos anaqueles por lado, cubren todos los lados menos dos; su altura, que es la de los pisos, excede apenas la de un bibliotecario normal. Una de las caras libres da a un angosto zaguán, que desemboca en otra galería, idéntica a la primera y a todas [...] Por ahí pasa la escalera espiral, que se abisma y se eleva hacia lo remoto. En el zaguán hay un espejo, que fielmente duplica las apariencias [...] La Biblioteca es una esfera cuyo centro cabal es cualquier hexágono, cuya circunferencia es inaccesible.

La «Biblioteca de Babel» considera al universo un almacén de información, por lo que la vida se convierte en la actividad de recuperar e interpretar dicha información. En el pasado, esta visión podría ser descartada como la curiosa alucinación de un erudito que confunde su propia vida bibliófila y bibliógrafa con la vida en sí misma. Cuando Edward Gibbon, el gran historiador del siglo XVIII, presentó el segun-

5. Clifford Stoll, *Silicon Snake Oil: Second Thoughts on the Information Highway*, Nueva York, Doubleday, 1995. Stoll también es el autor de una especie de historia de suspense tecnológica y real, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, Nueva York, Doubleday, 1989.

6. Jorge Luis Borges, *Ficciones*, Alianza, Madrid, 1956, 1975, págs. 89-90.

do volumen de su monumental *Decline and Fale of the Roman Empire** al duque de Gloucester, éste respondió: «¡Otro maldito libro grueso y cuadrado! Siempre garabatos, garabatos y más garabatos, ¿eh, Gibson?». ¿Acaso Borges, el escritor o «garabateador», no ha hecho más que evocar una metáfora del universo como que biblioteca? Sin duda. Sin embargo, esta metáfora señala algo realmente fundamental de la era de la información: todos somos ahora escritores, «garabateadores», aunque la escritura mediante teclado esté sustituyendo a las plumas y a los bolígrafos, y ya no se almacene tanto en «libros gruesos y cuadrados» como en el éter del ciberespacio. La promesa inherente a la era de la información es precisamente que la llave de la biblioteca infinita está en nuestras manos, esa biblioteca «cuya circunferencia es inaccesible», pero que constituye «una esfera cuyo centro cabal es cualquier hexágono». Volveremos a ocupar de nuevo el centro exacto del universo, del que fuimos desalojados hace tanto tiempo por la ciencia al descentrar a la humanidad. Desde este centro, podremos dominar las líneas visibles de todos los otros hexágonos, que se extienden remotamente hacia cualquier dirección, y alcanzar en tiempo real, al instante, las distancias más lejanas para recuperar la información precisa que queramos, en cualquier momento.

En los hexágonos infinitos (e infinitamente centrados) de la biblioteca, no sólo los escritores y los académicos podrán explorar sus anaqueles y estantes. Sus usuarios también serán empresarios y hombres de negocios, haciendo aparecer en pantalla datos del mercado, revalorizando aportaciones extraviadas de la producción, ordenando servicios financieros y contables, y sistematizando los movimientos de entrada y de salida de la información, con el propósito de optimizar sus operaciones y obtener el máximo beneficio; también los generales y otros oficiales bajo el C³I (comando, control, comunicación y servicios de inteligencia y de información), simulando batallas virtuales en sus pantallas; también los agricultores, organizando el mantenimiento y el cultivo de sus campos mediante el análisis de sus programas informáticos, conectados a las imágenes digitales de un satélite espacial; también los entrenadores deportivos, enviando tácticas precisas a sus jugadores en tiempo real, basadas en los cálculos de probabilidades de sus programas, con ordenadores portátiles conectados a las pantallas

* Trad. cast.: *Historia de la decadencia y ruina del Imperio Romano*. Madrid, Turner, 1984.

de las líneas de banda; también los conductores de taxi u otros vehículos, cuyos ordenadores estarán procesando el camino más rápido a través del laberinto de las calles de la ciudad, detectando instantáneamente el estado del tráfico. La base común de todas estas actividades aparentemente dispares, así como de miríadas de otras, es el procesamiento de la información. Cada una requiere conocimientos, habilidades y experiencia que no pueden ser totalmente separados del sujeto que las practica, *por el momento*. Pero cada vez más actividades, de un modo sin precedentes en épocas anteriores, son trasladadas al procesamiento informático y devueltas luego al mundo de la acción. Puede parecer un mecanismo añadido, incluso innecesario, pero se trata de una mediación que desata poderes nuevos y revolucionarios.

Este paso intermedio, la conversión del material previo en representaciones abstractas y manipulables por los programas informáticos, remite al lenguaje universal de la digitalización. La información se codifica para que pueda ser interpretada por las máquinas, lo que quiere decir en formas reducibles a las combinaciones de 0 y 1, que representan voltajes altos o bajos, mecanismos de apertura y de cierre. La codificación digital es un lenguaje universal porque cualquier medio de expresión puede ser almacenado digitalmente y recuperado posteriormente: textos, sonidos e imágenes pueden ser convertidos en datos y restaurados cuando sea necesario. Además, la restauración es exacta, por lo que una vez se ha codificado digitalmente algo, ya no tiene sentido distinguir entre originales y copias. Sólo existe una Mona Lisa; las copias, por más expertos que sean sus autores, sólo serán copias. Sin embargo, una imagen, un texto o una pieza musical producidos digitalmente pueden ser reproducidos infinidad de veces, sin la menor pérdida o degradación de su integridad, sea cual sea ésta. Aquellos que reciban el objeto pueden «perfeccionarlo», añadiéndole o sustrayéndole elementos, sin por ello comprometer de ningún modo la integridad de la versión recibida, que ahora coexistirá con múltiples versiones manipuladas, o variaciones. A diferencia del vandalismo artístico que borra un ojo o añade un bigote a la Mona Lisa, perjudicando de forma irreparable el original, los objetos digitales pueden ser alterados y reproducidos de forma indefinida: una Mona Lisa con un solo ojo y bigote puede coexistir durante siglos con una Mona Lisa digital intacta (suponiendo que alguien quiera otorgar cierta inmortalidad a la versión revisada, reproduciéndola).

Los objetos digitales tampoco requieren el mismo mantenimiento. La Mona Lisa, en tanto que objeto material, se deteriora, por lo

que es necesario ofrecerle condiciones adecuadas de temperatura, clima e iluminación, e incluso hacer ciertas restauraciones parciales de vez en cuando para contrarrestar el efecto negativo del paso del tiempo. Una Mona Lisa digital, por el contrario, no «envejece», ya que los códigos digitales que la describen son una abstracción que permanece, en cierto sentido, fuera del tiempo.⁷ Además, la pintura auténtica de la Mona Lisa es un objeto material que ocupa un cierto espacio físico: una pared específica de una de las galerías del Louvre, en París. Cuando se logró un acuerdo, hace algunos años, para exhibir numerosas pinturas de este museo en Nueva York, tuvieron que hacerse elaborados artificios y recurrir a sofisticados dispositivos para transportar tales objetos, así como para guardarlos y mantenerlos seguros una vez allí, y luego devolverlos intactos a sus lugares de origen. Una Mona Lisa digital, por el contrario, puede transmitirse casi instantáneamente desde París a Nueva York, por un coste extremadamente bajo en comparación con el transporte físico del mismo cuadro. De hecho, cualquier número de réplicas exactas de una Mona Lisa digital puede coexistir simultáneamente en todo tipo de situaciones y lugares alrededor del mundo.

La digitalización permite una alquimia sorprendente: el transporte (de objetos físicos) se transforma en comunicación (de bits de información). Tal transformación conlleva una importante reducción de los costos, lo cual ha generado un nuevo imperativo comercial: enviar bits en lugar de cajas. Por ejemplo, en otros tiempos los lectores del *New York Times* que no vivían en Nueva York tenían que esperar diariamente la llegada del periódico mediante camiones, trenes o aviones, hasta que se lanzó una versión digital vía satélite a varios centros de impresión alrededor del continente que producen el diario para su distribución local. Pero la digitalización permite una forma aún más directa de transmisión: ahora, puedo recibir el *Times* en la pantalla de mi ordenador, leer lo que quiera en la misma pantalla del ordenador, grabar artículos de interés especial en mi disco duro para posibles referencias o citas, o redistribuir artículos a quienquiera que tenga acceso a los servicios de Internet, en cualquier lugar, instantáneamente. Todo ello se efectúa, cabe insistir, con una total indiferencia a las otrora imponentes barreras del espacio y del

7. Esto sólo es verdad «en cierto sentido», ya que el código digital también debe ser almacenado.

tiempo; puedo recibir mi periódico diariamente y en tiempo real aunque esté en Toronto o en Tokio.⁸

La digitalización es una especie de alquimia, aunque no tenga nada de mágico: la clave reside en el lenguaje universal del 0 y del 1. Se trata de una universalidad sin precedentes, lo cual permite renovar la pertinencia y la promesa de la biblioteca de Borges en tanto que metáfora del mundo.

Del coloso al microprocesador: la alquimia se pone a funcionar

La digitalización ha provocado básicamente dos innovaciones: ordenadores más pequeños, más rápidos y más inteligentes, y sistemas de telecomunicación por red a escala internacional y en tiempo real.

La máquina pensante ya era una idea mucho antes de convertirse en realidad. Podríamos retroceder hasta el siglo XIX, cuando Charles Babbage concibió un Artefacto Analítico con muchos de los elementos de los ordenadores digitales contemporáneos. Pero Babbage estaba muy limitado por la tecnología victoriana, por lo que se imaginó una enorme máquina a partir de engranajes y palancas que, como era de prever, no fue realizada.⁹ Alan Turing publicó un artículo en 1937 proponiendo una máquina que sería capaz de llevar a cabo los diferentes pasos de la computación mental. Dicha máquina imaginaria se ha hecho célebre como «la máquina universal de Turing», una especie de forma matemática platónica del ordenador digital ideal, del que todos los ordenadores actuales sólo serían aproximaciones imperfectas. Durante la guerra, mientras trabajaba en el desciframiento de códigos en Bletchley Park, Turing se enfrentó a la necesidad de construir una máquina real para satisfacer las insaciables demandas de desciframiento de las comunicaciones militares

8. Para una minuciosa descripción de todas las posibilidades de la digitalización, véase Jim Davis y Michael Stack, «The Digital Advantage», en Jim Davis, Thomas A. Hirschl y Michael Stack, *Cutting Edge: Technology, Information Capitalism and Social Revolution*, Londres, Verso, 1997, págs. 121-144.

9. Los novelistas *ciberpunk* William Gibson y Bruce Sterling, autores de *The Difference Engine*, Nueva York, Bantam Books, 1991, imaginan una Inglaterra victoriana contrafactual en la que la máquina de Babbage no sólo se construye, sino que tiene una amplia difusión.

alemanas. El resultado fue el primer ordenador digital del mundo, una máquina enorme con 2.400 tubos de transmisión, adecuadamente llamada COLOSO. En la Universidad de Pennsylvania empezó otro proyecto militar durante la guerra que se completó en 1946, en los inicios de la Guerra Fría, y que dio como resultado el ENIAC, un ordenador que transformaba al COLOSO en un enano: 18.000 tubos de transmisión, 1.500 retransmisores, 70.000 reóstatos y 10.000 condensadores: las luces de toda Filadelfia parpadeaban cuando se encendía ENIAC; no podía almacenar programas, por lo que tenía que ser programado externamente; los tubos de transmisión ardían a una velocidad alarmante, pero el ordenador consiguió completar el trabajo que se le asignó: los cálculos para un modelo matemático de la bomba de hidrógeno.

Medio siglo después, el poder de los ordenadores ha crecido mucho, y sin duda inspira más confianza la capacidad de un simple PC de despacho que el mastodonte que era ENIAC. Ciertas innovaciones clave han transformado radicalmente la informática en términos de tamaño y velocidad. La primera fue en 1947 en los laboratorios de Bell, en Nueva Jersey, donde se desarrolló el primer transistor miniaturizado que remplazaría a los ineficaces e inseguros tubos de transmisión. El primer uso comercial del transistor fue la radio portátil en la década de los cincuenta, un signo temprano de la época de los medios de comunicación móviles y ubicuos que se avecinaban. Pero era de mucha mayor significación, aunque no se percibiese inmediatamente, la nueva capacidad para construir ordenadores más pequeños y económicos.¹⁰

A lo largo de la década de los sesenta, la informática se desarrolló, pero se mantuvo en un nivel muy parecido. Fue a partir de 1970 que se dieron diversos momentos decisivos que concentran un cierto número de innovaciones clave. A finales de la década de los sesenta, se desarrolló el primer microprocesador de silicio, comercializado a partir de 1971. El microprocesador, o chip, puede contener varios transistores, permitiendo una mayor miniaturización del poder informático. Además, no sólo pueden ser insertados en un ordenador, sino también, al menos potencialmente, en cualquier objeto,

10. Len Dye, «50 Years Ago, Information Age Began in Bell Labs», *Los Angeles Times*, 22, diciembre de 1997. Michael Riordan y Lillian Hoddeson, *Crystal Fire: The Birth of the Information Age*, Nueva York, W.W. Norton & Company, 1997.

haciendo emerger la ubicuidad de los ordenadores portátiles y desde las tarjetas a los coches «inteligentes». La ley de Moore, formulada en la década de los sesenta, preveía que podría desdoblarse el número de transistores de un mismo microprocesador cada seis meses. Tal y como se explicó en el *New York Times*:

El transistor es la unidad básica de almacenamiento de información para el microprocesador de un ordenador: un dígito para cada transistor. Así que cada dieciocho meses se doblará su capacidad de memoria, con todos los incrementos de velocidad y de eficacia que este aumento conlleva. Actualmente, los chips de Intel con más capacidad albergan treinta y dos millones de transistores.

La ley de Moore también predijo que mientras el poder de los microprocesadores informáticos siga aumentando tan significativamente, su precio caerá a un ritmo espectacular, hasta el punto de que un solo transistor que se vendía por 70 dólares a mitad de la década de los sesenta, puede adquirirse ahora por menos de una milésima de centavo.

Por más extraordinario que parezca, esta ley se ha mantenido durante treinta y dos años, mientras nacía el ordenador personal, el ordenador portátil, y los microprocesadores se introducían prácticamente en todos los rincones de la vida electrónica moderna.¹¹

Pero la ley de Moore ya no es válida actualmente. Los desarrollos posteriores la han convertido en obsoleta, como la tecnología del «destello» (*flash*), que permite almacenar más de un dígito en un mismo transistor; o los «megachips»,¹² que operan tres veces más rápido que los microprocesadores actuales más veloces; o los transistores de cuantos, que además de ser más rápidos que los transistores actuales usan mucha menos energía,¹³ o la investigación en microprocesadores incluso más microscópicos basados en mo-

11. John Markoff, «New Chip Make Today's Computer Passe», *New York Times*, 17 de septiembre de 1997.

12. John Markoff, «IBM and Digital to Report on New Super-Ships», *New York Times*, 4 de febrero de 1998.

13. Mark Prigg, «A New Device Based on Quantum Physics Promises a Revolution in Processing Speed», *The Sunday Times*, 22 de febrero de 1998; John Markoff, «Quantum Computers Leap From Theory to a Powerful Potential», *New York Times*, 28 de abril de 1998.

léculas,¹⁴ o, lo último y más espectacular, «nanotubos» hechos de carbono, con sólo unos átomos de diámetro, que pueden aparentemente actuar como semiconductores.¹⁵ A principios de 1998, se dio a conocer la noticia de que «los científicos israelíes son los primeros en haber conseguido que moléculas biológicas individuales formen un circuito eléctrico. Esta simbiosis de biotecnología y electrónica hará finalmente posible la producción de un transistor cien mil veces más pequeño que el tamaño de un cabello humano, y una centésima o menos del espacio requerido actualmente».¹⁶ Los semiconductores de proteínas pueden sustituir finalmente al silicio en ordenadores biomoleculares.¹⁷ No parece que podamos vislumbrar aún el fin de esta constante miniaturización del poder de los ordenadores, y es posible que ya hayamos superado nuestra capacidad práctica para usarlos de inmediato con su máxima potencia.

Otra innovación clave de la década de los setenta fue el desarrollo de los microordenadores u ordenadores personales (PC), comercializados al final de la década, al mismo tiempo que aparecían en el mercado diversos sistemas operativos. Diez años más tarde, el mercado ya ofrecía todo tipo de software, procesadores de texto, hojas de cálculo, programas de diseño gráfico o los más variados juegos, al mismo tiempo que emergían los ordenadores portátiles, potentes y móviles cuadernos de notas, capaces de viajar por cualquier parte. Hubo un desplazamiento desde los ordenadores con un valor económico muy alto, asociados estrechamente a organizaciones jerárquicas (Estados, grandes empresas y vastas instituciones) y usados exclusivamente por autoridades y directivos, hasta una tecnología de consumo relativamente económica y ampliamente difundida, que podía ser espontáneamente orientada hacia las tareas de todo tipo de usuarios: la democratización de la informática.

14. John Markoff. «Tiny Magnets May Bring Computing Breakthrough». *New York Times*, 27 de enero de 1997.

15. Malcom W. Browne. «Next Electronics Breakthrough: Power-Packed Carbon Atoms». *New York Times*, 17 de febrero de 1998.

16. Judy Siegel. «Technion Scientists 'Coax' Molecules to Form Electric Circuit». *Jerusalem Post*, 19 de febrero de 1998.

17. Robert L. Birge. «Protein-based computers». *Scientific American*, marzo de 1995, págs. 90-95.

El próximo paso provino de la inesperada colaboración entre la investigación militar de la Guerra Fría¹⁸ y la contracultura norteamericana. La primera red de ordenadores conectados fue el resultado de una investigación del Departamento de Defensa norteamericano, en 1969, llamada Arpanet. Tal red horizontal resultó ser irresistiblemente atractiva para los que conocieron sus ventajas y, a principios de la década de los ochenta, aunque aún bajo los auspicios del Departamento de Defensa, se había convertido en una red más científica que militar, engendrando otras redes que usaban Arpanet como plataforma comunicativa: el resultado fue llamado finalmente Internet. Tales desarrollos aún se centraban, sin embargo, alrededor de vastos núcleos institucionales: gobiernos, organizaciones militares y centros de investigación universitarios. Pero apareció la contracultura. A finales de la década de los setenta, dos estudiantes universitarios inventaron el módem y difundieron ampliamente, y sin costes, los protocolos que permiten transferir archivos entre ordenadores sin pasar por un servidor. Otros estudiantes, en 1979, crearon el protocolo que permite conectar varios ordenadores mediante el teléfono. Las redes espontáneas crecieron entonces juntas, dando lugar a la verdadera red de todas las redes, Internet, que se expandió rápidamente por todo el mundo. Lo que había empezado bajo el manto de la investigación militar durante la Guerra Fría se había desbordado de sus confines, convirtiéndose en algo sin ningún tipo de precedentes: un sistema nervioso de comunicación internacional generado por redes constantemente creándose y recreándose.

Llegados a este punto, entra en juego la segunda corriente fundamental de innovaciones tecnológicas: las capacidades de transmisión. La información digital se mueve a través de varios medios de comunicación, básicamente vía cables o mediante el espectro electromagnético. Las innovaciones en estas áreas han permitido un importante incremento de los datos transmitidos (el «ancho de banda») y de la velocidad de transmisión. El cable de fibra óptica ya puede transmitir mil veces más bits por segundo que el antiguo cable telefónico, pero aún se desconocen sus límites reales. Las transmisiones

18. Para un excelente análisis de cómo los ordenadores se desarrollaron dentro de los términos del discurso de la Guerra Fría al mismo tiempo que daban forma a este mismo discurso, véase Paul N. Edwards, *The Closed World: Computers and the Politics of Discourse in Cold War America*, Cambridge, Massachusetts, The MIT Press, 1996.

por microondas y por señales electromagnéticas «rebotadas» mediante satélites son otras de las importantes áreas aún pendientes de una mayor explotación y desarrollo.

Ambas corrientes de innovación tecnológica se han desarrollado en una trayectoria exponencial y explosiva, pero es en esta fusión de los ordenadores con la telecomunicación (la Red) donde reside el verdadero potencial revolucionario. Así como las capacidades de la mente humana aumentan considerablemente su capacidad de almacenar, clasificar, recuperar y manipular grandes cantidades de información mediante microprocesadores cada vez más pequeños, más rápidos y más poderosos, el alcance comunicativo de los individuos se incrementa de forma desmesurada mediante el cable de fibra óptica y la comunicación vía satélite, para formar una red de comunicación en tiempo real con todos los ordenadores.

Esta fusión tecnológica ha creado literalmente un nuevo mundo, un nuevo espacio: el ciberespacio, que existe en ninguna parte y en todas partes,¹⁹ y que consiste en una especie de *tabula rasa* en el sentido de que se construye y se reconstruye constantemente, se escribe y se reescribe mediante la interacción simultánea de todos los usuarios de la Red y su consiguiente reelaboración de la misma. El descubrimiento de un mundo con tales características, y otras muchas, un mundo aparentemente plástico, está determinado a hacer surgir lo *faústico* de aquellos que entrevén por primera vez sus contornos expansivos y aparentemente sin límites:

Luego me sentí como algún vigilante de los cielos
cuando un nuevo planeta se desliza al alcance de su vista.²⁰

Junto a Fausto, demos al diablo lo que es suyo: las posibilidades son ilimitadas y embriagadoras, el espacio y la distancia, ya reducidas mediante técnicas como el teléfono, se disuelven en el ciberespacio. La gente puede comunicarse con independencia de su localización física: las comunidades (¿sistemas de comunicación?)

19. Véase Julian Stallabrass, «Empowering Technology: The Exploration of Cyberspace», *New Left Review*, 211, mayo/junio de 1995, págs. 3-32.

20. «Then felt like a watcher of the skies / When a new planet swims into the ken» (John Keats, *La primera mirada al Homero de Chapman*, en *Poesía completa*, edición bilingüe, trad. de Arturo Sánchez, Barcelona, Ediciones 29, 1975, págs. 124-125).

pueden trascender no sólo su localidad, sino incluso aspectos artificiales como la nación o las fronteras políticas; las «comunidades virtuales» reúnen a gente con afinidades comunes independientemente de dónde vivan. Las personas pueden vivir vidas paralelas en las que inventan su propia imagen o representación para la Red (*on-line*); se reinventan a sí mismos en otro mundo paralelo que puede, o no, coincidir con el mundo «real». ²¹ Las relaciones virtuales pueden ser totalmente ajenas a otro tipo de relaciones, incluso incompatibles. Hace un tiempo que se puso de moda entre las chicas japonesas el «amante *tamagotchi*», o amante virtual, que sólo existe en el ciberespacio. ²² Pero no sólo las relaciones humanas pueden alterarse de un modo aún desconocido, la gente que interactúa en el ciberespacio con sus ordenadores también desarrolla fácilmente nociones alteradas de sí misma. Han nacido nuevas formas de expresión a partir de nuevas formas de comunicación, y todo ello conlleva cambios en la conciencia humana. ²³

De los robots a los ciborgs

El ciberespacio ya está haciendo surgir, aquí y ahora, y no en un futuro hipotético, formas artificiales de vida: en los laboratorios informáticos, se han diseñado programas para duplicar entornos concretos, como un océano, en los que se introduce una «especie», como peces, programados para adaptarse a las condiciones cambiantes de su entorno. A medida que pasan las generaciones, las adaptaciones

21. En la novela de Douglas Copland, *Microserfs*, Nueva York. Harper Collins, 1995, que transcurre entre un grupo de ex técnicos de Microsoft que tienen su propia empresa de software, en Silicon Valley, un personaje se enamora mediante el correo electrónico de una corresponsal en Waterloo, en Ontario, de la que sólo conoce la dirección codificada, sin saber nada de su sexo, edad, etc. En la novela, se encuentran y todo funciona bien pero, generalmente, aunque haya ocurrido alguna vez en la vida real, las relaciones ciberespaciales se mantienen, prudentemente como tales.

22. Glenda Cooper, «Cyberpets Superseded as Girls Seek Perfect Boy for Virtual Romance», *The Independent*, 19 de diciembre de 1997.

23. Mark Foster, *The Mode of Information: Poststructuralism and Social Context*, Chicago, University of Chicago Press, 1990; Cherry Turkle, *Life on the Screen: Identity in the Age of the Internet*, Nueva York, Simon & Schuster, 1995, y su anterior *The Second Self: Computers and the Human Spirit*, Nueva York, Simon & Schuster, 1984.

se vuelven bastante independientes del programa original: los peces nadan, comen, se reproducen y mueren en el ciberespacio. No son «reales», no tienen materialidad física y, sin embargo, se comportan como peces reales, interactúan con su entorno y, en definitiva, desarrollan una vida a lo largo de este proceso.²⁴ Instintivamente, tendemos a retroceder ante la idea de que la línea divisoria entre la «vida real» y su réplica «artificial» pudiese volverse borrosa, pero se trata de una de las extraordinarias cuestiones impuestas por las nuevas tecnologías y los nuevos mundos que han hecho emerger.

Otra área de desarrollo remite al «software inteligente». Los programas de software personalizados para las necesidades específicas de un usuario individual son llamados «delegados de software» (*software agents*), ya que actúan en nombre del usuario para llevar a cabo sus tareas. Los delegados de software, también llamados «clones sapientes» o simplemente «clones» (*knowbots or bots*), actúan como representantes digitales en diversos lugares del ciberespacio, simultáneamente, en nombre de sus usuarios. Por ejemplo, un delegado de software relativamente simple consiste en un programa que organiza las citas de su usuario de acuerdo con sus hábitos particulares, escogiendo los horarios que le convengan. El delegado automatiza el proceso, contactando con los futuros participantes de una reunión y llegando a un acuerdo mutuo para fijar el día y la hora. Para llevar a cabo esta tarea, el delegado debe estar programado con la capacidad para aprender y adaptarse a las peculiaridades de los individuos involucrados. Por ejemplo, debe saber que X nunca está disponible para reuniones los martes por la mañana, o que Y tiene una clara preferencia por los viernes. A otro tipo de delegado de software se le puede asignar la tarea de filtrar la voluminosa cantidad de información disponible en la Red según los intereses particulares de sus usuarios, por ejemplo, encomendándole que recoja diariamente de la prensa toda la información relativa al «terrorismo». Si resulta

24. Claus Emmeche. *The Garden in the Machine: The Emerging Science of Artificial Life*. Princeton, Nueva Jersey, Princeton University Press, 1994. Un pez virtual existe realmente en un ordenador de la Universidad de Toronto; véanse Stephan Strauss «Artificial Life», *The Globe and Mail*, Toronto, 10 de septiembre de 1994; Demetri Terzopoulos, Xiayuan Tu y Ralph Greszczuk, «Artificial Fishes with Autonomous Locomotion, Perception, Behavior, and Learning in a Simulated Physical World», en Rodney A. Brooks y Patti Maes (comps.), *Artificial Life: Proceedings of the 4th International Workshop on the Synthesis and Simulation of Living Systems*, Cambridge, Massachusetts, The MIT Press, 1994, págs. 17-27.

que sólo recoge aquellas noticias que contienen la palabra «terror», puedo desear que su búsqueda sea más precisa: un delegado de software inteligente será capaz de «aprender» de sus errores.

Los clones son realmente entrenados para recoger cierto tipo de información. Por ejemplo, alguien puede no haber tenido tiempo de hacer ciertas compras en la Red: los delegados de software pueden ser enviados para investigar las mejores ofertas en la Red, buscando rebajas e incluso regateando los precios. En un futuro próximo, los agentes de Bolsa podrían ser reemplazados por clones de Bolsa, es decir, agentes de bolsa virtuales.²⁵ Lo que resulta especialmente interesante de estos clones informáticos es que aprenden y se adaptan. Tal y como Pattie Maes, considerada como la «reina de los clones» por su trabajo en el Grupo de Delegados de Software de la MIT, ha dicho:

Los programas de los delegados difieren del software regular básicamente porque pueden ser descritos como entidades independientes, con una cierta noción de ellos mismos. Un delegado ideal sabe cuál es el objetivo y se esforzará en conseguirlo. Además, debe ser fuerte y adaptable, capaz de aprender de la experiencia y de responder a situaciones imprevistas con un amplio repertorio de métodos diferentes. Finalmente, debería ser autónomo, de modo que pudiese percibir el estado actual de su entorno y actuar independientemente para alcanzar su objetivo.²⁶

Existe un principio darwiniano funcionando entre los clones informáticos, hasta el punto de que un libro reciente lanzaba la cuestión de si no estamos ante una «nueva especie». Del mismo modo que se ha planteado con los robots, ¿pueden los clones rebelarse o volverse locos? El caso de la multiplicación de Barneys ofrece un ejemplo divertido: en una comunidad virtual de la Red, el ingeniero del programa instaló caprichosamente clones como animación de unos dinosaurios animados de color morado que se paseaban por todas partes cantando: «Te quiero, me quieres, somos una familia feliz». Algunos

25. Carol Alvarez Troy, «Envisioning Stock Trading Where the Brokers Are Bots», *New York Times*, 16 de noviembre de 1994.

26. Patti Maes, «Intelligent Software», *Scientific American*, septiembre de 1995, pág. 85. Véase también Maes, «Agents That Reduce Work and Information Overload», en Jeffrey M. Bradshaw (comp.), *Software Agents*, Menlo Park, California, AAAI Press y The MIT Press, 1997, págs. 145-164.

usuarios se cansaron tanto de los Barneys que empezaron a golpearlos virtualmente, con «patadas» y «puñetazos»: «Cada vez que un Barney se rompía en pedazos, cada uno de ellos se regeneraba en un nuevo Barney, hasta que la comunidad quedó totalmente invadida por ellos».²⁷ Aunque esto pueda parecer cómico, ya no es tan divertida la inquietante idea de delegados inteligentes y adaptables circulando por el ciberespacio, aprendiendo y evolucionando de forma autónoma. Todo ello puede conllevar cuestiones morales y legales: ¿cuáles son las obligaciones de un usuario por las acciones cometidas por su delegado en sus transacciones por el ciberespacio? Una más de las extrañas preguntas que plantea este nuevo mundo.

Tales cuestiones son todavía más perturbadoras si consideramos la disolución de las fronteras entre la biología (lo «natural») y las máquinas (lo «artificial»). La revolución de la información se desarrolla al mismo tiempo que la revolución de la ingeniería genética, cuyo descendiente es la biotecnología. La opinión pública ya se ha sensibilizado frente a algunas de sus trascendentales y perturbadoras consecuencias, especialmente a la posibilidad de la clonación humana, o al cultivo de órganos mediante el cual se mantienen vivas partes independientes del cuerpo para su posterior trasplante. La investigación genética se centra en el desciframiento e interpretación del ADN en tanto que programa, o software, de la vida. Además, la tecnología informática es muy útil para conseguir el plano o programa completo de la estructura genética, por lo que no es ninguna casualidad que ambas revoluciones se hayan desarrollado al mismo tiempo. El proyecto Genoma Humano no terminará su trabajo hasta bien entrado el siglo XXI, ya que de momento sólo se ha llevado a cabo aproximadamente un 2 % de la hercúlea tarea de computación requerida. Cuando termine, será posible «leer» todo el ADN, lo que significa que también podrá «escribirse» ADN, es decir, tener el poder de diseñar vida a partir de especificaciones concretas o, en otros términos, el poder de jugar a ser Dios.

Blade Runner,²⁸ una película de los años ochenta, describe la ciudad de Los Ángeles en el siglo XXI repleta de «replicantes», per-

27. Christopher Lehmann-Haupt, «Cyberspace Through a Darwinian Lens», *New York Times*, 19 de septiembre de 1997, reseña del libro de Andrew Leonard, *Bots: The Origin of New Species*.

28. Dirigida por Ridley Scott, *Blade Runner* se basaba en la novela de ciencia-ficción de Philip K. Dick, *Do Androids Dream of Electric Sheep?* (trad. cast.: ¿Sueñan los androides con ovejas eléctricas?: *Blade Runner*, Barcelona, Edhasa, 1997).

sonas elaboradas genéticamente y diseñadas por la poderosa Tyrell Corporation para sus propios intereses: «Más humanos que los humanos», comenta el diseñador. Los replicantes son esclavos programados para tareas específicas, aunque los últimos modelos desarrollan emociones y se convierten en rebeldes; sólo son contruidos, sin embargo, para un periodo de cuatro años de vida. Raquel es una replicante experimental que se cree humana: ciertos implantes de memoria la han dotado de una infancia y de un pasado que cree verdaderos. Aunque descubre el engaño, se enamora del detective Deckard (un *blade runner* entrenado para cazar y «retirar» a los replicantes peligrosos), que le corresponde. En una escena de caza muy particular, tras mostrarle a Raquel que todos sus recuerdos son implantes de memoria a partir de los cuales ha contruido su identidad, Deckard se queda solo con las fotografías de su propia familia y de su infancia. El espectador se queda con la inquietante sugestión de que el pasado de Deckard podría ser tan falso como el de Raquel. Tanto uno como el otro han contruido su identidad a partir de fragmentos de memoria: ¿acaso las viejas fotografías de Deckard son más «reales» que los implantes de Raquel? De donde sea que proceda, Raquel es una persona humana y autoconsciente, con un carácter y unos rasgos emotivos que atraen a Deckard por su melancólica y salvaje personalidad. En la última escena del filme, Deckard y Raquel huyen de una ciudad de Los Ángeles oscura, decadente y empapada de lluvia ácida. Su compañero detective les llama: «Es una pena que no pueda vivir más, aunque, realmente, ¿quién puede?».

Las tecnologías gemelas de la informática y de la ingeniería genética se orientan al unísono hacia la creación de inteligencia: inteligencia artificial en el caso de la primera, e inteligencia elaborada genéticamente en el caso de la segunda. Aunque se trate de caminos paralelos, son de hecho convergentes. Lo más probable es que el diseño informático se oriente cada vez más hacia la utilización de materiales biológicos, como los microprocesadores de proteínas, tanto respecto del hardware como respecto a las analogías con el cerebro humano (el ordenador más avanzado del mundo, sin un solo compo-

Éste es quizá uno de esos casos en que un filme supera el libro en el que se basa; sin duda ocurrió con relación a su impresionante éxito, que aún resuena tanto tiempo después de su lanzamiento. No es de extrañar que el filme siga siendo un objeto de culto en numerosas páginas *web* de Internet.

nente de silicio), para desarrollar software de inteligencia artificial: la próxima etapa en la escalada del poder informático, Freeman Dyson argumenta convincentemente que mientras la tecnología informática y la ingeniería genética «compitan para lograr el papel fundamental en la revolución industrial del siglo XXI».

ni la una ni la otra tienen muchas probabilidades de ganar. Mientras las estructuras físicas en el corazón de los modernos ordenadores se hacen cada vez más pequeñas, y mientras las estructuras químicas en el corazón de la ingeniería genética se hacen más versátiles, ambas tecnologías empiezan a superponerse y fusionarse. Es probable que los diseños de aparatos inteligentes de energía solar o las máquinas inteligentes de recogida de escombros usen tanto elementos electrónicos como biológicos combinados. La máquina autorreproductiva estará hecha tanto de genes como de enzimas, mientras que el cerebro o los músculos de ingeniería genética también tendrán circuitos integrados y motores eléctricos. Finalmente, los componentes materiales y biológicos estarán tan íntimamente compenetrados que seremos incapaces de distinguir dónde empieza uno y termina el otro.²⁹

Los científicos ya han sido capaces de hacer crecer células nerviosas de rata en un microprocesador de silicio, transmitiendo impulsos eléctricos desde las células al chip. Finalmente, tendría que ser posible conectar directamente las células del cerebro a un ordenador. Los microprocesadores de silicio, por ejemplo, podrían ser implantados en el cerebro, con lo que combinaríamos tipos distintos de inteligencia. El silicio es mejor en el almacenamiento y recuperación de información, así como en procesos de cálculo, mientras que el cerebro humano es más adecuado en el reconocimiento de estructuras y patrones: ¿por qué no investigar si pueden trabajar juntos, produciendo entonces un cerebro «biónico», capaz de combinar lo mejor de la inteligencia cuantitativa y cualitativa?³⁰

29. Freeman Dyson, *Imagined Worlds*, Cambridge, Massachusetts, Harvard University Press, 1997, págs. 120-121.

30. Steve Connor, «Brain Chip Signals Arrival of Bionic Man», *Sunday Times*, 16 de noviembre de 1997; Sandeep Junnarkar, «GeneChip Encodes DNA on Silicon», *New York Times*, 15 de marzo de 1997; Sandra Blakeslee, «Bionic Ship Built to Aid Brain Study», *New York Times*, 2 de diciembre de 1997.

Desde finales de la década de los cuarenta hasta mediados de los sesenta, la imaginación occidental concibió los ordenadores como máquinas de cálculo, y después como robots, máquinas capaces de pensar y de actuar. Los robots ya no esperan pasivamente las instrucciones humanas: como las personas, pueden moverse y actuar realmente en el mundo, pero, a diferencia de la inteligencia humana, la de los robots podía ser asignada a las tareas más rutinarias, repetitivas y peligrosas sin rechistar. Tales aplicaciones prácticas de los robots se han dado en todos los ámbitos: ¿acaso no son los robots de montaje en cadena más eficientes que los trabajadores humanos, además de no requerir tantas atenciones en su manejo? Los robots no se cansan, ni se aburren, ni cometen errores, aspectos en los que fácilmente incurrieran sus contrapartidas humanas. Las faenas más agotadoras del hogar podrían ser encargadas a robots mayordomos o cocineros. También las tareas más peligrosas y desagradables —como la extracción de materiales en las minas, por ejemplo, o las limpiezas tóxicas o la eliminación de bombas— pueden ser desarrolladas con más seguridad y eficacia por los robots.

Los robots fueron tan bienvenidos como temidos. Bienvenidos puesto que prometían eliminar las tareas más pesadas y monótonas, así como facilitar el trabajo y la vida. Temidos porque podían quizás eliminar todo el trabajo humano y adueñarse del mundo. Cuando los robots empezaron a utilizarse, circulaba entre los científicos informáticos el chiste siguiente: en algún punto del futuro lejano, todos los ordenadores de la galaxia se conectan en serie. Cuando la conexión permite activar el superordenador definitivo, la primera pregunta que se le introduce es la eterna cuestión que siempre ha obsesionado a la humanidad: ¿existe Dios? El cielo se oscurece y los truenos resuenan al emerger la respuesta: «AHORA existe». La ciencia-ficción de la década de los cincuenta contenía numerosas historias espeluznantes de los robots triunfando sobre la humanidad. Generalmente, eran descritos en tanto que analogías humanas, pero caricaturizadas: personajes a menudo metálicos, con brazos, piernas y cabezas, más listos y poderosos que las personas, pero sin emociones, sin un atisbo de pasión, amor u odio, sentimientos tan presentes en las personas reales. Es como si los robots fueran escalofrantes encarnaciones de las capacidades *prometeicas* de la humanidad para evocar los poderes de la ciencia y de la racionalidad matemática, que rompían con sus obligaciones y se convertían en una ame-

naza. Seguramente no fue una coincidencia que la amenaza del robot coincidiese con la era atómica. Cuando J. Robert Oppenheimer, el «padre de la Bomba», fue testigo de la inmensa y siniestra nube que se elevó por encima de la primera prueba atómica en Alamo-gordo, en 1945, le vino a la mente este verso del *Bhagavad Gita* hindú:

Me convierto en la Muerte, el más destruido de todos los mundos.³¹

Los robots también eran temidos como mensajeros de la muerte: la ciencia y la razón enloquecían atacando indiscriminadamente a la gente; la muerte como el triunfo del metal sobre la carne; la muerte como la victoria de lo frío e inerte sobre lo cálido y lo vital.

La descripción definitiva del robot como comerciante de la muerte remite al filme de los sesenta, *2001: Odisea del espacio*, en el que el famoso HAL, el ordenador con voz sintética que cuida de la nave espacial en dirección a Júpiter, decide que la tripulación le está entorpeciendo y empieza a matarla metódicamente.³² El papel de HAL es fundamental, ya que es descrito como omnipotente, con ojos y orejas panópticos, y una mente esencial para el funcionamiento de la nave y de sus habitantes. La arraigada presencia de Hal señala una comprensión más contemporánea de la inteligencia artificial. Mientras la revolución de la información prosiga en el siglo xx, será cada vez más difícil concebir la oposición entre el hombre y la máquina tal y como ocurría en el pasado: el «ordenador» como unidad discreta —CPU, pantalla, teclado y otros accesorios— que se instala en un escritorio o encaja en una maleta portátil, está condenado a seguir los pasos de todas las tecnologías obsoletas. El futuro nos depara el «ordenador ubicuo», la inteligencia arraigada y diseminada por nuestros entornos laborales y vitales.³³ Las tarjetas inteligentes, como las tarjetas de crédito con información insertada en un microprocesador, o los carnés de identidad con información personal, sólo

31. Robert Jungk, *Brighter Than a Thousand Suns: A Personal History of the Atomic Scientists*, Harmondsworth, Middlesex, Penguin, 1960, pág. 183.

32. David G. Stork (comp.), *HAL's Legacy: 2001's Computer as Dream and Reality*, Cambridge, Massachusetts, MIT Press, 1998.

33. Vinton G. Cerf, «When They're Everywhere», en Peter J. Denning y Robert M. Metcalfe (comps.), *Beyond Calculation: The Next Fifty Years of Computing*, Nueva York, Springer-Verlag, 1997, págs. 33-42.

son el principio: coches inteligentes, oficinas inteligentes, escuelas, fábricas y casas inteligentes, son algunos de los entornos en los que no habrá ordenadores aislados, pero el poder del ordenador estará en todas partes. Ya están apareciendo incluso materiales de construcción inteligentes que permiten, por ejemplo, construir puentes capaces de detectar la velocidad del viento y ajustar la tensión estructural automáticamente, o usar pinturas que rezuman protectores de fuego cuando detectan demasiado calor.³⁴ Este futuro también puede inspirar terror: en la novela de suspense y ciencia-ficción de Philip Kerr, *The Grid*,³⁵ de 1995, un edificio inteligente de Los Ángeles es vigilado y mantenido por una inteligencia artificial que, al igual que HAL, se convierte en un malévolo asesino. Pero tales miedos pueden ser reacciones atávicas, que asignan este antropomorfismo por fracasar la imaginación ante el reto de nuevas realidades sin precedentes en nuestra experiencia pasada.

Mientras desaparece la antigua imagen del robot, emerge la nueva figura que lo sustituye, un engendro situado en la intersección de las nuevas tecnologías y de la imaginación: el ciborg, mitad máquina y mitad hombre, quizás incluso con una parte animal. El concepto de ciborg se basa en el hecho de que, en palabras de Donna Haraway:

No existe ninguna separación fundamental, ontológica, entre nuestro conocimiento formal de la máquina y del organismo, de lo tecnológico y de lo orgánico [...] Una de las consecuencias es el incremento de capacidades que sentimos en la relación con nuestros instrumentos y herramientas [...] ¿por qué debería nuestro cuerpo acabarse en la piel, o incluir como máximo otros seres también encapsulados en piel? Desde el siglo XVII hasta nuestros días, las máquinas han cobrado cierta animación, con almas fantasmales que les permiten hablar o moverse, y dar cuenta de su desarrollo obediente y de sus capacidades mentales. También los organismos podían ser mecanizados, reducidos a un cuerpo en tanto que recurso de la mente. Tales relaciones entre la máquina y el organismo se han vuelto obsoletas, innecesarias. Para nosotros, tanto en la imaginación como en otras prácticas, las máquinas pueden

34. John Markoff, «New Wave in High-Tech: Deus Ex (Tiny) Machina», *New York Times*, 27 de enero de 1997.

35. Nueva York, Bantam Books, 1997. Originalmente publicado en Inglaterra, 1995, con el título *Gridiron* (trad. cast.: *El infierno digital*, Barcelona, Anagrama, 1997).

ser dispositivos protésicos, componentes íntimos, personalidades amistosas.³⁶

El ciborg ya es un estereotipo cultural: la película y la serie televisiva *RoboCop* describe una figura mecánica, parecida a un robot, con poderes sobrehumanos. Pero, oculto dentro del *RoboCop*, hay un ser humano que ha sido reconstruido con extensiones mecánicas para convertirse en el ser vivo más grande, más rápido y más mortífero. También ha perdido algo de su humanidad, ya que su identidad original se perdió y sólo fue recuperada parcialmente para su nueva coraza mecánica. Frente a la relativa simplicidad de este vehículo para fantasías violentas masculinas, son más complejas las variaciones con las que han jugado los filmes *Terminator* y *Terminator II*, en la que los ciborgs del futuro vuelven a las décadas de los ochenta y los noventa para volver a escribir el pasado, y asegurarse así la victoria de la inteligencia artificial respecto a la inteligencia humana. El *Terminator* original (Arnold Schwarzenegger) es una criatura parecida a un robot programada para matar, pero en *Terminator II* vuelve a ser programado para convertirse en un «buen chico», aunque ahora deberá enfrentarse a un ciborg del futuro más avanzado y mortífero, que encarna la fusión de la máquina con lo biológico: es capaz de transformarse sin ningún esfuerzo, por mimetismo, en cualquier forma existente, ya sea humana u objetual.

La cultura popular se ha apropiado generalmente del ciborg en tanto que una versión del robot puesta al día, distinto y en contra de los humanos «normales y naturales». Pero aunque los viejos estereotipos tardan en morir, existen otros modos de asimilar más íntimamente al ciborg en la estructura de nuestro propio conocimiento de nosotros mismos. La escritora feminista Donna Haraway desarrolló, en la década de los ochenta, la noción del ciborg como una especie de figura antirracista, blasfema y feminista.³⁷ El ciborg como símbolo de la desaparición de los límites y de las fronteras,

36. Donna J. Haraway, «A Cyborg Manifesto: Science, Technology, and Socialist-Feminism in the Late Twentieth Century», en Haraway, *Simians, Cyborgs, and Women: The Reinvention of Nature*, Nueva York, Routledge, 1990. Véase también Scott McCracken, «Cyborg Fictions: The Cultural Logic of Posthumanism», en Leo Panitch (comp.), *Socialist Register 1997: Ruthless Criticism of All That Exists*, Londres, Merlin Press, 1997, págs. 288-301.

37. Haraway, «A Cyborg Manifesto».

como forma que desafía una concepción fija de la «naturaleza», del género y de la raza, ofrece una visión multicultural muy sugestiva (aunque pueda ser utilizada por el capitalismo para vender la pluralidad cultural en un sentido más superficial).

También puede entenderse el ciborg en términos ecológicos: no somos criaturas autónomas encapsuladas en nuestro interior e independientes del exterior; por el contrario, estamos integrados en un amplio ecosistema social en el que se combinan elementos humanos y naturales, así como extensiones «artificiales» de la humanidad, en un entramado cibernético y relacional, y el ciberespacio es la plataforma en la que más visiblemente interactúan tales aspectos. William Gibson describe mejor que nadie estas cuestiones en su breve cuento «The Winter Market».³⁸ Lisa es/era una mujer, pero cuando Casey, el héroe de Gibson, la encuentra por primera vez, ya es una mujer ciborg, con su cuerpo enfermo y podrido por las drogas, encapsulado en un dermatoesqueleto de policarbono que le permite moverse y actuar (con dificultad) en el mundo. Se conocen en una fiesta y Lisa acepta irse con él a su casa. Aunque Casey rechaza su oferta sexual, les espera una relación mucho más íntima. Casey es el director de una empresa de sueños, reconstruidos con la tecnología de la realidad virtual para venderlos como productos a una inmensa sociedad mercantil multimedia. Los artistas de tales sueños se han convertido en estrellas pop internacionales. Lisa se encuentra convertida en una superestrella gracias al éxito descomunal de su sueño *Kings of Sleep* (*Reyes del sueño*), mientras Casey se debate entre la atracción y la repulsión en su relación con ella. Como su público, está enamorado de sus sueños, pero su relación con la Lisa «real» se mantiene distante, incómoda y ajena al sexo. Lisa sigue destrozando su ya decadente cuerpo con el abuso masivo de drogas, como si odiase la parte biológica de la que aún dispone. Luego, Casey descubre, gracias a la sociedad mercantil, que «se ha fusionado con la Red, cruzando realmente la frontera». Lisa, abandonando finalmente su cuerpo, es introducida en el ciberespacio, por lo que ya no está ni muerta ni viva, en el sentido convencional. Casey recibe la advertencia de que Lisa se pondrá en contacto con él en un futuro próximo,

38. «The Winter Market», en William Gibson. *Burning Chrome*, Nueva York, Ace Books, 1987 (trad. cast.: *Quemando cromo*, Barcelona, Minotauro, 1994).

cuando tengas que coordinar la próxima entrega, lo que sin duda ocurrirá pronto, ya que necesita urgentemente dinero. Está tomándose grandes cantidades de ROM del procesador central de una multinacional, y los beneficios de *Kings* no podrán alcanzar para cubrir todo lo que ha costado tenerla situada allí.

Casey, aturdido, pregunta: «Si me llama, ¿será *ella*?». La respuesta: «Sólo Dios puede decirlo. Quiero decir, Casey, que la tecnología está ahí, entonces, ¿quién, tío, realmente quién puede saberlo?». Se trata sin duda de una parábola moral para la era del ciberespacio: la inmortalidad es posible, pero sólo mediante un acto de mercantilismo definitivo.

Ciencia sombría en la biblioteca de Babel

La biblioteca de Babel de Borges se presenta a sí misma como el universo pero, evidentemente, no se trata realmente del «universo», ni su arquitectura remite a la de la materia. Se trata de un «universo» analógico: sus anaqueles almacenan información bajo forma de textos que contienen «datos», que reflejan o reproducen el universo material. La naturaleza de la biblioteca de Borges existe *ab aeterno*. La arquitectura de la información es demasiado compleja y elegante para ser un producto del hombre, el «bibliotecario imperfecto». No podemos olvidar que la información es sobre algo, ya sea Dios o la Naturaleza, y no algo en sí misma. Pero esta cuestión puede oscurecerse cuando centramos nuestra atención en la biblioteca misma. Borges también afirma que «el número de símbolos ortográficos es veinticinco» (las letras del alfabeto más el punto, la coma y el espacio), lo que ha permitido formular una teoría general de la biblioteca. En consecuencia, todos los libros constan de elementos iguales, aunque «no hay, en la vasta biblioteca, dos libros idénticos. De esas premisas incontrovertibles [puede deducirse] que la biblioteca es total y que sus anaqueles registran todas las posibles combinaciones de los veintitantos símbolos ortográficos...». En otros términos: «Todo lo que es dable expresar: en todos los idiomas. Todo: la historia minuciosa del porvenir...».

Cuando se proclamó que la biblioteca abarcaba todos los libros, la primera impresión fue de extravagante felicidad. Todos los hombres se sintieron señores de un tesoro intacto y secreto. No había problema personal o mundial cuya elocuente solución no existiera: en algún hexágono. El universo estaba justificado, el universo bruscamente usurpó las dimensiones ilimitadas de la esperanza.

Por consiguiente, nuestra propia era del «infobombo»: la promesa ilimitada de un estupendo Internet, la encarnación de la biblioteca de Borges condensada en millones de pantallas de ordenador individuales en tanto que ventanas abiertas al ciberespacio, una «esfera cuyo centro cabal es cualquier hexágono, cuya circunferencia es inaccesible». No se trata de pequeñas minucias: las promesas del diablo son prometedoras, y no es de extrañar que el canto de la sirena se haya llevado a tantos. Pero, un momento... el ciberespacio no es otro universo en el que podamos escaparnos como a través de una puerta mágica. Los mundos ideales existen en la mente de los soñadores que, sin embargo, viven en *este* mundo, respiran, comen cuando tienen hambre, beben cuando tienen sed, o no, según sus circunstancias materiales. El ciberespacio también es un mundo «ideal», pero los soñadores sólo acceden a él mediante el hardware informático, los cables de fibra óptica, los complejos sistemas de telecomunicación y de la Red, así como los sistemas sociales y económicos que mantienen y comercializan estas tecnologías. Los cibernautas están *conectados* en más de un sentido. Existe, o debería existir, una *economía política* del ciberespacio. Incluso en el delirio flotante de este nuevo mundo, la vieja ciencia, penosa y sombría, como la gravedad, vuelve a situar a los cibernautas con los pies en la tierra.

Hay que mencionar ciertos hechos incómodos pero inevitables: la mayoría de la gente del mundo real no sólo no tiene ordenador, sino que tampoco tiene acceso telefónico y, para una gran mayoría, la revolución de la información no es ni tan siquiera un rumor; las llamadas autopistas de la información, que el vicepresidente norteamericano Al Gore promociona como un pregonero carnavalesco, podrían ser inauguradas como una inmensa autopista de peaje para las clases más adineradas de Norteamérica, Europa y las zonas ultra-desarrolladas de Asia pero, al alcanzar África, América Latina y las partes menos desarrolladas de Asia, podría reducirse a unos delgados hilos en manos de algunas islas privilegiadas; seguramente, para

la mayoría del Tercer Mundo, simplemente se detendrían.³⁹ No hay ninguna razón para pensar que la revolución de la información pueda ofrecer una solución mágica al endémico problema de la pobreza y el subdesarrollo, sino que más bien puede ser el nuevo nombre que reciba la perpetua y cada vez más profunda dominación de muchos pobres por unos cuantos ricos. El acceso a Internet puede ser de tanta ayuda para los campesinos de Bangladesh como ser recogidos en autostop en el último Challenger enviado al espacio; pero es sin duda útil para las empresas multinacionales que gobiernan el sistema de la economía internacional, que sigue manteniendo Bangladesh como un gueto de miseria.

Lo mismo ocurre en las mismas sociedades occidentales. Un razonable y actual ordenador *clónico*, con software pirata, módem y el abono anual de conexión a Internet, quizá no representen una gran inversión, pero ya excluyen a mucha gente, del mismo modo que el contexto específico de la cultura informática. El resultado es que Internet tiene decididamente un aspecto de clase media. Además, sus usuarios tienden de forma desproporcionada a ser masculinos, blancos y el resto de las categorías privilegiadas. Sin duda tales tendencias pueden cambiar con el tiempo pero, del mismo modo que con el subdesarrollo del Tercer Mundo, hay muchas ideas sobreexcitadas flotando en círculos políticos y burocráticos (como en la mente frenética de Newt Gingrich) que aseguran que un ordenador en cada co-

39. Un estudio reciente indicaba que hay alrededor de 3,4 millones de ordenadores conectados a Internet en Estados Unidos (el 70 % del total internacional) y alrededor de medio millón en Europa occidental. En contraste, África sólo tiene 27.100, América del Sur y Central 16.000 y el Extremo Oriente 13.800. Un informe de una fundación no gubernamental advertía sobre una nueva forma de pobreza, «la pobreza de la información», que amenaza el desarrollo del mundo: «Existe el peligro de un nuevo elitismo de la información que excluya a la mayoría de la población mundial [...] La tecnología podría de hecho aumentar el desfase entre ricos y pobres» (Mark John, «Third World Faces Information Poverty-report», Reuters, Londres, 11 de octubre de 1995). Incluso este informe puede errar el grado de dominación de Internet por los usuarios norteamericanos: tras sus pasos llegó otro informe mostrando que el número de norteamericanos que usan ordenadores conectados a Internet se disparó en la primera mitad de 1995 hasta 12 millones: «On-line services», AP, Nueva York, 15 de octubre de 1995. Los resultados preliminares de otro informe de 1997 muestran que el 45 % de los hogares norteamericanos tienen ahora un ordenador personal, es decir, el 80 % de aquellos hogares con un ingreso anual superior a 100.000 dólares (*Computer Intelligence*, 1998, Consumer Technology Index, CT 198).

cina resolvería de algún modo los problemas del desempleo o de la decadencia económica regional. Desde luego, queda descartada la posibilidad de que el ala derecha de la política neoliberal, algunos de cuyos representantes balbucean sobre el poder transformador de los ordenadores, pueda ingeniar y ejecutar, así como subvencionar, un proyecto con muchos puestos de trabajo que repartiese el hardware y el software necesario entre los pobres y los desempleados. Desgraciadamente, los socialdemócratas, quizá por ser menos utópicos, han sido igualmente cómplices en promocionar el ordenador como un aumento de las capacidades. Incluso los moderados proyectos lanzados por gobiernos socialdemócratas para «reeducar» (una plegaria de las crisis contemporáneas del capitalismo) a los pescadores innecesarios por el agotamiento de las existencias, a los mineros del carbón con las minas cerradas o a los trabajadores con habilidades vinculadas a industrias pesadas en vías de desaparición, con una formación en «informática básica», lo cual ha mostrado rápidamente su limitado alcance. En el mejor de los casos, tales trabajadores reeducados podrán tener acceso instantáneo a una inteligencia en la que no hay puestos de trabajo disponibles; al menos podrán compartir las colas del desempleo y tener unas mínimas relaciones humanas con otros en situaciones parecidas, aunque al final el resultado sea el mismo.

La atracción de los neoliberales por el «infobombo» tiene muy poco que ver con una redistribución de la riqueza y el poder. El ordenador como «incremento de capacidades» es una estupenda y ambigua pieza de retórica, además de ofrecer una conveniente y moderna razón para el recorte drástico del sector público: ¿quién necesita ejércitos de trabajadores en el sector público para servicios de asistencia si los clientes del Estado ya tienen la posibilidad de conectarse directamente? ¿Quién necesita hacer importantes inversiones en infraestructuras materiales y en mantenimiento si los servicios son directamente accesibles en la Red? Los políticos norteamericanos de derechas, cansados de ver cómo el dinero de los impuestos recae en universidades e institutos de investigación, han empezado a proponer la «universidad virtual», en la que se ofrecen cursos a los clientes (antiguamente llamados estudiantes), que reciben información diseñada por programadores (antiguamente llamados profesores), hacen sus deberes y pasan sus exámenes sin apartarse nunca de sus ordenadores caseros. En la visión apoteósica de esta propuesta, todo el equipo de ayuda y mantenimiento, así como

la mayoría de los profesores y del aparato administrativo, podría ser descontado del gasto público, y el emplazamiento material (antiguamente llamado campus) podría ser vendido al sector privado para un uso más productivo y rentable. Se trata de un paradigma para otros proyectos como el «sector público virtual» o el «Estado virtual». Como en la realidad virtual, los usuarios permiten que sus sentidos les engañen para creer que, de algún modo, están en un lugar en el que realmente no están, que están haciendo cosas que realmente no ocurren: el opio de las masas, sin duda.

Existe una ideología entre los cibernautas actuales, especialmente los norteamericanos, que puede ser calificada como capitalismo fronterizo o individualismo duro. Su propia imagen remite al colonizador solitario explorando los confines de la civilización, armado con el equivalente contemporáneo de un revólver de seis tiros, el módem de alta velocidad; siente una poderosa aversión por sus enemigos tradicionales: los gobiernos y sus intentos de regular y domesticar las energías salvajes. Por ello han habido feroces reacciones a los torpes intentos de la Administración Clinton para imponer una vigilancia en Internet desde el «microprocesador del tijereteo», así como para embargar la exportación de varios programas para cifrar información; a los toscos intentos del FBI para imponer la intervención de la comunicación digital (¡y hacer pagar a los usuarios por este privilegio!); a las iniciativas para censurar desde varias instancias gubernamentales la pornografía y la apología de la violencia (*hate mail*) en el ciberespacio.⁴⁰ Probablemente se trate de respuestas razonables bajo las circunstancias actuales, pero constituyen ejemplos clásicos de conducción con el espejo retrovisor.

Ni el liberalismo individualista de las empresas ni el intervencionismo agresivo del Estado constituyen nuevas políticas económicas pertinentes para el ciberespacio. Tanto el hardware como el software son producidos por gigantescas multinacionales como IBM o Microsoft, y la infraestructura de Internet es actualmente el meollo de las disputas entre los gigantes del teléfono, del cable y de otros accesorios comunicativos. La verdadera frontera reside en la mercantilización de la información por el capital. Para cambiar de registro metafórico, el ciberespacio es como si los miembros de la Cámara de los Comunes fueran atacados por recintos. El incansable

40. Véanse los capítulos 4 y 6.

énfasis de los últimos años en la «propiedad intelectual», en tanto que elemento crucial de los acuerdos sobre comercio internacional, señala claramente la dirección tomada por la llamada revolución de la información. La arquitectura del ciberespacio podría muy bien asemejarse a la visión ficticia de William Gibson:⁴¹ vastas y misteriosas colecciones de datos tejiendo impresionantes fortalezas, ferrozmente protegidas por las mayores multinacionales, mientras que el «mundo real» se revuelca en la miseria urbana, la criminalidad mezquina, la violencia y el escapismo de oropel.

Del macro al micro

La información es un recurso cuya relación con el capitalismo de este fin de siglo es parecida a la que tuvo el petróleo con el capitalismo en los inicios de este mismo siglo, lo cual no quiere decir, como algunos han extrapolado imprudentemente, que el capitalismo industrial haya muerto. Los automóviles aún constituyen el medio de transporte fundamental para gran parte del mundo, y el petróleo aún debe ser refinado para abastecer su voraz apetito de combustible. La información no ha reemplazado a los viejos recursos, así como el postindustrialismo no ha reemplazado al industrialismo. Pero los ordenadores y las nuevas tecnologías de la comunicación han reestructurado los modos de producción y de distribución. La producción y el consumo en masa, en la trayectoria de su promesa de crecimiento, se han transmutado. La producción (incluyendo los servicios) requiere menos trabajadores y una mayor «flexibilidad», y el consumo masivo de productos, comercializados por un marketing a gran escala, es progresivamente igualado por un marketing *niche* de productos específicamente orientados a sus clientes potenciales. En ambos lados de la ecuación, tanto la información como su comunicación a alta velocidad son recursos cruciales. El desplazamiento desde la producción primaria hacia el sector de los servicios que requieren mucha información, tan evidente en los países industrializados y ricos, es otra señal de este mismo cambio. El control de la información y de su transmisión será la llave del éxito en el mundo capitalista del futuro.

41. William Gibson, *Neuromancer*, Nueva York, Berkley, 1984 (trad. cast.: *Neuromante*, Barcelona, Minotauro, 1998).

La idea de que este recurso crucial podrá convertirse en un bien público es un idealismo equiparable a la necesidad.⁴² Así que los miembros ciberespaciales de la sala de los Comunes son encerrados en un recinto tan rápidamente como se expande el espacio. Los abogados de la «libertad electrónica» tienen sus corazones en el lugar adecuado, pero sus cabezas enterradas bajo tierra. Los jóvenes piratas informáticos, que para su propia diversión y beneficio irrumpen en las oscuras torres de información que tejen sus redes por encima del mundo cableado, están más cerca de la realidad actual. Durante el cuestionado ataque de Estados Unidos a Iraq a principios de 1998, un «ciberasalto» conjunto a las bases de datos del Pentágono hizo saltar la alarma de una «infoguerra» impulsada por los enemigos de Norteamérica: resultaron ser dos piratas informáticos adolescentes. Cuando uno de ellos, con el apodo de Makaveli, fue interrogado sobre sus motivaciones políticas, respondió con menosprecio: «Es poder, tío, ya sabes, poder»,⁴³ lo que presumiblemente quería decir poder en sí mismo, sin ningún otro motivo. El mentor de Makaveli, un joven israelí que se hacía llamar «el Analista», fue elogiado por el primer ministro de Israel, Benjamin Netanyahu, y considerado en su país, por mucha gente, como un héroe popular. En una entrevista, «el Analista» declaró que «odiaba» a las grandes organizaciones y a los gobiernos, y sugería el «caos» como una buena alternativa de gobierno.⁴⁴ Pero incluso estos recientes bandoleros de la información son algunas veces absorbidos por las mismas organizaciones a las que han apuntado con éxito: tras penetrar su sistema de seguridad electrónica, son contratados como perspicaces guardas de seguridad para mantener alejados a otros posibles piratas informáticos, y quizás... ¿para intentar introducirse en los sistemas de seguridad de la competencia? Ya estamos entrando en una nueva era que deja tras

42. Para un ejemplo de lo insípida que puede ser cualquier discusión de estos temas que evite o ignore la realidad subyacente de la propiedad capitalista de la información, véase Anne Wells Branscomb, *Who Owns Information? From Privacy to Public Access*. Nueva York, Basic Books, 1994. Después de 186 páginas discutiendo la pregunta del título sobre la propiedad de la información, concluye con una banalidad sobrecogedora que «nosotros [?] construiremos el tipo de "infoestructura" legal que nosotros [?] necesitamos y queremos» (pág. 186).

43. James Glave, «Pentagon "Hacker" Speaks Out», *Wired News*, 3, marzo de 1998.

44. Rebecca Trounson, «Hacker Case Taps Into Fame, Fury», *Los Angeles Times*, 27 de abril de 1998.

de sí la frontera del pirateo individualista: la guerra electrónica organizada, con grupos disciplinados y corporativos de piratas informáticos situándose sistemáticamente para romper o sabotear los bancos de datos o el software operativo de los competidores económicos puede convertirse en el pan de cada día.⁴⁵ El mundo de las empresas de datos financieros fue sacudido en 1998 por la noticia de que una investigación federal y secreta de Estados Unidos, que incluía informadores confidenciales y conversaciones registradas, revelaba que un gigante de la información financiera, filial de Reuters, había encargado, presuntamente, a especialistas informáticos robar datos confidenciales de los ordenadores de uno de sus mayores competidores, Bloomberg.⁴⁶ Lo que más sorprendía era la acusación pública contra una firma respetable de servicios financieros, aunque este tipo de ciberespionaje entre multinacionales pueda ser más frecuente de lo que generalmente se admite. Los virus informáticos, transmitidos inicialmente por individuos independientes, por malicia o por el simple placer de la gamberrada, pueden llegar a ser utilizados cada vez más como armas específicamente orientadas a los sistemas informativos de la competencia (la guerra biológica del ciberespacio, atacando las sinapsis de la economía informativa del enemigo).⁴⁷ Existe una creciente literatura sobre la «infoguerra» como una nueva frontera de las hostilidades internacionales, e incluso un gurú de la nueva ciencia militar: Winn Schwartau.⁴⁸ Las técni-

45. Un informe publicado a principios de 1998 descubrió que «el 64 % o más de quinientas organizaciones señalan una brecha en su sistema de seguridad ocurrido en los últimos doce meses. Se trata de un claro incremento de más del 48 % de las brechas señaladas el pasado año, más el 22 % del año anterior» (Matt Richtel, «Study Finds Rise in Computer Crime», *New York Times*, 5 de marzo de 1998).

46. Kurt Eichenwald, «Reuters Subsidiary Target of U. S. Inquiry Into Theft of Data From Bloomberg», 30 de enero de 1998, y Eichenwald, «Reuters Unit Puts 3 Executives on Paid Leave», *New York Times*, 31 de enero de 1998.

47. En una conferencia sobre «infoguerra», un especialista de la guerra electrónica contó el extraño plan de un grupo de piratas informáticos norteamericanos que, supuestamente motivados por una rabia patriótica frente al espionaje económico francés contra Estados Unidos, pretendía organizar un «asalto electrónico a los principales centros nerviosos de la economía francesa». Aunque aparentemente capaces de infligir daños considerables, el plan fue abandonado cuando el FBI los amenazó con detenerlos: «Dawn of the Infowar Era», *Intelligence Newsletter*, 271, 14 de septiembre de 1994, pág. 1.

48. Matt Richtel, «New Manhattan Project Hopes To Raise Awareness of Hacking», *The New York Times*, 21 de septiembre de 1997; Winn Schwartau, *Informa-*

cas para penetrar y trastocar los sistemas informáticos del enemigo no se limitan necesariamente a los requisitos de los Estados, sino que se adaptan a cualquier competición financiera o empresarial. La amenaza de tácticas de «infoguerra» ya ha provocado la atención creciente hacia medidas de seguridad y protección, como los muros de protección alrededor de los datos. Las áreas de comunicación de los servicios de inteligencia estatales ya están ofreciendo su considerable saber hacer respecto a la protección de la información al sector privado, a precios muy razonables. La sección de protección de la información de la Jefatura de Comunicaciones del Gobierno Británico (GCHQ) puede ahora autofinanciarse mediante los ingresos conseguidos gracias a la venta de sus consejos a las empresas inglesas.⁴⁹ Tales desarrollos no son sorprendentes, atendiendo a las amplias oportunidades de agresión que las nuevas tecnologías permiten, pero dejan muy lejos la «promesa de Internet» relativa a los horizontes ilimitados de la información, dispuestos para que todo el mundo que quiera pueda recorrer sus campos y recoger las flores de la verdad en libertad.

Deberíamos considerar detenidamente por qué la promesa de Internet se ha convertido en este espejismo tan agradable. No se trata de que los capitalistas sean gente endiablada, o de que las multinacionales y las corporaciones conspiren contra los intereses públicos (aunque ambas proposiciones fueran ciertas, quedan fuera de lugar). La información es un producto: los datos «crudos», sin procesar, no son aún información, aunque también exigen ser recopilados y almacenados de forma accesible, por lo que ya existen numerosos pretendientes esperando compensaciones por su trabajo. El procesamiento de esos datos para convertirlos en un producto terminado y útil para consumidores potenciales aumenta considerablemente su valor, lo cual se reflejará en el precio final. Sólo en el sector privado existen los recursos tanto para producir información sofisticada como para adquirir los productos terminados a una escala comercialmente viable. Los servicios de información del sector público podían conseguir en otros tiempos bastante información a precios relativamente bajos pero, en estos tiempos neoliberales, principios del

tion Warfare: Cyberterrorism-Protecting your Personal Security in the Electronic Age, Emeryville, California, Thunder's Mouth Press, 1996.

49. Información confidencial.

mercado tales como «pagar por usar», la recuperación del coste o los servicios orientados a «clientes» específicos, han provocado prácticamente la privatización del sector público de la información. Incluso los otrora bastiones privilegiados de la información secreta del Estado, los servicios de seguridad e inteligencia, están vendiendo sus datos y su información al mejor postor en el sector privado.⁵⁰ Aunque los gobiernos introduzcan mucha información gratuita en Internet, sólo se trata de un mecanismo de legitimación democrática bajo el que se oculta su suministro al sector privado para recuperar los costes: el hecho de que esta información esté disponible para todo el mundo es por lo general una prueba de su valor relativamente bajo en tanto que producto comercial.

El ciberespacio será un tesoro escondido para aquellos que ya posean un tesoro para gastarse. Para el resto de los mortales, puede consistir en un sobrecargado, desordenado, anárquico y desorganizado revoltijo de infobasura, tan poco valioso que incluso se ha descartado su inclusión en las aceras de las autopistas de la información para aquellos usuarios casuales que quisieran recoger o consultar unos de sus curiosos artículos. Con el tiempo, toda esa porquería será limpiada y reemplazada por pequeñas empresas que venderán baratijas y otras ofertas comerciales: los espectadores de televisión, especialmente los norteamericanos, ya han visto este futuro en los canales de venta al público. Incluso *Internet*, tal y como lo conocemos actualmente, puede ser reemplazado por *Intranets* privadas. Las *Intranets* son extensiones de redes locales que usan la misma tecnología telecomunicativa que Internet, pero delimitada a un uso interno y autorizado. Corporaciones transnacionales como Xerox pueden ofrecer todos los servicios comunicativos de la Red a sus empleados, sea cual sea su localización, e incluso ampliar su oferta a solicitantes y clientes dentro de unos límites establecidos, manteniendo fronteras de seguridad. A finales de esta década, las *Intranets* se han hecho tan populares que la instalación de servidores delimitados a un uso interno ya ha superado a la de servidores abiertos a toda la Red. Todo esto señala un futuro en el que los miembros ciberespaciales de la

50. El Estado de Maryland amasó 12.9 millones en 1996 vendiendo accesos a su base de datos, relativa a la administración de los vehículos con motor, a empresas de marketing; véase Rajiv Chandrasekaran, «Door Flung Open to Public Records», *Washington Post*, 8 de marzo de 1998.

Cámara de los Comunes estarán cada vez más encerrados en diversos recintos, hasta el punto de que los miembros ordinarios no podrán entrar a menos que sean socios o que paguen por este privilegio.

La Red como metáfora

Quizás sea un error considerar a la Red como el Internet de la década de los noventa: Internet no es más que una encarnación particular de las posibilidades de las nuevas tecnologías de la información en un momento determinado del desarrollo tecnológico. Lo más probable es que cambie, quizá hasta volverse irreconocible, y más pronto de lo que pudiese esperarse en este mundo febril y darwiniano de las innovaciones en alta tecnología. Mucho más interesante resulta la Red en tanto que metáfora de una nueva forma de organización que las nuevas tecnologías de la información hacen posible. He empleado «hacen posible» deliberadamente: la organización de la Red lleva un cierto tiempo acompañándonos, pero las nuevas tecnologías de la información son las que han hecho posible su creciente predominio y la sustitución de antiguas formas de organización.

Manuel Castells ha titulado el primer volumen de su monumental investigación en tres volúmenes sobre *La era de la información, La sociedad red*. Para Castells, ya ha cristalizado un nuevo paradigma tecnológico e informático cuyos efectos de dominación incluyen

una *lógica de la Red* aplicable a cualquier sistema o relación que use esas nuevas tecnologías de la información. La morfología de la Red parece adaptarse con una creciente complejidad a la interacción, y a modelos impredecibles de desarrollo que emergen del poder creativo de dicha interacción. Ahora es posible poner en práctica esta configuración topológica, la Red, en todo tipo de procesos y organizaciones, mediante las recientes tecnologías de la información disponibles. Sin ellas, sería demasiado lento y pesado implantar la lógica de la Red. Sin embargo, tal lógica necesita estructurar lo inordenado al mismo tiempo que preservar su flexibilidad, ya que lo inordenado, carente aún de estructuras, es la fuerza motriz de cualquier innovación en la acción humana.⁵¹

51. Manuel Castells. *The Information Age: Economy, Society and Culture*, vol. 1: *The Rise of the Network Society*, Oxford, Blackwell, 1996, págs. 62-63 (trad. cast.: *La era de la información: economía, sociedad y cultura*, vol. 1, *La sociedad red*, Madrid, Alianza, 1999).

Castells sigue considerando las ramificaciones de esta lógica de la Red a una escala internacional, señalando incluso cómo empieza a elaborar de nuevo nuestra concepción del espacio, que se habría deslizado desde un «espacio de lugares» hasta un «*espacio de flujos*»: «La articulación espacial de las funciones dominantes tiene lugar, en nuestras sociedades, en la red de interacciones que han hecho posible los dispositivos tecnológicos e informáticos. En tal red, no existe un lugar en sí mismo, ya que las posiciones se definen mediante flujos».⁵²

Antiguas formas de organización, en especial los grandes Estados o las mayores multinacionales, están enormemente presionados por la lógica de la Red, ya sea para reorganizarse o para hundirse. Las multinacionales se han adaptado mucho mejor y más rápidamente que los Estados y otros organismos públicos. En parte, esto se debe a su mayor sensibilidad hacia el mercado y sus tarifas. Los mismos mercados son, de hecho, estructuras similares a la Red, que entrenan a sus usuarios para pensar en términos de flujos los movimientos de la oferta y de la demanda. La primera víctima importante de la nueva Era de la Información fue la economía planificada y esclerótica del bloque soviético. Estos dinosaurios burocráticos, que en otros tiempos se protegieron a sí mismos mediante el aislamiento de los mercados internacionales (tanto por iniciativa propia como parcialmente impuesto durante la primera fase de la Guerra Fría), ya no podían seguir arreglándose ante las crecientes presiones que recibían. Los gobiernos occidentales, por el contrario, han empezado a cambiar y a adaptarse, aunque no sigan el mismo ritmo que el sector privado.

Uno de los elementos clave en la organización de una red es el declive progresivo en la organización vertical de las estructuras autoritarias a favor de *conexiones horizontales que atraviesan las fronteras de la organización tradicional*. Las antiguas formas de organización se basaban en el mando y control desde arriba, con una estructura jerárquica rigurosamente definida. La policía y el cuerpo militar son los ejemplos extremos de una estructura y una organización jerárquicas y disciplinadas, con un fuerte sentido de la identidad (a menudo llamado *esprit de corps*). Las empresas tradicionales no eran tan militantes, pero conservaban una conciencia muy clara de

52. Castells, *op. cit.*, pág. 412.

su integridad, así como la integración vertical de sus operaciones aseguraba un control global de todos los aspectos de la producción, la distribución y el marketing. Las nuevas formas de organización son menos jerárquicas, y sus límites son menos precisos en dos sentidos. En primer lugar, la comunicación horizontal dentro de la organización se ve facilitada por las nuevas tecnologías, lo que impulsa más fácilmente el trabajo en cooperación, moderándose por lo tanto la autoridad jerárquica tradicional. En segundo lugar, cada vez se hace más trabajo en los mismos hogares, lo cual también desdibuja los límites de una organización. En contraste con las antiguas formas, la organización por redes se descentra tanto por dentro como por fuera. Tales cambios quedan ilustrados en un informe reciente sobre Monsanto, una empresa en la vanguardia de la biotecnología. Al explicar sus estrategias, un ejecutivo de Monsanto indicaba que «la construcción de una red de empresas que pueda trabajar conjuntamente alrededor del mundo es un aspecto clave para nosotros». Otro ejecutivo comentaba que la empresa «puede incluso experimentar algún día con el hecho de que los trabajadores escojan sus propios directores, así como con presupuestos adaptados a la cantidad de gente que quiera trabajar en un proyecto».⁵³ En términos de gestión empresarial, la «nueva empresa es una red de equipos distribuidos que actúan como clientes y como servidores entre ellos».⁵⁴

En una economía de la Red, se crean constantemente grupos de trabajo con estructuras de tipo molecular para encontrarse con (y anticipar) desafíos concretos. Las asociaciones y alianzas estratégicas obedecen a proyectos específicos, creándose «empresas y sociedades virtuales». La «desintermediación» es (además de un barbarismo) un término forjado para describir la obsolescencia de intermediarios que la comunicación directa mediante la Red ha provocado. Dell Computers ha construido una empresa multimillonaria internacional dedicada a la venta de hardware que puede adquirirse directamente mediante el teléfono o Internet. Grandes empresas cuya existencia dependía hasta ahora de una producción específica, como coches o teléfonos, ven ahora cómo su modo de organización sigue

53. Barnaby J. Feder, «Getting Biotechnology Set to Hatch», *New York Times*, 2 de mayo de 1998.

54. Don Tapscott, *The Digital Economy: Promise and Peril in the Age of Networked Intelligence*, Nueva York, McGraw-Hill, 1996, pág. 12.

los dictados de la innovación productiva, más que el movimiento contrario. Así que lo que antes eran empresas de hardware electrónico, de desarrollo de software, de teléfonos y de cables de televisión, o empresas de entretenimiento, convergen ahora para ofrecer servicios integrados.

Todos estos elementos conllevan *flexibilidad*, un término que ha alcanzado una cierta notoriedad al referirse, y racionalizar, el desempleo y los desajustes a gran escala de formas de vida consolidadas: una fuerza de trabajo flexible remite a una fuerza de trabajo reemplazable. La era de las innovaciones en tecnología de la información ha coincidido con el ascenso de la agenda neoliberal en la reestructuración de los Estados y las grandes empresas, en tanto que reducción de personal: las nuevas tecnologías se han empleado a menudo como el justificante de despidos y clausuras. Tal justificación podría remitir más a simples excusas que a razones verdaderas, pero saber si las nuevas tecnologías son el factor más determinante del desempleo permanente y de la persistente presión hacia abajo que reciben los trabajadores en sus formas de vida o, por el contrario, todo ello remite al contexto político concreto que han adoptado poderosas elites, es una cuestión demasiado larga y compleja que no podemos tratar aquí. Sin embargo, hay un punto muy claro: la lógica de la Red exige sin lugar a dudas una mayor flexibilidad, tanto para la gestión y la dirección como para las fuerzas de trabajo, así como en las escuelas y otras instituciones de la sociedad de la Red. Por su lado, la flexibilidad exige ajustarse constantemente a los cambios, lo que a vez conlleva un estado de inseguridad permanente, una inseguridad endémica, penetrante y de la que no hay salida.

Nos encontramos ante una gran paradoja de la sociedad de la Red: aunque su forma exige y recompensa la flexibilidad y la innovación, la inseguridad engendrada por sus efectos conlleva un tipo de conducta muy distinto: la aversión al riesgo. La imprevisibilidad e inestabilidad inherentes a la Red o redes electrónicas crean un imperativo urgente de organización que reponga, al menos, grados tolerables de estabilidad y de previsión. Se trata de una paradoja muy acentuada: las nuevas tecnologías de la información que, por un lado, promocionan el riesgo y la innovación, son las mismas que, por otro lado, nos ofrecen los medios técnicos para reducir los factores de riesgo. Los sistemas coordinados informáticamente pueden controlarse y corregirse ellos mismos, que es lo que los hace tan adapta-

bles, pero el control continuo también les otorga la capacidad de identificar, aislar y eliminar los factores de riesgo dentro de su estructura organizadora, y también les permite aumentar su capacidad de exploración del entorno externo para evitar factores de riesgo potenciales: las nuevas tecnologías de la información también son tecnologías de vigilancia, lo que discutiremos en detalle en el próximo capítulo.

4. «La noche tiene mil ojos»: nuevas tecnologías de vigilancia

Ver es creer: de las «tecnoniñeras»* a los satélites espías de «pago por uso»

En un caso de 1997 que llamó la atención de la opinión pública a escala internacional, Louise Woodward, una joven niñera británica que trabajaba para una familia de Massachusetts, fue acusada de asesinar al bebé de ocho meses que estaba a su cuidado. Aunque fue absuelta, poco después de este caso, tan seguido por la opinión pública, una nueva tendencia de la industria privada de la vigilancia lanzó al mercado «tecnoniñeras», equipamientos de vigilancia videográfica que podían instalarse subrepticamente en guarderías y hoga-

* En el original: *nannycam*, de *nanny* (niñera), y *cam*, acrónimo de *(C)omputer (A)ided (M)anufacturing*. (N. del t.)

res para registrar las actividades del día, y permitir así una posterior inspección secreta de los padres.¹ En la publicidad de sus nuevos productos, las empresas de seguridad privadas alimentan sin duda el miedo potencial de sus clientes y, desde luego, el sentimiento o complejo de culpa entre las madres trabajadoras, inculcando un cierto grado de recelo sobre la negligencia, si no cosas peores. Ahora disponemos de una nueva y sofisticada tecnología que puede resolvernos el problema: equipos diminutos, con microcámaras de vídeo de dos a tres centímetros de ancho, que pueden ser colocados en osos de peluche, relojes, plantas e incluso en detectores de humo. Gracias a su creciente popularidad, los precios de esta tecnología han caído espectacularmente, y se han hecho accesibles incluso para familias con ingresos relativamente modestos. El vídeo puede ser retransmitido en un canal televisivo dedicado a este fin, o registrado en videocasete para su revisión posterior. Otra posibilidad más sorprendente consiste en conectar la cámara al ordenador mediante software, lo que permite a los padres echar rápidas ojeadas a sus hijos en tiempo real a través del ordenador de su oficina. Otra variante remite a los servicios de vigilancia *on-line* que ofrecen algunas guarderías de la Red. Los padres que trabajan también pueden ser, por lo tanto, padres que cuidan virtualmente de sus hijos mediante la magia de estas nuevas tecnologías.

Una de las rarezas de las «tecnoniñeras» es la insistencia en el secreto, como si se tratase de una especie de operación clandestina de algún servicio de inteligencia. Alguna de las empresas que suministran tales «tecnoniñeras» llevan incluso nombres como Spymaster (maestro de espías). No es de extrañar que las niñeras y las organizaciones que las representan hayan expresado su consternación y furia por ser registradas secretamente en vídeo. Tales empresas no parecen haber captado los fundamentos de la lógica panóptica, ya que, bajo sus principios, las niñeras verían de forma transparente y clara, desde el principio, que sus contratos conllevan la observación, registro y análisis de todos sus movimientos. Al saber de antemano que serán constantemente controladas, se disciplinarían ellas mismas para comportarse del modo requerido, interiorizando las reglas de sus em-

1. Robert Uhlig, «Spy Camera Keeps a Private Eye on Au Pairs», *Daily Telegraph*, 16 de diciembre de 1997; Gary Strauss, «Nanny Cams Ease Parental Angst», *USA Today*, 26 de febrero de 1998.

pleadores. Quizás el futuro nos depare auténticas «tecnoniñeras» panópticas. Sin duda ofrecerían la ventaja, respecto a la obsoleta vigilancia benthamiana, de que estas nuevas tecnologías permiten operar desde lugares remotos. Con las versiones que ofrecen algunos servicios desde la Red y con la movilidad de los ordenadores portátiles, los padres pueden inspeccionar a sus hijos en tiempo real desde cualquier lugar de trabajo: ¿mamá debe irse de viaje de negocios para conseguir una venta o cerrar un trato en Alaska? Ningún problema; siempre podrá mantener un ojo atento a su niñera, y a su bebé, entre las clases de *sushi* con los clientes de su empresa. Al saberlo, la niñera no se relajará en ningún momento a lo largo de su trabajo. Esto es al menos lo que nos sugiere la teoría panóptica.

La «tecnoniñera» es sólo un pequeño ejemplo de cómo las nuevas tecnologías están transformando el ojo electrónico, haciéndolo penetrante, dominante y ubicuo. Otro ejemplo, con ramificaciones mucho mayores, es el uso creciente de cámaras de vídeo teledirigidas por ordenadores (*videocam*) para vigilar espacios públicos. Los circuitos cerrados de televisión (CCTV) se usan cada vez más, desde hace algún tiempo, para controles de seguridad en lugares públicos, como oficinas, tiendas, bancos, vestíbulos de ciertos edificios, garajes, etc. Los guardas de seguridad que manejan diversas cámaras de televisión, o la captura de sospechosos de robo por una cámara de vídeo, ya son hechos familiares.² Pero la tecnología de la vigilancia videográfica está en un proceso de innovaciones que aumentan sus hasta ahora limitadas consecuencias. El primer tipo de innovaciones es cuantitativo: el alcance de estos ojos electrónicos es mucho más penetrante y omnipresente. El segundo es cualitativo: la tecnología del reconocimiento facial y la digitalización de la información, conectada a una base de datos central, ofrecen la perspectiva de un desplazamiento: desde los propósitos defensivos o de seguridad pasiva, en los que se ha empleado básicamente hasta ahora tal tecnología, hasta una nueva era de identificación activa y de localización de individuos.

Una noticia de la ciudad de Nueva York pone de manifiesto el descubrimiento que hace una mujer de la ubicuidad del ojo electrónico:

2. Para una interesante investigación sobre las cámaras videográficas de vigilancia, véase Peter J. Schuurman, *Spying, Peeping and Watching Over: The Beguiling Eyes of Video Surveillance*, Queen's University, MA, Departamento de Sociología, 1995.

Barbara Katende había llegado al punto en que ya no daba ninguna importancia a las cámaras de vídeo. Las que estaban instaladas en el Palacio de Justicia donde trabaja la hacían sentirse más segura, así como las situadas en los bancos y cajeros automáticos. Había aceptado incluso las situadas en grandes almacenes para prevenir el robo.

Pero la semana pasada, la señora Katende, de 26 años, vislumbró una cámara en un tejado situado a unos ciento cincuenta metros de su apartamento, en Kew Gardens. Un tejado que había visto innumerables veces, sin fijarse nunca en él, cada vez que se asomaba a la ventana de su sexto piso con las persianas abiertas, holgazaneando en ropa interior, envuelta en una toalla o incluso desnuda.

Las cámaras controlan el tráfico en el cruce entre las vías rápidas de Van Wyck y Gran Central. Pero, tal y como aprendió la señora Katende de un periodista, tienen un poderoso zoom, pueden orientarse en todas direcciones y están controladas por un técnico en un estudio de televisión a kilómetros de distancia, en el centro de Manhattan. La señora Katende quedó horrorizada ante la idea del técnico desplazando la cámara hacia su apartamento, por aburrimiento, o por algún motivo peor. «Si no tienes intimidad en tu propia casa —dijo la señora Katende— ya no te queda intimidad en ningún lugar, ¿verdad?»³

El voyeurismo furtivo con alta tecnología es una cosa, pero la proliferación de cámaras de vídeo tiene una significación mucho más amplia. Las cámaras han invadido progresivamente más espacios de Nueva York, extendiendo silenciosamente su ojo electrónico por toda la ciudad. En algunos casos, se ha promocionado de forma deliberada su instalación, como es el caso de las cámaras que controlan la plaza de Washington Square en Greenwich Village, la primera iniciativa de una serie de medidas contra el crimen tomadas por el alcalde Rudolph Giuliani y su jefe de policía.⁴ Pero las cámaras no son exclusivas de la policía ni del gobierno: muchas están en manos privadas y se usan por motivos muy variados, desde la seguridad a los informes televisivos sobre el tráfico. Los propósitos declarados son inocuos, incluso benignos. Los críticos sugieren, sin embargo, que los detectives privados y los nuevos agentes de información sa-

3. David M. Halbfinger, «Spread of Surveillance Cameras Raises Prospect of Prying Eyes», *New York Times*, 22 de febrero de 1998.

4. Felicia R. Lee, «Cameras Drive Drug Dealers From Greenwich Village Park», *New York Times*, 3 de enero de 1998.

brán cómo sacar otros provechos a estas cámaras. Aunque no formen un sistema integrado y único, el mosaico de ojos electrónicos públicos y privados empieza a cubrir potencialmente casi toda la ciudad.

Siguiendo el ejemplo de grandes ciudades como Baltimore, pionera de una amplia vigilancia videográfica, coordinada por la policía en barrios con un alto índice de criminalidad,⁵ ciudades más pequeñas han instalado un sistema mucho más amplio, gracias a sus necesidades más modestas de cobertura. East Newark, por ejemplo, una pequeña ciudad de Nueva Jersey con 2.000 habitantes, tras un hecho violento aislado, instaló dieciséis cámaras de vigilancia con ejes rotativos para controlar ininterrumpidamente las nueve manzanas que la componen.⁶ Lyons, ciudad aún en parte rural en el Estado de Nueva York, con 4.300 habitantes, ha instalado cámaras de vigilancia en todas sus calles principales, a pesar de su bajo índice de criminalidad.⁷ Inglaterra ha usado este sistema de vigilancia policial mediante el vídeo seguramente más que cualquier otro país de Europa occidental, por lo que es relativamente normal encontrarse con una amplia vigilancia videográfica en los centros de todas las ciudades británicas. La idea consiste en ponerse rápidamente al día: más de 450 ciudades habían instalado tales sistemas a finales de 1997, unas 74 más que tres años atrás. Es como si se tratara de una dinámica acumulativa por contagio: las ciudades «sin protección» temen convertirse en el objetivo de los criminales si no adoptan el mismo sistema, y existen algunos hechos que confirman este efecto. Todo ello ha llevado a ciudades de menos de 1.500 habitantes a procurarse su propio sistema de vigilancia videográfico. Además, la misma dinámica conlleva la extensión de la cobertura en la misma ciudad, ya que la instalación de cámaras desplaza el miedo hacia los lugares sin cobertura, por lo que se acaba exigiéndola en todas las calles residenciales y en todas las áreas públicas.⁸

5. Michael Cooper, «Public TV Surveillance Draws Mixed Reactions», *New York Times*, 5 de febrero de 1997.

6. Evelyn Nieveseast, «Welcoming "Big Brother" Watchfully: Public TV Surveillance Draws Mixed Reactions», *New York Times*, 5 de febrero de 1997.

7. «In a Small Town, Cameras Keep Watch», *New York Times*, 7 de diciembre de 1997.

8. Paul Brown, «Demand for Closed-Circuit TV Triggers Fear of Crime», *The Guardian*, 9 de enero de 1998.

Estos sistemas de vigilancia videográfica intensiva no necesitan ser meramente pasivos, controlados «manualmente» por gloriosos guardas de seguridad. Ya se están desarrollando, y empezando a salir al mercado, aplicaciones comerciales que ofrecen servicios de control automatizado:

Imaginemos el parque de una ciudad invadido por cámaras, discretamente colocadas, que envían sus imágenes a un ordenador programado para mantener un ojo vigilante. Esto puede parecer sombríamente orwelliano, pero David Aviv, un antiguo ingeniero aeroespacial, ha patentado justamente un sistema de estas características para combatir el crimen. Aviv dice que su invención, a la que llama Ojo Público, usa patrones de reconocimiento para detectar robos o actos violentos, gracias a la base de datos en la que ha digitalizado y almacenado todo un repertorio de acciones físicas. La cámara envía al ordenador imágenes en tiempo real de una persona que, por ejemplo, usa el cajero automático; el ordenador recoge entonces ciertas imágenes congeladas y las compara con las de su base de datos, en busca de acciones amenazadoras [...] Aviv también ha usado otro patrón de reconocimiento basado en la voz, para detectar los comportamientos verbales agresivos.⁹

La extensión cuantitativa de los equipos de vigilancia videográfica sólo remite a una parte de sus consecuencias. Los nuevos métodos de reconocimiento facial, que aún se encuentran en fase experimental, pueden estar disponibles para usos comerciales en unos cinco años. Una vez más, la clave está en la digitalización. Con el software adecuado (uno de los más desarrollados actualmente es el denominado «Observador de personas»), a menudo inspirado analógicamente en el funcionamiento del cerebro humano, los rasgos faciales pueden reducirse a un código digital. Si el software es suficientemente sofisticado, y no hay ninguna razón para pensar que no pueda ser así, tal código podría ser tan específico en su capacidad de reconocimiento como en los mismos seres humanos, con sus considerables habilidades en este campo. Incluso un cambio de las apariencias (la adición o sustracción de cabello, gafas, cosméticos, etc.) podría ser detectado por un software que haya analizado los rasgos faciales con el suficiente deteni-

9. Teresa Riordan, «Engineer Invents Computerized Surveillance System», *New York Times*, 13 de octubre de 1997.

miento.¹⁰ Las ventajas de los sistemas de reconocimiento automático radican, evidentemente, en sus inmensas capacidades de almacenamiento y memorización, así como en la velocidad del procesamiento. Los beneficios de estos sistemas de reconocimiento «biométrico» son obvios: ya no será posible suplantar la identidad de otra persona con intenciones fraudulentas; una tarjeta de crédito robada será inútil si la persona que pretende usarla es identificada inmediatamente como un impostor. En la actualidad ya existen, por ejemplo, algunos cajeros automáticos que exploran la retina de la persona que usa la tarjeta de crédito para identificarla, con el mismo margen de seguridad que dan las huellas digitales.¹¹ Pero los sistemas de análisis videográfico, cuando sean operativos, ofrecerán mucho más que eso: permitirán, por ejemplo, identificar a un fugitivo, aislando su rostro de la multitud, ya sea un condenado en fuga, un conocido terrorista o un supuesto desaparecido. Todo ello nos lleva de nuevo al creciente entramado de la vigilancia videográfica en espacios urbanos, públicos y privados. Si tal expansión se conectara a los sistemas de análisis videoinformáticos, existiría una tecnología que haría realmente difícil esconderse o perderse. Naturalmente, no tiene por qué ocurrir algo sólo porque sea posible, pero, aunque sólo se implantaran parcialmente, tales sistemas automáticos de vigilancia darían un irónico vuelco a muchas de las críticas dirigidas a las modernas sociedades de masas, tales como el anonimato y la impersonalidad. En la época de las máquinas inteligentes, podemos imaginarnos cualquier cosa.

Otro aumento tecnológico de la visión consiste en su capacidad de ver a través de barreras visuales. Ya se está desarrollando una cá-

10. Saul Hansell, «Use of Recognition Technology Grows in Everyday Transaction», *New York Times*, 20 de agosto de 1997; Michael Stutz, «Saving Face With Person Spotter», *Wired News*, 19 de febrero de 1998.

11. El Reino Unido anunció para finales de 1997 una prueba de exploración del iris con unos lentes de cámara en ATM. La tecnología «puede reconocer una huella ocular individual, el único patrón encontrado en el iris, una anilla coloreada de tejido que envuelve a la pupila. Cada persona tiene un patrón diferente de filamentos, marcas y estrías en el iris, convirtiéndose en un distintivo parecido a la huella dactilar». Un usuario registrado tiene su patrón registrado, quedando reducido a un código digital. «Entonces, cada vez que usen la tarjeta, tendrán que mirar a la cámara a una distancia de treinta o cuarenta centímetros. La exploración del iris se extraerá de la imagen y será comparada con el código almacenado en la base de datos central para confirmar la identidad del individuo» (Nigel Hawkes, «Machines Will Pay up in Blink of an Eye», Londres, *The Times*, 2 de diciembre de 1997).

mara electromagnética que será capaz de detectar armas escondidas bajo la ropa desde ocho a dieciocho metros de distancia. Esta cámara de ondas milimétricas se aprovechará de las señales electromagnéticas del cuerpo humano: los objetos «fríos», tales como pistolas y cuchillos, e incluso los explosivos plásticos, casi no emiten tales señales y básicamente bloquean las que emite el cuerpo humano, por lo que la cámara será capaz de obtener una imagen precisa de tales objetos en pantalla. Estas cámaras pueden ser llevadas a mano, o instaladas en vehículos policiales, lo que permitiría a la policía reconocer a sospechosos sin tan siquiera abandonar la seguridad de sus coches patrulla. Entre otros dispositivos a punto de ser operacionales, cabe mencionar los sistemas visuales con rayos X, que emiten una dosis muy baja de radiación que, al reflejarse en la piel, compone, en menos de un segundo, una imagen completa del cuerpo humano y de todo lo que transporte. La Búsqueda Infrarroja (FLIR), desarrollada originalmente por los militares para localizar aviones enemigos, puede detectar diferencias muy ligeras de temperatura, por lo que, instalada en vehículos móviles o transportada a mano, pueden realmente «ver a través» de las paredes. Las patrullas de la frontera entre México y Estados Unidos podrían usarlas para detectar inmigrantes ilegales.¹² La tecnología de visión nocturna, también desarrollada previamente para su uso militar, permite a la policía transformar la noche en día. La tecnología danesa de fotocopia estroboscópica permite obtener cientos de fotografías en cuestión de segundos, con lo que será posible obtener la fotografía individual de todos los participantes en una huelga o manifestación ilegal.¹³ Al combinarse estos inventos con las tecnologías de reconocimiento facial y con el acceso a los bancos de datos internacionales, la policía tendría la posibilidad de una identificación instantánea de los individuos. Las proyecciones holográficas, que pueden ir acompañadas por sonidos artificiales apropiados, crean imágenes visuales falsas, que pueden confundir y desorientar a un presunto delincuente.

Las ventajas de estas nuevas tecnologías desde la perspectiva de la seguridad o del refuerzo de la ley son obvias, como también sus

12. David Banisar, «Big Brother Goes High-Tech», *Covert Action Quarterly*, 56, 1996.

13. Steve Wright, *An Appraisal of Technology for Political Control*, Luxemburgo, Parlamento Europeo, Dirección General de Investigación, 1998, 4.1.

amenazas para la intimidad de los ciudadanos. Aunque se desarrollen para un propósito concreto, tales innovaciones siempre pueden utilizarse para otros fines, lo que por lo general ocurre rápida y fácilmente. Muchas se ha originado en la investigación militar y se han usado posteriormente en el trabajo policial. Incluso en este contexto, las tecnologías pueden transferirse con facilidad de un objetivo a otro. Lo que se desarrolló como dispositivo de vigilancia contra el crimen puede reorientarse contra los refugiados, los disidentes políticos o los huelguistas del sindicato. Tales tecnologías también se están desplazando hacia manos privadas, empresas de seguridad que se sitúan al margen de cualquier regulación o legitimidad democrática, lo que sin duda constriñe a los servicios estatales. Finalmente, estas nuevas tecnologías también se abren paso hacia el mercado general. En los últimos años, hemos asistido a la proliferación comercial de dispositivos de fisgoneo y espionaje a precios espectacularmente económicos, sin que fuera necesario dar ninguna explicación para adquirirlos.

Incluso mientras se mantienen básicamente en el sector estatal, tales tecnologías de visualización conllevan cuestiones delicadas. Tal y como señala el informe publicado en un periódico:

Algunos de los nuevos instrumentos de detección pueden implicar nuevas cuestiones constitucionales respecto al trabajo policial, y no existen precedentes para las respuestas: la cámara de ondas milimétricas permitiría a los oficiales de policía detectar armas escondidas bajo la ropa desde el otro lado de la calle: ¿constituiría esto un cacheo ilegal? ¿O sería causa suficiente para confiscar el arma? ¿Puede el uso de dispositivos capaces de ver a través de la ropa, aunque los fabricantes digan que no revelan detalles íntimos, implicar una invasión de la intimidad?¹⁴

Los ojos electrónicos instalados en las calles y en los tejados no pueden compararse, sin embargo, con los impresionantes superojos del espacio que giran en órbita alrededor de la Tierra. El reconocimiento por satélite cambió el rumbo de la Guerra Fría y transformó el oficio del espionaje. Al acabarse las hostilidades, la década de los

14. Fox Butterfield, «Devices May Let Police Spot People on the Street Hiding Guns», *New York Times*, 7 de abril de 1997.

noventa ha visto cómo se desclasificaban parcialmente ciertos documentos, e incluso cómo se comercializaban las tecnologías de visualización. Los científicos ya han iniciado algunas tentativas de colaboración con los servicios de inteligencia y con los organismos militares para poder acceder a la vasta, y mayormente secreta, base de datos recopilada por los satélites de espionaje, con el propósito de investigar fenómenos como la medición de los efectos del cambio climático.¹⁵ Algunos usos comerciales ya se han consolidado; un periodista acompañó un día a un agricultor canadiense en su segadora, y descubrió un elemento nuevo en una escena familiar:

En un soleado día del pasado agosto, Terry Gates puso su segadora John Deere en punto muerto y descansó entre sus gloriosas 1.600 hectáreas de trigo y cebada [...] Mientras el motor seguía en punto muerto, el granjero puso un cartucho de datos en un aparato de su salpicadero que era, de hecho, un ordenador 486. Segundos más tarde, una exposición coloreada aparecía en su pantalla: el Sistema de Posicionamiento Global (GPS), mediante satélites a 18.000 kilómetros de distancia por encima de la Tierra, le dio al señor Gates su posición dentro de un campo de trigo de dos metros cuadrados. En la pantalla, entre rojos, verdes, azules y amarillos —indicando la distribución de potasio en la tierra— pudo ver una muestra gráfica de la franja de seis metros de tierra en la que había probado un fungicida el último verano. Tal y como esperaba, su cosecha por metro cuadrado había aumentado en esta diminuta área. Hubo un tiempo en que los granjeros extendían alambres y «cables» para delimitar su territorio. Ahora, granjeros «cableados»* mediante ondas a su GPS están desplazando los límites de lo que pueden producir desde su territorio.¹⁶

Los agricultores instalan receptores en sus tractores para recoger datos de los satélites, y luego pueden transferirlos a ordenadores personales para un análisis más detenido: en la era de la vigilancia videográfica, el agricultor, en medio de sus campos, se conecta directamente al espacio, desde donde puede ver más y mejor que desde el suelo.

15. Jeffrey T. Richelson, «Scientists in Black», *Scientific American*, febrero de 1998, págs. 48-55.

* Juego de palabras en el original entre *wire* (alambre) y *wired* (conectado... a la Red). (*N. del t.*)

16. Alexander Wooley, «Precision Farming», *The Globe & Mail*, Toronto, 15 de marzo de 1997.

Tal agricultura de precisión se basa en el sistema norteamericano de navegación por satélite, el GPS, que identifica los objetos terrestres mediante longitud y latitud, y que fue ampliamente utilizado en la guerra del Golfo para dirigir jeeps, tanques y misiles. Existe un sistema ruso similar al GPS, y ambos disponen de satélites totalmente equipados y en órbita terrestre ininterrumpidamente, emitiendo sin parar señales que pueden recibirse desde cualquier parte del mundo. Toda persona que disponga de un receptor puede localizar inmediatamente su posición y sus coordenadas geográficas.¹⁷ Los excursionistas por tierras remotas, por ejemplo, pueden comprobar sus coordenadas con un pequeño GPS manual. Mediante futuros perfeccionamientos, será posible el seguimiento constante de, por ejemplo, enfermos de Alzheimer o niños pequeños. Como ocurre con casi toda esta tecnología, el GPS tiene dos caras: la primera es muy conveniente y aumenta nuestras capacidades, la segunda remite a la vigilancia y al control. Ya es posible, por ejemplo, «etiquetar» a alguien para no perderle la pista en ningún momento, y con la mayor precisión.

Mientras los Estados intentaban recuperar los costos de sus servicios, la visualización mediante satélites ha empezado a introducirse lentamente en el mercado. El siguiente paso consiste en el lanzamiento, en 1997, del primer satélite comercial, muy parecido a los de espionaje: el Early Bird 1 fue lanzado mediante un cohete ruso en el este de Rusia, por Earth Watch Inc., su constructor, de Longmont, Colorado. Este hecho fue entendido como el fin del monopolio estatal respecto a la recopilación desde el espacio de imágenes de alta resolución. Para desgracia de la empresa, el Early Bird desapareció misteriosamente poco después de entrar en la órbita terrestre.¹⁸ Aunque este fracaso pone de manifiesto que la actual tecnología de los satélites aún no está exenta de fallos, ya se han puesto en marcha otros proyectos comerciales en la estela del Early Bird. Los satélites de la próxima generación, a punto de llegar, serán capaces de distinguir objetos en el suelo con un diámetro inferior a un metro. El gobierno norteamericano retiene el derecho de apagar los sensores comerciales en tiempo de guerra o de tensión internacional. También prohíbe a los operadores con licencia de los satélites norteameri-

17. Warren L. Strutzman y Carl B. Dietrich, Jr., «Moving Beyond Wireless Voice Systems», *Scientific American*, abril de 1998, págs. 92-93.

18. Michael Learmonth, «Sky Spy», *Metro*, 16-22 de abril.

canos vender imágenes a los gobiernos de Cuba, Libia, Corea del Norte, Irán e Iraq, así como a cualquier otro país, institución o grupo «bajo sospecha».¹⁹ Presumiblemente, los futuros lanzamientos desde otros países estarán sujetos a menos controles, a menos que se llegue a un acuerdo internacional para limitar la explotación comercial de este potencial militar de vigilancia y visualización por satélite. El problema radica en que los satélites son de «doble uso»: imágenes encargadas para un uso científico o comercial también pueden tener un uso militar. Aunque el reconocimiento por satélite pueda haber ayudado a estabilizar la relación entre las superpotencias durante la Guerra Fría, la misma tecnología puede desestabilizar regiones en la era inmediatamente posterior, ofreciendo a los Estados beligerantes o rebeldes, e incluso a sofisticados grupos terroristas, la capacidad de calcular y situar con precisión los objetivos que pretenden alcanzar.²⁰

Las posibilidades comerciales de los satélites de espionaje son numerosas. Tal y como proclamaba el *Sunday Times* inglés: «Los satélites de espionaje, hasta ahora bajo el dominio exclusivo de los servicios de seguridad, pasarán a estar disponibles para cualquiera que tenga una tarjeta de crédito. Por algunos cientos de libras esterlinas, pronto será posible ver los jardines de las superestrellas, fisgonear un entrenamiento de terroristas en los campos de Libia, o controlar a la esposa en su viaje de negocios a Amsterdam».²¹ Empresas comerciales tan distintas como las compañías de seguros o las traineras de pescadores ya han indicado su interés potencial en la visualización por satélite. Sin embargo, el representante de un grupo de defensa de los derechos civiles ya ha expuesto que «en ausencia de cualquier legislación respecto a la intimidad, la gente no puede hacer nada para protegerse contra este tipo de vigilancia». La vigilancia desde el espacio está fuera del alcance de las legislaciones nacionales. Si alguien pretendiese saber qué escondes en tu patio trasero, habría necesitado, normalmente, tu permiso o una orden judicial de registro: nada de eso es necesario para obtener imágenes de alta resolución de tu patio trasero desde el espacio.

19. Jim Wolf, «Colorado Spy-quality Satellite Ready to Sell Images», *Reuters*, 25 de diciembre de 1998.

20. Gerald Steinberg, «Dual Use Aspects of Comercial High-Resolution Imaging Satellites», *Mideast Security and Political Studies*, 37, febrero de 1998.

21. Paul Nuki, «Snoopers to Get Eye in the Sky», *Sunday Times*, 16 de febrero de 1997.

Para redondear la imagen de una vigilancia visual mundial, podemos volver a poner los pies en la tierra, literalmente. En Japón, la investigación aplicada se orienta hacia la creación de «ciberinsectos», insectos transformados y controlados artificialmente para misiones de espionaje. Por ejemplo, se ha introducido un microordenador en la «mochila» de una cucaracha, que recibe señales por control remoto y transmite impulsos eléctricos a las patas del insecto, guiando su dirección. Podrían diseñarse «cucarachas robot», con diminutas cámaras y micrófonos, para rastrear escombros en busca de las víctimas de un terremoto, o para espiar a los rivales comerciales o militares.²² Investigadores militares ya han pensado en desarrollar aviones de espionaje en miniatura, capaces de revolotear por los campos de batalla o por los campamentos enemigos como abejas o mosquitos. Podría llegar a ser posible disponer de una «mosca en la pared» en las reuniones secretas de la competencia.

«La noche tiene mil ojos» es una vieja canción de jazz, pero el futuro nos depara muchos más de los que dice la canción. Además, con tecnologías de datos digitales y con un sistema de comunicación internacional de redes teleinformáticas, el potencial para compartir información es realmente impresionante. Por ejemplo, podrían coordinarse sistemas para seguir a individuos particulares: mientras entran y salen de las cuadrículas de vigilancia local, los satélites tomarían el relevo, lo que equivale a una cobertura mundial. De momento, no se vislumbra en el horizonte inmediato ningún Gran Hermano con el poder o la influencia suficientes para coordinar todos estos sistemas pero, incluso de forma discontinua y azarosa, ya existe un entramado de vigilancia visual que permite una cobertura más allá del ideal más disciplinario de Jeremy Bentham, con su inspector pretecnológico observando atentamente con sus ojos naturales el pequeño círculo de celdas a su alrededor.

La humanidad vivió un momento vertiginoso cuando la misión espacial de Apolo a la Luna envió, en 1969, fotografías de la Tierra desde el espacio: por primera vez pudimos ver nuestras casas, a nosotros mismos, desde fuera, desde el espacio. Algunos tuvieron la esperanza de que esto ayudaría a desarrollar una concepción global más ecológica de nuestro planeta pero, irónicamente, las mismas

22. Steve Connor, «Menagerie of Cyberbeasts Begins March Out of the Laboratory», *The Times*, Londres, 13 de abril de 1997.

imágenes pueden ser interpretadas como el principio de otra vertiginosa inversión de la perspectiva: esta vez, la totalidad de la Tierra se convierte en el objetivo de un ojo autorreflexivo y panóptico.

«Te oigo»: las paredes del mundo tienen oídos

La intervención de las líneas de comunicación y los micrófonos ocultos han sido los principios básicos de las operaciones de los servicios de seguridad e inteligencia. Nadie es capaz de leer la mente de otra persona, pero se puede obtener una buena cantidad de información sobre los motivos e intenciones de la gente mediante la interceptación de intercambios verbales, especialmente si tales comunicaciones son consideradas confidenciales por sus interlocutores.

En la mayoría de los países occidentales existen leyes para regular el uso de las intervenciones telefónicas y de los micrófonos ocultos, tanto por la policía como por las fuerzas de seguridad. Tales controles son, como mucho, deficientes, ya que las consideraciones sobre seguridad nacional, ley y orden prevalecen sobre las preocupaciones relativas a las libertades civiles. Pero, por más deficientes e irregulares que pudiesen ser en la práctica, se están convirtiendo en cada vez más obsoletos mediante avances tecnológicos que han superado las mismas capacidades de regulación: la mayoría de las regulaciones sobre la intervención de teléfonos, por ejemplo, se basa en la intervención física, en una especie de receptor instalado en el cableado telefónico que recoge y registra las voces que se comunican por este canal. Los micrófonos ocultos también remiten a objetos físicos, colocados subrepticamente en algún «anfitrión» insospechado o en el interior de las paredes, e incluso ocultos en una persona que registra lo que dicen en su proximidad.

Esta especie de escucha furtiva, aunque obsoleta, continua desarrollándose a gran escala. Además, las mejoras tecnológicas permiten que cualquier persona dispuesta a gastarse una modesta cantidad de dinero pueda adquirir dispositivos de escucha y registro muy sofisticados, altamente sensibles y fácilmente camuflables. Los micrófonos ocultos ya no son una prerrogativa del FBI o de la DEA: pueden ser empleados por esposas celosas, socios financieros sospechosos o simplemente por alguien adicto a fisgonear lo que hacen los otros. Un ejemplo reciente es el del fiscal Kenneth Starr, que ins-

taló micrófonos ocultos en Linda Tripp para registrar una supuesta conversación íntima con Monica Lewinsky en un bar, una conversación que estuvo a punto de provocar la destitución (*impeachment*) del presidente de Estados Unidos. Y, del mismo modo que el caso de Louise Woodward disparó la venta de «tecnoniñeras», los vendedores de equipos de escucha furtiva vieron el caso Tripp como un «espacio publicitario» en el que se anunciaban sus productos. Whashington, «con sus abogados, acuerdos, tratos y desconfianzas», siempre ha sido un mercado básico para los artesanos de la escucha furtiva. «Nuestro negocio da las gracias a la paranoia: ¡es fabulosa!», decía un vendedor de equipos de vigilancia por Internet.²³ Aunque los negocios siempre han estado en el centro de muchas de las actividades llevadas a cabo con micrófonos ocultos, también existe un interés creciente por los dispositivos de escucha para otros fines: la policía los usa para registrar sus encuentros con sospechosos; los trabajadores/as para intentar demostrar un acoso sexual; los padres para controlar a sus hijos; los maridos suspicaces para vigilar a sus mujeres. Sin duda se trata de buenas noticias para el negocio privado de la vigilancia. La tecnología de escucha clandestina ha evolucionado especialmente en su capacidad de miniaturización. La legendaria oliva en una copa de Martini que esconde un minimicrófono puede parecer una fantasía de James Bond, pero existen otros dispositivos tan espectacularmente pequeños e indetectables que están disponibles para cualquiera dispuesto a pagarlos.

La colocación física de un dispositivo ya no es un requisito para interceptar una conversación: la tecnología láser permite enviar un rayo altamente concentrado hacia una ventana desde cualquier lugar remoto, mientras no haya ningún obstáculo entre la emisión del láser y el objetivo. El rayo láser es ultrasensible a las vibraciones del cristal de la ventana, y las transmite inmediatamente a los escuchadores; sin embargo, mediante la magia de la digitalización, los ruidos extraños pueden simplemente eliminarse, dejando sólo la conversación que se pretende grabar. Ocurre lo mismo cuando se vuelve a grabar un antiguo disco de vinilo en un disco compacto digital, y se eliminan los siseos y saltos que hayan podido deslucir la grabación original. En consecuencia, las técnicas tradicionales del contraespionaje,

23. Margaret Webb Pressler. «Clandestine Recorders Get the Buzz», *Los Angeles Times*, 23 de febrero de 1998.

tales como tirar de la cadena o subir el volumen de la música, se volverán inútiles. Además, una conversación puede «limpiarse» hasta alcanzar un estado incluso más transparente y claro del que realmente oyeron los mismos participantes mientras la sostenían.

Interceptar una conversación cara a cara sigue siendo un aspecto importante de la vigilancia. Pero en el mundo en que ahora vivimos, las conversaciones cara a cara pueden convertirse en una parte realmente muy pequeña de todas las comunicaciones verbales importantes en las que la gente se involucra. El teléfono, en tanto que extensión popular e internacional de la voz humana, siempre ha sido un medio ideal de interceptación. Pero cada vez hay menos tráfico telefónico mediante cables: las llamadas urbanas e internacionales, una área de telecomunicación en constante crecimiento, es generalmente transmitida mediante satélite o por torres de retransmisión. En las áreas metropolitanas, incluso las llamadas urbanas desbordan a menudo los anticuados cables, por lo que numerosas llamadas son desviadas hacia una transmisión por satélite. Existe, por lo tanto, una impresionante cantidad de comunicaciones telefónicas en el éter, bajo la forma de impulsos electromagnéticos. Todas ellas pueden ser recogidas del aire y escuchadas, sin ningún tipo de intervención física como las empleadas en las antiguas escuchas telefónicas. No sólo se puede hacer: se está haciendo. El sistema de comunicaciones del satélite Intelsat es uno de los más usados para la retransmisión alrededor del mundo de las comunicaciones basadas en llamadas telefónicas, faxes, telefaxes, Internet y correo electrónico. En paralelo y a la sombra de esta red de cobertura mediante satélite, existe otra red de puestos de escucha y de estaciones de control, organizada por los servicios de inteligencia occidentales y supuestamente secreta, que intercepta y controla todas las comunicaciones de Intelsat. Se trata de la red UKUSA, llamada así por los aún secretos acuerdos entre la Agencia Nacional de Seguridad (NSA), de Estados Unidos, y la Jefatura de Comunicaciones del Gobierno Británico (GCHQ), en tanto que socios principales. La NSA es claramente el socio directivo, por los recursos superiores de que dispone; en un segundo nivel se sitúan los socios ordinarios: Canadá, Australia y Nueva Zelanda; y finalmente, un círculo de países que pueden colaborar con la Alianza ofreciendo, por ejemplo, su territorio para la instalación de puestos de escucha. El propósito original de UKUSA remitía al contexto de los servicios de inteligencia en la época de la Guerra Fría: cada me-

tro cuadrado de todo el bloque soviético estaba sometido a la interceptación y desciframiento de cualquier comunicación política o militar.²⁴ Terminadas las hostilidades, quedaba fuera de lugar desmontar toda esta instalación internacional con alta tecnología: los aspiradores del cielo siguieron, pues, aspirando todas las telecomunicaciones, a pesar del recelo de los críticos y de incluso algún desertor de los mismos servicios de inteligencia.²⁵ Interceptan incluso las telecomunicaciones retransmitidas por tierra, completando de este modo una casi total cobertura del mundo de las comunicaciones.

La simple capacidad de interceptar las comunicaciones alrededor del mundo, un día cualquiera, debería ser, en sí misma, algo sin duda inútil, hasta el punto de convertir a los servicios de inteligencia en equivalentes actualizados de los aprendices de brujo. Lo que hace interesantes las capacidades de la interceptación es que, actualmente, los sofisticados programas de software permiten una búsqueda electrónica: una inmensa cantidad de «ruido» se transforma en un pequeño número de «señales significativas». Del mismo modo que los dispositivos comerciales de búsqueda recorren rápidamente Internet, volviendo con numerosos hallazgos a partir de los términos entrados para la búsqueda, también el volumen diario de las telecomunicaciones puede ser sometido al mismo proceso, y encontrar, en la inmensidad de los escombros, la minúscula pepita de oro. El reconocimiento mediante términos clave puede llevarse a cabo mediante palabras, frases o con las direcciones de emisores o de destinatarios concretos. También se está haciendo mucho para el desarrollo de la investigación sobre el reconocimiento de la voz, para lograr hablar con los ordenadores: sin lugar a dudas, podemos afirmar que este software también se utilizará, ante todo, como un dispositivo más para separar el grano de la paja en la interceptación de las comunicaciones.

En 1996, un periodista de investigación y activista Nicky Hager publicó un destacado libro, muy detallado, sobre el papel de su país

24. Jeffrey T. Richelson y Desmond Ball, *The Ties That Bind: Intelligence Cooperation Between the UKUSA Countries*, Boston, Allen & Unwin, 1985; James Bamford, *The Puzzle Palace: Inside National Security Agency, America's Most Secret Intelligence Organization*, Nueva York, Penguin Books, 1983.

25. Mike Frost, un ex agente del servicio de inteligencia canadiense, la CSE, ha escrito unas controvertidas revelaciones: Frost, *Spyworld: Inside the Canadian and American Intelligence Establishments*, Toronto, Doubleday, 1994.

en la red de interceptación telecomunicativa de los servicios de inteligencia, revelándose por primera vez un sistema internacional e integrado: ECHELON. Claramente bajo liderazgo norteamericano, ECHELON conecta a todos los ordenadores de los países colaboradores de UKUSA y emplea diversas categorías de términos clave: «En el sistema ECHELON, cualquier diccionario de una plataforma de computación contiene no sólo los términos clave de su agencia responsable, sino también las listas de las otras agencias y servicios [...] En consecuencia, cada plataforma de computación recoge todas las llamadas telefónicas, faxes, telefaxes, mensajes por Internet y otras comunicaciones electrónicas, según los parámetros programados por los términos clave de todos los aliados, y les envía automáticamente esta información».²⁶ Todas las agencias estatales han negado siempre que pudiesen usar esta capacidad de vigilancia con sus propios ciudadanos, en trabajos de espionaje nacional. Pero ECHELON deja muy claro que los requerimientos especiales no son necesarios: todo el proceso se ha automatizado de tal modo que las líneas divisorias se desvanecen.

Hay ciertos aspectos a destacar en este sistema de interceptación comunicativa. En primer lugar, el mayor beneficiado es Estados Unidos, que tiene un papel dominante en el establecimiento de los términos clave de búsqueda. Los socios normales, como Canadá, Australia o Nueva Zelanda, sólo obtienen un beneficio muy limitado a cambio de su participación, y una amplia mayoría de países queda sencillamente excluida. ¿Qué uso está recibiendo el material interceptado, y con qué fin? Al terminarse la guerra, el consenso anti-comunista que animaba tal alianza ha perdido su sentido. Se habla mucho de contraterrorismo, de la amenaza del crimen organizado internacional y de preocupaciones económicas. Los críticos temen que los intereses nacionales de Estados Unidos se estén ventilando bajo la tapadera de los servicios internacionales de seguridad. Volveremos sobre estas cuestiones en el último capítulo. Por ahora sólo queremos señalar que, en el mundo de las operaciones comunicativas clandestinas, los Estados, con sus servicios de inteligencia y seguridad, y básicamente Estados Unidos, la mayor superpotencia del mundo, son los que juegan el papel preponderante en la intercepta-

26. Nicky Hager, *Secret Power: New Zealand's Role in the International Spy Network*, Nelson, Nueva Zelanda, Craig Potton Publishing, 1996, pág. 29.

ción de las comunicaciones. De momento, el sistema es demasiado complejo y sofisticado como para que cualquier individuo e incluso un grupo organizado pudiese usarlo realmente. También debe señalarse que la evolución tecnológica en las capacidades de transmisión puede adelantarse a la capacidad de cualquier agencia estatal, aunque disponga de alta tecnología para la interceptación clandestina de mensajes: pueden quedarse sin recursos cuando el cable de fibra óptica sustituya definitivamente el antiguo cableado en la transmisión de datos, por su impresionante capacidad de transporte, pensada para la era de la información. Ciertos conocidos de este tipo de agencias estatales me han comentado personalmente su incapacidad para interceptar las transmisiones en cables de fibra óptica, lo que les obliga a interceptar el receptor final, una tarea mucho más caótica y compleja. Pero las agencias y servicios de inteligencia no agotan nunca sus recursos, por lo que ya están desarrollando la tecnología TEMPEST, que les permite interceptar directamente las emisiones y comunicaciones de un ordenador, e incluso entrar en su disco duro mediante las radiaciones electromagnéticas que éste emite.²⁷

Algunas innovaciones en telecomunicaciones también han facilitado la interceptación. Los teléfonos móviles son un buen ejemplo, y en estos últimos años se han hecho muy populares tanto para las comunicaciones laborales como para las personales. Una nueva generación de satélites comerciales se encargará de este tipo de comunicaciones telefónicas, permitiendo a sus usuarios una verdadera cobertura internacional.²⁸ Esta tecnología de comunicación internacional sin cables es muy conveniente, pero los teléfonos móviles constituyen un auténtico riesgo en materia de seguridad. El portavoz del Congreso, Newt Gingrich, lo supo a su pesar cuando una pareja de Florida recogió y registró una conversación entre teléfonos móviles en la que participaban el mismo Gingrich, una congresista de Ohio y otros republicanos, incluyendo al líder de la mayoría en el Congreso. La conversación tuvo lugar el mismo día que Gingrich tuvo que admitir que había violado las reglas éticas del Congreso, por no haber obtenido los consejos legales adecuados sobre el uso de dinero exento de impuestos, y por haber dado infor-

27. Marie Wylie, «Who's Your PC Talking To», *Perspectives*, 11 de febrero de 1998.

28. John V. Evans, «New Satellites for Personal Communications», *Scientific American*, abril de 1998, págs. 70-77.

mación incorrecta durante la investigación de todo este asunto. A lo largo de la conversación, los participantes discuten la mejor manera de manejar los cargos relativos a las reglas éticas del Congreso. El *New York Times* publicó una transcripción parcial de la conversación: los demócratas alegaron que la conversación violaba los acuerdos establecidos entre Gingrich y el Comité de Normas de Conducta Oficial, mientras que los republicanos alegaron una violación de la intimidad. La pareja dijo que había registrado la llamada «porque pensaron que era un hecho histórico».²⁹ Los sofisticados dispositivos de escucha para las comunicaciones entre teléfonos móviles, que están disponibles comercialmente y pueden, por ejemplo, registrar varias conversaciones a la vez en distintas pistas, así como localizar geográficamente a los interlocutores, remiten a una área legal muy confusa en Estados Unidos. Los gobiernos y las empresas de telecomunicaciones compran tales productos, pero también son accesibles a los traficantes de drogas, al crimen organizado y a los grupos terroristas, que pueden usarlos en contra de las mismas agencias estatales de seguridad que imponen la ley y el orden. En California, se abrió un proceso judicial contra una compañía que vendía este tipo de material, pero no fue más que una operación antipromocional sin mucho vigor. Irónicamente, gran parte de las pruebas aportadas por el gobierno se basaban en interceptaciones de teléfonos móviles.³⁰ Es casi imposible imponer legalmente un monopolio gubernamental y corporativo sobre una tecnología que ya es muy barata y que está ampliamente disponible en el mercado. De este modo, cualquier persona sensata que use un teléfono móvil asumirá que alguien —la policía, la mafia, una esposa celosa o un entrometido cualquiera— *puede* estar escuchando.

Por si no fuera suficiente esta posibilidad permanente de interceptación de los teléfonos móviles, también ha trascendido a la opinión pública que tales teléfonos pueden usarse para controlar la localización de sus usuarios: mientras el teléfono está conectado, emite una señal que se envía a la estación central de la empresa. En consecuencia, tal control puede centralizarse, retransmitiendo todas

29. Alison Mitchell, «Ohio Congressman Threatens Suit Over Intercepted Conference Call», *New York Times*, 13 de noviembre de 1997.

30. John Markoff, «High-Tech Eavesdropping Raises New Questions on Personal Privacy», *New York Times*, 13 de octubre de 1997.

las señales a una auténtica estación central, de modo que pueda detectar y localizar toda la red de teléfonos móviles. En Inglaterra ya se retienen durante dos años todos los datos registrados de los teléfonos móviles, y están a disposición de los servicios de seguridad estatales; a partir de este material ya se ha dictado una condena por asesinato. En Estados Unidos, las propuestas de regulación federal emanan, típicamente, de necesidades eminentemente prácticas: disponer de un servicio de emergencia 911 para los teléfonos móviles, con dispositivos de identificación y localización, para que las patrullas puedan atender los casos de urgencia en el mismo lugar de los hechos. Sin embargo, varios portavoces civiles se han mostrado suspicaces ante el interés mostrado por el FBI para centralizar un sistema de control. Tal y como ha comentado el consejero principal del Centro para la Democracia y la Tecnología, un grupo de defensa de las libertades civiles, la tecnología contiene una paradoja intrínseca: «Los representantes de la ley tienen razón en afirmar que tales tecnologías ayudarán a detener a los delincuentes, pero también ayudarán a estos últimos a acechar a sus víctimas».³¹

«No salga nunca de casa sin ellas»: etiquetas electrónicas y tarjetas inteligentes

Hemos revisado los ojos y los oídos de las nuevas tecnologías panópticas. Los dispositivos de identificación electrónica son otra clase de técnicas muy relacionadas con las anteriores. Tal y como corresponde a la tecnología panóptica, muchos de estos mecanismos fueron desarrollados para usos carcelarios. Las etiquetas electrónicas, por ejemplo, se diseñaron para los presos en libertad condicional. Tales etiquetas emiten una señal que permite controlar la localización del preso, notificando a las autoridades si se desplaza fuera del área en la que debe permanecer. Este procedimiento se ha usado en Norteamérica para diversos casos bajo revisión.³² También el Reino Unido lo está usando cada vez más, ya que es considerado como una alterna-

31. Peter Wayner, «Technology That Tracks Cell Phones Draws Fire», *New York Times*, 23 de febrero de 1998; Chris Oakes, «“E911” Turns Cell Phones Into Tracking Devices», *Wired News*, 6 de enero de 1998.

32. David Lyon, *The Electronic Eye: The Rise of Surveillance Society*, Minneapolis, University of Minnesota Press, 1994, págs. 102-107.

tiva mucho más barata que el encarcelamiento.³³ Tales métodos pueden considerarse una extensión del poder panóptico de las cárceles más allá de sus límites materiales pero, como era de esperar, otros métodos de identificación mediante tecnologías similares, aparentemente menos coercitivos, se están introduciendo en toda la sociedad.

Las tarjetas de crédito y de entidades bancarias, o tarjetas de identidad (ID) y otras tarjetas de identificación, están generalmente pensadas para ofrecer más comodidad y seguridad. Sin embargo, lentamente pero de forma inexorable, se convierten en un equivalente de las etiquetas electrónicas, permitiendo localizar y controlar a sus propietarios. Las tarjetas de identificación laboral, cada vez más usadas en grandes organizaciones públicas y privadas, empezaron como, y a menudo siguen siendo, simples trozos de plástico con una fotografía y quizás una firma. Un guarda de seguridad puede exigir la tarjeta en cualquier punto de entrada, y contrastar el rostro de la fotografía con el del usuario. También puede requerirse a todos los empleados que trabajen en lugares prominentes que las lleven permanentemente a la vista. Todo ello puede parecer un poco tosco, pero es probablemente efectivo para propósitos de seguridad. Las nuevas tecnologías ofrecen ciertos perfeccionamientos que aún son bastante caros, pero resultan por lo general atractivos para los empresarios. Las tarjetas de identificación inteligentes codifican información única, como las huellas dactilares, la impresión de toda la palma de la mano o los patrones de la retina. Mediante equipos específicos, puede explorarse automáticamente tanto la tarjeta como el portador para comprobar la equivalencia. En el futuro, también podrían emplearse otras marcas de identificación como el reconocimiento de la voz, del rostro, e incluso «huellas ADN». Pero el uso de las tarjetas inteligentes de identificación no se detiene en las puertas de las grandes empresas: una vez dentro, un sistema de control puede localizar y seguir a todo el mundo, por todas partes. Los edificios inteligentes también podrían asegurarse una distribución automática de sus empleados en los lugares prescritos: algunos pueden estar autorizados a acceder a ciertos lugares pero no a otros, según sus funciones y su condición, y sus tarjetas contendrían esta información para que pudiese ser interpretada por máquinas. Tales meca-

33. Richard Ford, «Tagging for 6,000 Freed Prisoners», *The Times*, Londres, 17 de febrero de 1998.

nismos ofrecen unas ventajas obvias en seguridad para los empresarios, aunque cabe indicar que también podrían ser beneficiosos para ciertos empleados, como mujeres trabajando a altas horas de la noche. Pero las ventajas para el empresario no se acaban en la seguridad: las tarjetas de identificación inteligentes también permiten controlar el rendimiento e incluso saber, por ejemplo, cuánto tiempo tarda un empleado en tomarse un café a media mañana o cuántas veces va al servicio.

Las tarjetas inteligentes de crédito, de débito, monedero u otras funciones bancarias ofrecen modos menos obvios de control y de vigilancia; tales tarjetas «tontas» registran todos sus movimientos: las facturas mensuales ya son de hecho un registro, tanto de los lugares donde su propietario las ha usado como de lo que ha comprado, y algunas veces incluso con el itinerario de sus viajes. Pero estos rastros pueden ser engañosos, ya que las tarjetas pueden perderse o ser sustraídas, y su uso fraudulento es relativamente sencillo. La policía ya ha descubierto en diversos países estratagemas a gran escala con números falsos o robados de tarjetas de crédito, con una pérdida que asciende a miles de millones de dólares. Para citar sólo un ejemplo, en San Francisco, un pirata informático se infiltró en un servidor de Internet y recogió 100.000 números de tarjetas de crédito que luego intentó vender, según información del FBI. Utilizó presuntamente un programa mediante el cual recogió dicha información de una docena de empresas que venden sus productos vía Internet. Desgraciadamente para él, intentó vender la información conseguida a un agente clandestino del FBI por 260.000 dólares.³⁴ Los bancos utilizan la tecnología empleada por las armas inteligentes para encontrar y destrozar al enemigo, aunque en esta ocasión lo hizo para neutralizar las tarjetas de crédito robadas. Los ordenadores construyen y analizan el perfil de gasto de los propietarios de las tarjetas de crédito. El software, llamado Falcon, aprende a reconocer patrones de conducta tras analizar una gran cantidad de transacciones. «En sus aplicaciones defensivas, los ordenadores han aprendido a reconocer perfiles visuales de sus objetivos potenciales, tales como los tanques enemigos. El sistema permite a los pilotos y a los ejércitos terrestres disparar en dirección al enemigo

34. Richard Cole, «FBI Says Hacker Took 100,000 Credit Card Numbers», *New York Times*, 23 de mayo de 1997.

más allá de su horizonte visual, y dependerá del misil encontrar y destrozarse el objetivo.» La misma lógica se aplica al uso fraudulento de las tarjetas de crédito: se contrasta su uso real en las transacciones cotidianas con los perfiles fraudulentos y adecuados, almacenados por la base de datos central: las conductas sospechosas o anómalas pueden ser identificadas para una investigación más minuciosa. Además de este software inteligente, los investigadores de este tipo de delitos «han accedido a una red internacional de ordenadores, creada originalmente por el gobierno norteamericano [...] [para construir] una base de datos mediante la cual sus miembros pueden compartir información sobre organizaciones fraudulentas sospechosas y sus técnicas».³⁵

Las tarjetas de crédito inteligentes que verifican si el usuario es realmente el propietario de la tarjeta benefician tanto los intereses de las empresas como de los usuarios, por lo que, a medida que las tecnologías de reconocimiento bajen sus precios y se difundan más ampliamente, aumentará la presión para que se incluyan más datos personales en el microprocesador. Al mismo tiempo que se incrementa la tendencia hacia una sociedad sin dinero en efectivo, las tarjetas inteligentes con mecanismos más precisos de verificación irán dejando un rastro más evidente. Además, tales tarjetas ofrecen la posibilidad de confeccionar perfiles mucho más detallados de sus usuarios: cuándo y dónde compran normalmente, cuándo y dónde viajan, etc. Y esta información podrá desplazarse desde las empresas de crédito hasta los comercios que acepten su uso, en el caso de que la ley permita tales transferencias de datos y los vendedores quieran conocer más detalladamente el perfil de sus compradores. También existe la posibilidad de usar huellas dactilares para comprobar la identidad de cualquier usuario de las tarjetas de crédito, incluso en las transacciones en la Red. Las huellas dactilares del usuario pueden ser contrastadas con las que tiene registradas la empresa en el mismo momento de la transacción mediante, por ejemplo, los teclados con escáner que ya han empezado a comercializarse: al teclear, las huellas se transmiten por la Red.³⁶ Las implicaciones de estas técnicas para la vigilancia y el mantenimiento de la ley son, por lo menos, intrigantes.

35. Michael White, «Technology That Guides Missiles Is Used to Zero In on Cards Thieves», *New York Times*, 24 de septiembre de 1997.

36. Laurie J. Flynn, «New Products Expand Recognition-Technology Market», *New York Times*, 8 de febrero de 1987.

tes. Aunque la competencia entre distintos tipos de tarjetas parece complicar la posibilidad de un control internacional, las técnicas de comprobación electrónica de los datos ya permiten, de hecho, el equivalente de una cobertura internacional; trataremos más detalladamente esta posibilidad en el próximo capítulo.

El potencial de las tarjetas inteligentes ha interesado tanto a los gobiernos como a las grandes empresas privadas. Una tarjeta de identificación personal universal protegería a los Estados contra abusos a la seguridad social o a otros servicios de bienestar, además de simplificar y reducir el coste de numerosas tareas burocráticas. En diversos países, el número de la seguridad social (o su equivalente)* ya se usa para tales fines: no se puede ganar dinero legalmente ni acceder a ningún servicio estatal sin el uso de dicho número. Mediante el número de la seguridad social (o del carné de identidad) puede entonces conocerse automáticamente el perfil de los ciudadanos, sus relaciones con Hacienda, su empleo de los servicios sociales, etc. En 1966, Lexis-Nexis, una agencia de información instalada en Ohio, Dayton, concedió a todos sus clientes un fácil acceso a los números de la seguridad social durante un breve periodo de tiempo. Como parte de su servicio de «Localización de personas», sus clientes podían buscar información sobre personas concretas en la base de datos de la empresa, mediante millones de números de la seguridad social. Los delegados de Lexis-Nexis dijeron que «esperaban que los clientes usaran este servicio de localización para encontrar testigos y herederos, así como para localizar a criminales sospechosos». Los números de la seguridad social se mantuvieron accesibles durante diez días, hasta que la presión pública puso fin a su disponibilidad. La administración de la seguridad social norteamericana tiene una dirección en Internet, pensada en tanto que servicio público, que elabora actualizaciones y presupuestos para futuras inversiones; durante un tiempo también podía accederse a una información detallada de los ingresos y beneficios de los ciudadanos. «Los abogados que defienden la intimidad de las personas se pusieron en pie de guerra, alegando que esta dirección pública podía usarse fácilmente con malas intenciones por ex esposas/os, propietarios inmobiliarios, agencias de crédito y servicios de búsqueda.» Cediendo a la presión, la Administración cerró la mencionada direc-

* Por ejemplo, el número del carné de identidad. (N. del t.)

ción asegurando que se plantearían volverla a abrir contando con un mayor control de seguridad, incluyendo contraseñas de protección.³⁷

Con independencia de los abusos comerciales, el gobierno ya puede combinar y contrastar datos de sus variados bancos de información. A causa de toda la imaginería asociada con el Gran Hermano, especialmente en Norteamérica, los carnés de identidad levantan más suspicacia entre los ciudadanos que las tarjetas del sector privado, aparentemente más descentralizado, por lo que es probable que se tome bastante tiempo el que se consolide un carné de identidad universal e inteligente. La situación es diferente en otros países, por ejemplo europeos, en los que ya es tradicional el uso del carné de identidad. Pero en el Reino Unido, el gobierno laborista ha recogido la cuestión donde la había dejado el anterior gobierno conservador, considerando tales carnés como «parte de un conjunto de medidas para mejorar los servicios públicos». Aunque los carnés serían voluntarios, los ministros «esperan que todo el mundo decida utilizarlos», por las evidentes ventajas que aportarán.³⁸ Las presiones para una instauración de carnés de identidad universales, y especialmente en versiones electrónicas e inteligentes, aumentarán en un futuro próximo hasta el punto de que será imposible evitarlas. En esta época de claro dominio neoliberal en los gobiernos y programas públicos, las ventajas del carné nacional de identidad son evidentes para los Estados, cada vez más conscientes y protectores con los presupuestos decrecientes de que disponen para los servicios sociales y de bienestar. Pero en una era de globalización, las presiones para la instauración de un carné de identidad inteligente provienen tanto de dentro como de fuera. Los viajes internacionales y la emigración son tanto un requerimiento de la economía internacional como una amenaza potencial para la seguridad: los viajes de negocios y de los profesionales, así como la emigración, son el fundamento de una economía global, pero los movimientos terroristas, el tráfico de drogas, los asesinatos internacionales, el blanqueo financiero, etc., así como

37. Ben Elgin, «Web-accessible records jeopardize Internet User», *ZD Internet Magazine*, 2 de septiembre de 1997; Margot Williams y Robert O'Harrow, Jr., «Online Searches Fill in May Holes», *Washington Post*, 8 de marzo de 1998; Blaine Harden, «Paranooids Find a Reason to Be Paranoid», *Washington Post*, 6 de agosto de 1997.

38. Valerie Elliot, «ID Smartcards Back on Agenda. Says Minister: Whitehall's Planned Electronic Revolution Will Mean "Joined-up Government"», *The Times*, Londres, 11 de febrero de 1998.

un amplio e irregular movimiento de refugiados políticos y económicos, socavan los «legítimos» mecanismos de la economía transnacional. Por el momento, los pasaportes se emiten de manera que puedan ser verificados por máquinas: se exploran en los mostradores de facturación y en los controles de inmigración, conectados automáticamente a una base de datos en la que aparece el archivo del portador. En la mayoría de los casos no hay menciones especiales, pero hay una minoría fichada por distintas razones, por lo que sus portadores pueden ser detenidos en el momento o denegárseles la entrada. La información sobre vuelos y billetes internacionales se concentra en una base de datos común a la que tienen acceso todos los transportistas, lo que resulta muy conveniente, ya que facilita la resolución de cualquier problema derivado de la cancelación o pérdida de un vuelo. No se suele saber que tal base de datos es rutinariamente accesible al NSA de Estados Unidos, así como a otros servicios policiales y de inteligencia norteamericanos. La NSA tiene, por tanto, acceso a un control global de todas las personas que viajan por avión, con lo que complementa su acceso global a las telecomunicaciones. El problema reside, sin embargo, en los pasaportes y documentos de vuelo robados o falsificados, por lo que la NSA sólo puede estar segura de qué documentos están viajando entre países, pero nunca pueden tener la misma certeza sobre las personas que llevan dichos documentos. Con la instauración universal de carnés de identidad inteligentes —algo que, supuestamente, queda aún muy lejos— cada pasaporte estará vinculado, únicamente y de forma verificable, a las características personales de su portador. Llegados a este punto, se establecerá un verdadero régimen de control internacional, así como, sin duda, una serie de coacciones a las libertades individuales.

Cuando la pantalla te devuelve la mirada: dispositivos de búsqueda y *cookies*

El «incremento de potencialidades» que ofrece Internet, tanto a los individuos como a los grupos, ha generado mucho entusiasmo. Trataremos más adelante las cuestiones políticas que todo ello conlleva³⁹ pero, de hecho, las nuevas tecnologías de la información in-

39. Véase el capítulo 7.

crementan sin duda las capacidades y el poder de las personas. Así ocurrió con las primeras tecnologías de la información: la prensa escrita socavó el poder del papado y contribuyó a la expansión de la Reforma protestante, además de fomentar el individualismo, la emergencia de una burguesía urbana y el nacimiento de un humanismo científico.⁴⁰ El teléfono provocó una drástica reducción de los límites que impone la distancia, así como la radio, y especialmente la televisión, ofrecieron mundos hasta entonces desconocidos y remotos. Pero, aunque la prensa otorgó más libertad, también fue censurada: muchos libros fueron prohibidos y quemados; los teléfonos han sido intervenidos, y la radio y la televisión pueden ser tanto instrumentos educativos como de propaganda.

Las nuevas tecnologías de la información son un arma de doble filo: aumentan nuestras capacidades y nuestro poder, pero también hacen a sus usuarios más vulnerables a la vigilancia y a la manipulación. Ambos aspectos son inseparables: es precisamente lo que aumenta nuestras capacidades lo que nos hace más vulnerables. El ciberespacio no constituye una excepción: navegar por la Red nos permite nuevas formas de comunicación con personas de todo el mundo, pero también puede significar que todas nuestras comunicaciones sean interceptadas por terceros que, al mismo tiempo, nos localizan e identifican. Esto puede querer decir que otras personas o grupos están construyendo un perfil en red de nosotros mismos: qué direcciones visitamos, qué anuncios nos interesan, qué productos compramos, a qué periódicos nos suscribimos o con quién mantenemos correspondencia electrónica. También puede significar que nos han copiado el número de nuestra tarjeta de crédito, y que está usándose a nuestras espaldas. Podría incluso ocurrir que personas totalmente desconocidas accedan al disco duro de nuestro ordenador personal, observen lo que guardamos en él y, quizás, decidan cambiar o borrar ciertos archivos, o transmitirnos un virus. Desde luego, puede no ocurrirnos nunca nada parecido. Pero podría ocurrir.

Entre las maravillosas ventajas que Internet ofrece a sus usuarios, cabe mencionar los dispositivos de búsqueda que rastrean la Red para traernos todas las direcciones que coinciden con los tér-

40. Ronald J. Deibert. *Parchment, Printing, and Hypermedia: Communications in World Order Transformation*. Nueva York, Columbia University Press, 1997, págs. 47-110.

minos que hemos introducido. Por ejemplo, al escribir este libro, he necesitado a menudo alguna referencia concreta o alguna cita, sin disponer de las fuentes adecuadas en aquel momento. En otros tiempos, un escritor en esta situación hubiera tenido que buscar el libro que pudiese contener tales referencias en su biblioteca particular; si no lo encontraba, hubiera tenido que desplazarse a una biblioteca para encontrarlo. Con Internet, el tiempo de búsqueda se reduce drásticamente: no es necesario desplazarse más allá del ordenador. Además, se trata de un servicio totalmente gratuito: puedo descargar la cita en mi ordenador y, acto seguido, engancharla en el lugar elegido de mi texto. Tal tecnología aumenta sin duda nuestras capacidades.

Pero precisamente este mismo poder de búsqueda puede invertirse y usarse para fines mucho menos benignos. Prueben esto: si han entregado alguna vez su número de teléfono a un desconocido —lo que ocurre fácilmente en cualquier negocio o transacción por teléfono— diríjase a la siguiente dirección de AT&T: www.anywho.com, tecleen su teléfono, y entonces podrán leer información detallada sobre su propia localización, incluyendo un mapa para acceder a ella; una base de datos instantánea para «cibercazadores». Existe mucha información personal en la Red a la que puede accederse por curiosidad, por intereses comerciales, o por motivos más siniestros. Los agentes de información, que ofrecen búsquedas expertas, son a menudo capaces de acceder a bases de datos restringidas, a las que un usuario normal sólo podría acceder con muchas dificultades o le sería sencillamente imposible.⁴¹ Los métodos de los detectives privados han recorrido un largo camino desde la antigua imagen que ofrecía Raymond Chandler del sabueso del pasado; actualmente, es muy posible que estén navegando por la Red en busca de información para atrapar a una esposa infiel o a un socio de negocios tramposo. Del mismo modo, es probable que los criminales naveguen por el ciberespacio en búsqueda de víctimas, como si vagaran por callejuelas.

No es de extrañar que, adelantándose a las posibles regulaciones gubernamentales, el Consejo Industrial de las Tecnologías de la Información, un consorcio privado de agentes de información y de em-

41. Charles Pappas. «To Surf and Protect». *Yahoo Internet Life*, diciembre de 1997.

presas de evaluación y aval de créditos, haya introducido un conjunto de «principios» y «consejos» para proteger a los usuarios de la Red. Tales principios son totalmente voluntarios, sin ninguna previsión de que se conviertan en legislación.⁴² Los individuos tienen que «decidir excluirse» por sí mismos, indicando a las empresas suscritas a tal acuerdo que no desean que su información personal se inserte en las bases de datos de acceso público. Los críticos han señalado que la mayoría de la gente ni siquiera sabe que tales bases de datos existen.⁴³ Dichos acuerdos fueron tomados bajo el beneplácito de la Comisión Federal del Comercio (FTC) norteamericana y de la Administración Clinton, y «pusieron en marcha la primera prueba significativa de la política sobre la intimidad defendida por la Administración Clinton, cuyo objetivo explícito consiste en proteger la vida privada de las personas en la era de Internet, sin recurrir a una nueva legislación o regulación oficial». La FTC tiene previsto hacer una inspección de 1.200 direcciones comerciales de Internet para «calibrar el efecto de tal autorregulación en la intimidad de los consumidores», presentando posteriormente un informe al Congreso.⁴⁴ Como era de esperar, sin embargo, la tendencia de la Administración Clinton a «dejar que el mercado se regule a sí mismo» no podía ir más allá. Los acuerdos alcanzados dejaron algo al margen: las agencias y organismos al servicio de la ley podían seguir teniendo un fácil acceso a las mencionadas bases de datos. Tradicionalmente, tanto los gobiernos como la justicia han puesto límites a la obtención de información sobre los ciudadanos por parte de la policía sin una citación judicial.⁴⁵ En la era del ciberespacio, la autorregulación de la industria y del comercio permite a los agentes de la ley ir más allá de las directrices establecidas para proteger la intimidad de los ciudadanos.

Las capacidades de búsqueda apenas agotan las bases tecnológicas orientadas a la vigilancia de las actividades de la Red. Entre las técnicas más interesantes de cibervigilancia cabe destacar las

42. «Tech Firms: Don't Worry. We'll Guard Your Privacy», *Reuters*, 8 de diciembre de 1997.

43. Katharine Q. Seelye. «Companies Agree to Protect Personal Data», *New York Times*, 18 de diciembre de 1997.

44. «FTC to Survey Web Privacy Policies», *Wired News*, 2 de marzo de 1998.

45. John Markoff. «Pact to Test Controls on Data», *New York Times*, 18 de diciembre de 1997.

cookies.^{*} Los usuarios que se registran en alguna dirección pública o *website*, o que descargan software desde la Red a su ordenador personal, colocan directamente tales *cookies* en sus discos duros; consisten en una serie de números que identifican al usuario para el vendedor o suministrador, por lo que aceleran las transacciones. Por ejemplo, si me suscribo a un servicio, una *cookie* implantada en mi ordenador me reconoce cada vez que entro en la dirección del servicio, ahorrándome el largo proceso de identificarme y dar la contraseña. Por esta razón se han hecho populares entre los usuarios, y aún más entre los propietarios de las direcciones en la Red, ya que codifican información sobre el usuario recopilada en el momento de registrarse, pero potencialmente ampliable mediante la información disponible en otras direcciones y bases de datos, gracias a los vínculos basados en la misma identidad del usuario. A pesar de esta comodidades, las *cookies* pueden estar realmente envenenadas: son una llave para acceder a los discos duros de los ordenadores, con un impresionante potencial de abuso.⁴⁶ A medida que se han ido conociendo sus peligros potenciales, han aparecido varios productos defensivos, como los programas «trituradores de *cookies*», que pueden removerlas del disco duro. Y algunos navegadores de la Red como Netscape ofrecen la posibilidad a sus usuarios de rechazar todas las *cookies*, o de ser advertidos anticipadamente cada vez que se instalará una o que está a punto de activarse una ya instalada. La mayoría de los usuarios, sin embargo, aunque rechacen de vez en cuando alguna *cookie* de fuentes sospechosas, tenderán probablemente a facilitar a menudo las operaciones, aceptando su instalación automática. Yo mismo hice el experimento de probar la opción que consiste en hacer que el ordenador pida permiso cada vez antes de instalar una *cookie* pero, en menos de veinticuatro horas, ante la avalancha de mensajes que invadía mi pantalla, opté por menos seguridad pero más comodidad; tal es el paradigma del dilema que plantea la tecnología de Internet: entre el incremento de capacidades, por un lado, y la vigilancia, por otro.

* *Cookies*, literalmente, significa galletas, pero en lenguaje informático, incluso en castellano, se utiliza la palabra inglesa para indicar los códigos incrustados en el disco duro que identifican al usuario de la Red.

46. Robert O'Harrow, Jr., «Picking up on cookie crumbs», *Washington Post*, 9 de marzo de 1998.

@ El fin del ingenio: la vigilancia en el correo electrónico

El correo electrónico (*e-mail*) está en el corazón de la popularidad de Internet en tanto que tecnología de la comunicación, y se está convirtiendo rápidamente y a distancia en el sistema más usado para la comunicación interpersonal y entre organizaciones en el mundo desarrollado, sustituyendo al «correo caracol»,* en tanto que viejo sistema postal cómicamente limitado. Incluso el fax, que experimentó un rápido auge por su ubicuidad en los negocios y oficinas caseras, declina a medida que los usuarios descubren que incluso largos documentos pueden transferirse instantáneamente por correo electrónico, en tanto que «nexo» (*attachment*), de ordenador a ordenador o de una red a otra en cualquier lugar del mundo. El correo electrónico ilustra perfectamente el incremento de capacidades que ofrece Internet, al abolir virtualmente todo límite espacial o temporal en la comunicación. En un futuro próximo, esta tecnología podría fusionarse con el teléfono, dando lugar a un sistema híbrido de comunicación en tiempo real en el que la voz y el texto se combinan, incluso en el mismo mensaje.⁴⁷

Dicho todo esto, el correo electrónico es la forma más insegura de comunicación. La mayoría de las legislaciones prohíben abrir el correo sin autorización y, además, casi todo el mundo lo condena en tanto que vulnera la intimidad de las personas. En tiempo de guerra o en condiciones excepcionales, los gobiernos han exigido una censura del correo, y muchos siguen usándola como una arma de represión, en cuyo caso se constriñe mediante estipulaciones y advertencias de procedimiento. Sin embargo, la misma facilidad con que el correo electrónico circula alrededor del mundo ha transformado la noción de las relaciones comunicativas. Tal y como ha comentado el criptógrafo Whitfield Diffie en una declaración al Congreso: «La Constitución no menciona ningún derecho a la conversación privada. Supongo que nunca se le ocurrió a nadie por aquel entonces que pudiese impedirse. Ahora, sin embargo, estamos entrando en un mundo en el que la comunicación electrónica es tan buena y barata que emergerán negocios amistosos y relaciones personales entre

* Correo convencional (*N. del e.*)

47. «Net could revolutionize phone service: New phone technology could be "unstoppable"». *USA Today*, 10 de febrero de 1998.

partes que sólo muy de vez en cuando podrán permitirse el lujo de viajar para visitarse mutuamente. Si no aceptamos el derecho de estas personas a proteger la intimidad de sus comunicaciones, daremos un paso de gigante hacia un mundo en el que la comunicación íntima sólo pertenecerá a los ricos».⁴⁸

La vigilancia en el correo electrónico tiene muy pocos límites, tanto públicos como privados, a pesar su creciente importancia. Ya hemos señalado que, a escala gubernamental, la red UKUSA de los servicios de inteligencia, mediante el programa ECHELON, intercepta casi toda la comunicación que circula por los sistemas de comunicación vía satélite. Pero esto sólo es una parte del problema: los servidores de Internet pueden archivar todas las entradas y salidas de correo electrónico. Los empresarios no sólo pueden archivar todo el correo electrónico que circula por la red de ordenadores de sus empresas, sino que pueden incluso exigir el derecho a leer la correspondencia de sus empleados, alegando que, puesto que los ordenadores son propiedad de la empresa, también lo es lo que éstos contengan. Amitai Etzioni, el prestigioso sociólogo y filósofo de la comunicación, citando fallos judiciales y la ausencia de protección legislativa estatal o federal, ha criticado que «el derecho a la intimidad de un empleado en el correo electrónico tiene muy poca o ninguna protección legal». Con informes que sugieren que más de un tercio de las empresas controlan regularmente a sus empleados electrónicamente, con técnicas que incluyen el chequeo del correo electrónico, Etzioni concluye que los empresarios están socavando cualquier sentimiento de comunidad en los lugares de trabajo.⁴⁹ Esta cuestión también presenta otra vertiente: tanto los gobiernos como los empresarios tienen un legítimo interés en asegurarse de que los sistemas de comunicación que ponen a disposición de otros no se usen para fines criminales o inmorales y, realmente, algunas mujeres y minorías raciales han reivindicado protección contra el acoso sexual o contra los mensajes racistas que reciben de otros empleados con el fin de intimidarlos. En última instancia, puede que el acceso al correo electrónico con propósitos ilegales o corruptos sea, en algunas ocasiones, de interés público: fue gracias al correo electrónico

48. Ashley Dunn, «The Fall and Rise of Privacy», *New York Times*, 24 de septiembre de 1997.

49. Amitai Etzioni, «Some Privacy, Please, for e-mail», *The New York Times*, 23 de noviembre de 1997.

archivado que pudo desvelarse la conspiración del coronel Oliver North y otros en el Irangate.⁵⁰

Uno de los aspectos más preocupantes de la interceptación del correo electrónico es que tanto el emisor como el receptor pueden ser identificados y localizados mediante su dirección electrónica, gracias al ubicuo signo «@». Tal vulnerabilidad ha impulsado a algunos usuarios a ingeniar sistemas que puedan garantizar el anonimato frente a posibles fisgones como, por ejemplo, los sistemas de «retransmisión» (*re-mailing*): el emisor envía su mensaje electrónico a través de un centro de retransmisión que elimina cualquier marca de identificación que permitiese identificar o localizar a dicho emisor, y luego ocurre lo mismo con los mensajes de respuesta o de entrada hacia dicho emisor. Para cualquier persona preocupada sobre la intimidad, esto puede parecer una buena idea, pero para los gobiernos y servicios de inteligencia y seguridad tal retransmisión suena a tapadera para comunicaciones infames, desde instrucciones para el tráfico de drogas hasta planes terroristas. Se han hecho numerosas acusaciones, aunque sin ninguna comprobación independiente, de que numerosos servicios de inteligencia de países occidentales, incluyendo Estados Unidos, han adoptado una táctica clásica de contraespionaje y han tomado el control de una gran parte de tales servicios de retransmisión.⁵¹ Si hay algo de verdad en estas acusaciones, lo que tendría que ser un servicio para garantizar el anonimato a sus clientes es de hecho un sistema de vigilancia gubernamental. Sean cuales sean los hechos, hay algo evidente: el correo electrónico, a pesar del incremento de capacidades que ofrece, es una forma inherentemente insegura de comunicación, lo que nos lleva a la importante cuestión de la criptografía en Internet. Si parece más o menos inevitable que los gobiernos, los empresarios y otros organismos públicos y privados intercepten y controlen el correo electrónico, entonces la solución quizás consiste en hacer ilegible cualquier mensaje electrónico a toda persona que no sea el receptor previsto intencionalmente.

50. Véase el capítulo 6.

51. Jon Dillon. «Are the Feds sniffing your re-mail?», *Covert Action Quarterly*, junio de 1998.

La guerra de los magos en la Red: encriptar, desencriptar y las puertas celadas

Tal y como hemos señalado en un capítulo precedente,⁵² uno de los grandes triunfos de los servicios de inteligencia aliados fue su capacidad para descifrar los códigos del Eje enemigo, y poder leer así sus comunicaciones militares. Esta aplicación de técnicas matemáticas avanzadas para desentrañar los códigos enemigos era parte de lo que sir Winston Churchill mencionaba con admiración como «guerra de magos». Las proezas de Bletchley Park en el Reino Unido, que permitieron abrir las puertas de los secretos mejor conservados, así como el desciframiento «mágico» de los códigos japoneses por Estados Unidos, sólo fueron dos episodios espectaculares en la carrera entre técnicas de encriptación y desencriptación. Pero el punto débil de la criptografía ha consistido siempre en la necesidad que tienen tanto el emisor como el receptor de usar la misma clave para descifrar los mensajes encriptados, lo que conlleva que haya un acuerdo previo entre ellos o que un servicio de mensajeros traslade las claves de un lado para otro. De aquí provienen los clásicos instrumentos de espionaje: libros con los códigos de desciframiento, o máquinas como la alemana «Enigma» que, una vez en manos del enemigo, podía ser analizada y dominada. Los norteamericanos obtuvieron durante la guerra un libro soviético de claves o códigos que les permitió, tras años de análisis, el desciframiento «Venona» de las comunicaciones soviéticas, con su red de espionaje en Estados Unidos, y la identificación de agentes soviéticos de espionaje atómico. Más recientemente, se ha afirmado que la Agencia de Seguridad Nacional (NSA) ha mantenido durante años un acuerdo secreto con Crypto AG, una empresa suiza que vende tecnología punta en criptografía a diversos países y organizaciones comerciales, permitiendo a la NSA y a los servicios de inteligencia que colaboran con ella un acceso completo a comunicaciones supuestamente secretas.⁵³

La seguridad de las comunicaciones en el ciberespacio progresó a paso de gigante en la década de los setenta, con una aportación fundamental en criptografía denominada «encriptación de clave pú-

52. Véase el capítulo 1.

53. Wayne Madsen, «Crypto AG: the NSA's Trojan Horse?», *Covert Action Quarterly*, 63, invierno de 1998.

blica». A diferencia de la criptografía simétrica, en la que tanto el emisor como el receptor usan la misma clave, la encriptación de clave pública es asimétrica, usando dos claves relacionadas, una pública y la otra privada, siendo imposible derivar por computación la clave privada de la pública. Un sistema de clave pública permite que sólo los receptores de los mensajes encriptados puedan ser capaces de leerlos, ya que sólo combinando ambas claves puede abrirse la información. La clave privada es un valor matemático, un algoritmo denominado a veces puerta celada (*trap door*): si se sabe, dicho valor abre la puerta a la comunicación, pero si se desconoce, la puerta queda cerrada y el mensaje inaccesible. Ashley Dunn ofreció una sencilla descripción de este mecanismo en el *New York Times*:

Alice [...] tiene una caja de seguridad con dos llaves. Una de ellas, que Alice siempre conserva como una llave privada, sólo puede abrir la caja; la otra llave, de la que existen varias copias y está ampliamente difundida, sólo puede cerrarla. Cuando Bob [...] quiere mandar un mensaje a Alice, consigue una llave pública (de cierre), coloca su mensaje en la caja de seguridad abierta y entonces la cierra con su llave pública. Cuando Alice quiere leer el mensaje, abre la caja con su llave privada, y deja luego la caja abierta. De este modo, sólo Alice puede leer los mensajes, pero cualquiera puede enviárselos.⁵⁴

Existen pruebas recientes de que la idea de una clave pública de encriptación fue «descubierta», si éste es el término adecuado, por los criptógrafos británicos que trabajaban en la GCHQ, la agencia que relevó a Bletchley Park al acabarse la guerra (aunque la NSA puede haber estado trabajando con ideas similares incluso antes, desde el principio de la década de los sesenta). Constreñidos por el secreto en interés de la seguridad nacional, los criptógrafos de la GCHQ nunca hicieron público su descubrimiento.⁵⁵ Dos criptógrafos norteamericanos ajenos al Estado secreto, Martin Hellman y Whitfield Diffie, publicaron un texto decisivo en 1976 sobre la clave pública de encriptación. Un año después, otros tres investigado-

54. Ashley Dunn, «Of Keys, Decoders and Personal Privacy», *New York Times*, 1 de octubre de 1997.

55. Peter Wayner, «British Document Outlines Early Encryption Discovery», *New York Times*, 24 de diciembre de 1997.

res llevaron a la práctica tal idea, aportando una puerta celada específica y monodireccional denominada algoritmo RSA.

La clave pública de encriptación significa el fin del monopolio estatal y la democratización de la encriptación. Varios programas de software que permiten encriptar y desencriptar ya están disponibles en el mercado, el más conocido de los cuales es el PGP (Pretty Good Privacy), con un sistema de 128 bits que es seguramente indescifrable, incluso para los ordenadores más desarrollados. En contraste, el actual programa estándar del gobierno norteamericano, el DES, un sistema de clave de 56 bits, pudo ser descifrado en 39 días por un grupo de programadores y aficionados, en una especie de desafío deportivo.⁵⁶ Los sistemas de 128 bits son exponencialmente más complejos que los de 56. Con programas como el PGP en el mercado, se abre la perspectiva de que cada usuario de Internet pueda asegurar sus comunicaciones frente a los ojos fisgones de los competidores, los enemigos e incluso el Estado.

Existen importantes y poderosos grupos de presión a favor de una potente encriptación. Los negocios en la Red nunca habían sido tan vulnerables a la vigilancia indiscreta de cualquier aficionado. Uno de los problemas remite a la preocupación pública sobre la seguridad de la información financiera, como los números de las tarjetas de crédito, usados en la Red para las transacciones comerciales; sin duda podría resolverse mediante la encriptación de clave pública o con las técnicas de reconocimiento biométrico, tales como las huellas dactilares electrónicas introducidas directamente en la Red. Otra cuestión remite a la preocupación corporativa por la propiedad intelectual y su protección, sin duda un problema mayor en la era de la transmisión digital instantánea; usando una versión de la encriptación de clave pública, cinco multinacionales de la informática y la industria electrónica, incluyendo Intel y Sony, han llegado a establecer diversos modos de prevenir las copias ilícitas de los archivos digitales con contenido copyright: «El acuerdo señala un nuevo paso muy prometedor en la siempre delicada relación entre los creadores de expresiones artísticas —películas, música—

56. «Team of Computer Enthusiasts Cracks Government-Endorsed DES Algorithm in Less Than Half The Time Of Previous Challenge», *PRNewswire*, 26 de febrero de 1998.

ca y libros— y las nuevas tecnologías, como Internet, que facilitan tanto la distribución como la posibilidad de piratear el material».⁵⁷

Los gobiernos no están muy satisfechos con la encriptación de clave pública. El gobierno norteamericano, en particular, dado su papel hegemónico en tanto que la única superpotencia que perdura en el mundo y su función policial a escala internacional, es especialmente hostil a la encriptación de clave pública. La Administración Clinton se ha embarcado en varias batallas legislativas para intentar controlar esta tecnología: empezaron con torpes intentos por imponer el llamado «clipper chip», una puerta celada electrónica controlada por el gobierno. Aunque tales intentos fracasaron, la Administración ha exigido un riguroso control de las exportaciones con encriptación de clave pública, y ha doblado sus esfuerzos para conseguir mecanismos legislativos que le permitan controlar las puertas celadas de todos los paquetes privados vendidos en Estados Unidos, lo que ha sido llamado depósito de clave pública. La postura del gobierno, reiterada en diversas ocasiones por el director del FBI, es que la encriptación de clave pública permitirá al crimen organizado y a los grupos terroristas mantener fuera de sus planes a los servicios estatales de seguridad. Cabe señalar que el mismo FBI ha exigido también que se mantengan los estándares del nuevo equipo telefónico, lo que le permitiría seguir interviniendo las líneas telefónicas a voluntad.

Hay muchos aspectos de gran importancia envueltos en esta historia, sin que podamos predecir aún los resultados. Por un lado, podría parecer una clásica cuestión de derechos individuales frente a la seguridad nacional, con los mismos argumentos desplegados en las intervenciones telefónicas, los micrófonos ocultos o los informadores humanos a los que recurre la policía y las fuerzas de seguridad. Pero tal similitud es muy superficial. La tecnología de encriptación con clave pública es totalmente distinta de las medidas convencionales del contraespionaje o de la contravigilancia: es perfectamente capaz, si no se impone una puerta celada gubernamental, de asegurar efectivamente la intimidad de las comunicaciones durante el suficiente tiempo como para neutralizar las capacidades de desciframiento en casi todas sus facetas. Incluso si en el futuro se perfeccionase espectacularmente la habilidad de descifrar, la

57. Greg Miller, «Firms Agree on Digital Anti-Piracy Technology», *Los Angeles Times*, 26 de febrero de 1998.

encriptación a base de 128 bits es tan compleja que cualquier desciframiento tardaría lo suficiente como para satisfacer el deseo de intimidad de la mayoría de la gente y sin duda el suficiente para que tanto los criminales como los terroristas llevaran a cabo sus planes. Además, la disponibilidad actual de estos dispositivos de encriptación conlleva un problema que podríamos calificar de «genio fuera de la botella»: por más controles que se impusieran en el futuro, la tecnología ya estaría disponible para cualquiera que pretenda usarla o distribuirla ilegalmente (apenas un problema en la era de Internet y de la transmisión digital de datos). El control de la exportación por el gobierno de Estados Unidos parecería una estrategia obsoleta, sólo apropiada en la época en que las fronteras nacionales y los controles de aduana podían detener el movimiento transnacional de bienes y servicios. Tampoco han sido muy efectivas las exhortaciones del gobierno norteamericano a otros gobiernos con el fin de obtener acciones similares en sus respectivas jurisdicciones nacionales. El Centro de Información Íntima y Electrónica, un grupo de investigación con base en Washington, descubrió en un informe sobre 243 gobiernos que Estados Unidos es virtualmente el único país democrático e industrializado que pretende regular la encriptación de alta tecnología.⁵⁸ En ausencia de un régimen de control internacional, no hay nada que pueda detener la expansión de la encriptación con clave pública. Un argumento definitivo en contra de puertas celadas gubernamentales es que aquellos con motivos para evitar el control del gobierno evitarían, de todos modos, tales controles; para los ciudadanos y organizaciones que aceptan las reglas democráticas y las legislaciones vigentes, el monopolio estatal de las puertas celadas podría representar un problema de seguridad mayor: ¿qué ocurriría si fallos de seguridad u oficiales corruptos dentro del gobierno proveyesen los secretos a criminales, a grupos terroristas o a Estados hostiles? Una parte importante de las comunicaciones y de los sistemas informáticos quedarían entonces al descubierto frente a una devastadora agresión ciberespacial. La Comisión del presidente Clinton sobre Protección de Infraestructuras Básicas, al mismo tiempo que repite la exigencia de la Administración respecto a un depósito gubernamental de clave pública, tam-

58. Jeri Clausing, «Support for Encryption Is Less Than U.S. Claims, Study Says», *New York Times*, 9 de febrero de 1998.

bién sugiere que el modo más adecuado para obtener una buena seguridad nacional podría consistir en sistemas de encriptación de alta tecnología que hiciesen a las infraestructuras de información invulnerables a cualquier agresión.⁵⁹

Parecería que sólo un bando puede finalmente vencer en esta batalla: la postura del gobierno es teóricamente cuestionable, e imposible de controlar en la práctica; en consecuencia, parece más probable que se produzca finalmente una amplia difusión de la encriptación con alta tecnología. Aunque esta eventualidad ofrecería una cierta protección a criminales y terroristas, también ofrece una amplia protección a los ciudadanos, asociaciones y organizaciones contra la amenaza de una intromisión de intereses públicos o privados. Atendiendo a la impresionante capacidad de intromisión y vigilancia que ofrecen las nuevas tecnologías que hemos estado examinando, este tipo de seguridad descentralizada y democrática podría ser la mejor opción.

El Pequeño Hermano y las niñeras de la Red: la censura en el ciberespacio

La encriptación ofrece seguridad en las comunicaciones del ciberespacio, pero la seguridad respecto al contenido del correo electrónico privado sólo es un aspecto: lo que se dice y está disponible en Internet ha levantado un conjunto muy distinto de preocupaciones en torno a la censura. Existe, en efecto, un cierto pánico público respecto a la amenaza que Internet plantea a la moral, especialmente con relación a la pornografía y a la apología de la violencia, mientras que Internet en tanto que instrumento de subversión política ha preocupado menos en los países occidentales que en el Tercer Mundo, aspecto sobre el que volveremos.⁶⁰ La alarma respecto a la pornografía y la propaganda racista ha circulado con estruendo por todo el mundo occidental, y se han propuesto, e incluso en algunos casos llevado a la práctica, diversas medidas para contrarrestarlas. La in-

59. Un resumen de los hallazgos ha sido publicado a finales de 1997: Comisión del presidente Clinton sobre Protección de Infraestructuras Básicas, *Critical Foundations: Thinking Differently*; véase Peter Wayner, «U.S. Commission finds that nation is vulnerable to cyberterrorism», *New York Times*, 23 de octubre de 1997; y Chris Oakes, «A New Crypto Furor», *Wired News*, 7 de noviembre de 1997.

60. Véase el capítulo 6.

tensidad del pánico puede quizás atribuirse a la convergencia de dos factores. En primer lugar, la introducción de un nuevo medio de comunicación espectacularmente diferente siempre ha precipitado la ansiedad social: la naciente industria del cine fue constantemente denunciada como inmoral y subversiva, y Hollywood se ha comparado a menudo con Sodoma y Gomorra, así que la censura local o gubernamental se aplicó desde los inicios de la distribución cinematográfica. Como la televisión, cada vez bajo una mayor presión para ser censurada, Internet parece especialmente subversiva por el hecho de introducirse directamente en los hogares, y ser por lo tanto accesible a los niños (que pueden tener más astucia tecnológica que sus padres). Además, la naturaleza ilimitada de Internet también puede incrementar el pánico. En segundo lugar, la tecnología de la Red ha coincidido, en numerosas sociedades occidentales, con el incremento de tensiones sociales y culturales en relación con las diferencias de género, raciales y étnicas. Las campañas en contra de la pornografía han provocado curiosas alianzas entre los conservadores de la mayoría moral y las feministas. Las revisiones y negociaciones para una mayor pluralidad cultural frente a las tradicionales hegemonías han impulsado reivindicaciones a favor de una prohibición legal de la apología de la violencia. Al mismo tiempo, la atmósfera fronteriza de Internet parece haber canalizado una gran cantidad de pornografía y manifestaciones racistas en este nuevo medio de comunicación, en el que prevalece la mayor libertad frente a la censura y a regulaciones de cualquier tipo. Una vez más, el ancestral grito de «tendría que haber una ley» resuena por todas partes, un grito que, irónicamente, proviene casi siempre de aquellos que son más vehementes con relación al libre mercado y para mantener al Estado al margen de la sociedad.

Como ocurre generalmente con este tipo de pánicos, el medio se confunde con el mensaje: Internet, así como la panoplia de medios en los que se inserta, se convierten en la diana de todos los ataques, en lugar de los abusos y malos usos a los que se les puede someter. Pero la naturaleza inusual de esta nueva tecnología convierte a la censura en un problema mucho más complejo, difícil y quizás incluso intratable. Una vez más, podemos apreciar una de las paradojas fundamentales de este nuevo medio de comunicación, que tanto incrementa la capacidad de los usuarios como los hace vulnerables a la supervisión y al control.

La libertad de expresión de un racista, de un antisemita, de un pederasta o de un violador fantasioso y misógino, puede ser una amenaza directa, o por lo menos causa de perjuicio y ansiedad, para las minorías raciales, los judíos, los niños y las mujeres. Esto es, desde luego, tan cierto para Internet como para cualquier otro medio de comunicación, como la imprenta o el vídeo. La diferencia respecto a Internet es que no permite tan fácilmente el control o la prohibición por parte de las autoridades locales o nacionales. El resto de los medios de comunicación depende de lugares específicos de producción y distribución en los que la ley puede aplicarse, pero el ciberespacio trasciende todas las fronteras nacionales: aunque una dirección pública en Internet (*website*) puede introducirse desde cualquier localidad, una vez en la Red, se mueve como el mercurio. Un ejemplo relativamente trivial: algunos países, como Canadá y Francia, han prohibido la publicación de sondeos electorales durante un cierto periodo de tiempo antes de unas elecciones nacionales. En ambos países hubo dichas elecciones en 1997, y en ambos hubo, hasta el último momento, varias direcciones y páginas *web* de Internet en las que podían consultarse diversos sondeos electorales, entre otro tipo de informaciones y propaganda; cuando llegó el momento en que la prohibición se ponía efectivamente en marcha para la prensa, la radio y la televisión, las direcciones públicas de Internet sencillamente saltaron a las denominadas direcciones reflejas (*mirror sites*), situadas en otros países, ajenos a la jurisdicción francesa o canadiense, pero tan accesibles desde Internet como lo eran antes del salto.⁶¹ En consecuencia, ¿cómo pueden los Estados censurar direcciones de Internet que pueden eludir sus jurisdicciones, aunque se dirijan a la ciudadanía nacional mediante sus mensajes e imágenes? ¿Puede limitarse la libertad de los mensajeros con la intención de minimizar la vulnerabilidad de aquellos a los que tales mensajes amenazan?

No existe ninguna duda de que la opinión pública exige a voces un cierto control de la Red. Un informe canadiense mostraba una clara demanda social de censura, especialmente por parte de mujeres, sobre todo madres con niños pequeños. Los encuestados sugerían que las dificultades tecnológicas para una censura en Internet no eran un elemento disuasorio para tales exigencias: «Existe un impe-

61. Andy Riga, «Web sites move south to dodge election law», *Montreal Gazette*, 30 de mayo de 1997.

rativo moral en juego. La gente puede saber que hay obstáculos técnicos, pero quiere que alguien siga intentándolo de todos modos». ⁶² Con la opinión pública sensibilizada, los políticos no pueden andar lejos. La respuesta inicial del gobierno de Estados Unidos se alineó con el «tendría que haber una ley» popular. La Administración Clinton presentó a la Corte Suprema el Acta para la Decencia en las Comunicaciones, que pretendía proteger a los niños del material indecente que invade la Red: la publicación de dicho material de modo que pudiese ser accesible para las personas con menos de 18 años era considerada un acto criminal, imponiéndose castigos de hasta dos años de cárcel y 250.000 dólares en multas. Tal propuesta fue inmediatamente desafiada por diversos grupos de defensa de las libertades civiles, y numerosas partes del Acta fueron eliminadas por la Corte Suprema en tanto que inconstitucionales. Esto no detuvo a los legisladores estatales, que intentaron presentar sus propias leyes, ni al Congreso, que introdujo versiones modificadas del Acta fracasada. ⁶³ Sin embargo, la atención se ha desplazado recientemente hacia una versión mucho más ingeniosa de autocensura en la Red: la Plataforma para la Selección del Contenido de Internet (PICS) está adaptada a servidores de Internet de gran escala y trabaja con el navegador de Microsoft, el Explorer; su función consiste en bloquear cierto tipo de búsquedas mediante unas etiquetas electrónicas fijadas en direcciones específicas. El usuario no se da cuenta de este bloqueo: sólo recibe las coincidencias que le trae el buscador (y que han superado la censura) mediante el término introducido. Empresas como CyberPatrol y NetNanny han desarrollado listas de lo que es aceptable, usando una combinación de búsquedas automáticas con palabras clave, junto a sus propios juicios de valor. El vicepresidente Al Gore ha considerado loable este desarrollo y ha animado a los padres y a los ciudadanos interesados para que den una nota populista al proceso de filtro, y añadan sus propias propuestas de material indecente para las listas de direcciones proscritas en Internet. ⁶⁴ Instituciones como las bibliotecas y los colegios, que ofrecen amplias

62. Chris Cobb, «Rein in the Net, Canadians Say», *Montreal Gazette*, 22 de diciembre de 1997.

63. Jeri Clausing, «States Keep Up Efforts on Internet Restrictions», *New York Times*, 19 de febrero de 1998.

64. Jeri Clausing, «Gore Announces Efforts to Patrol Internet», *New York Times*, 3 de diciembre de 1997.

facilidades informáticas, han instalado sus propios filtros, a menudo bajo la amenaza de no recibir más ayuda o subvención del gobierno federal.⁶⁵ Algunos defensores de las libertades civiles han empezado a preguntarse si su exitosa campaña contra el Acta para la Decencia en las Comunicaciones no habrá sido de hecho un fracaso: la filtración descentralizada, opaca y no gubernamental puede convertirse en algo mucho peor que el viejo diablo de la censura estatal, tal y como ha argumentado un catedrático de Harvard, Lawrence Lessig. Las PICS pueden ser impuestas por cualquiera, en un ordenador personal, en la red de una empresa, en un servidor de Internet e incluso en un país, sin que los usuarios finales tengan ningún conocimiento de ello, lo cual facilita sin duda a los censores centralistas. «La combinación del software de filtro con las PICS conduce hacia una arquitectura rígida de bloqueos, que es antagónica con los valores originales de Internet encarnados en la libertad de movimiento y el incremento de la comunicación.»⁶⁶

A medida que se acumulaban las experiencias con las PICS, así como la práctica de CyberPatrol, NetNanny y otros servicios similares, también aumentaron las críticas sobre los criterios empleados por tales censores privados. Por ejemplo, los grupos de gays y lesbianas vieron como sus páginas *web* se excluían sistemáticamente, quizás por presunciones homofóbicas, o simplemente por la exclusión en los buscadores de cualquier término que se refiera al sexo. En algunos casos, los juicios ideológicos son bastante descarados: la Organización Nacional de las Mujeres (NOW) tenía una dirección en Internet bloqueada porque CyberPatrol declaró que «es bien sabido que su tendencia es lesbiana [!]». En otros casos, la censura puede consistir sencillamente en el resultado inadvertido de la limitación de términos de búsqueda: un club de fútbol que usaba la expresión «chicos menores de 12 años» fue bloqueado por considerarse una posible dirección pederasta.⁶⁷ Sin embargo, en una censura privada

65. Pamela Mendels, «Plan Linking Internet Subsidy to Filters Finds Critics», *New York Times*, 24 de enero de 1998.

66. Carl S. Kaplan, «Is a Better CDA Preferable To Opaque Censorship?», *New York Times*, 30 de octubre de 1997.

67. Carl S. Kaplan, «Filtering Companies Assailed for Blocking "Unpopular" Voices», *New York Times*, 11 de diciembre de 1997; Matt Richtel, «Filters Use Different Approaches And Get Different Results», *New York Times*, 31 de diciembre de 1998.

y descentralizada de este tipo, surge un problema de responsabilidades: ¿a quién hay que pedir cuentas o dirigir una queja? La cuestión se vuelve aún más complicada cuando los filtros se desarrollan con la participación de ciudadanos interesados.

Parece irónico que en el difuso y descentralizado mundo de Internet se haya desarrollado un método difuso y descentralizado de autocensura que se muestra tan difícil de afrontar e incluso de comprender. La antigua y centralizada censura estatal en las democracias liberales podía por lo menos ser bastante evidente y señalable.

Del taylorismo a la transparencia: trabajadores vigilados

La paradoja entre el incremento de capacidades y una mayor vulnerabilidad es especialmente intensa en relación con la expansión de las nuevas tecnologías en los lugares de trabajo. El taylorismo, o la gestión «científica», con sus estudios sobre la temporalidad y los movimientos de los trabajadores para aumentar la eficacia productiva, representa la mayor ideología panóptica en la etapa fordista, relativa a las cadenas de montaje, del capitalismo industrial.⁶⁸ La informatización de los puestos de trabajo, junto a otras nuevas tecnologías de vigilancia institucional, como las tarjetas inteligentes de identificación o las etiquetas electrónicas, podrían parecer una simple extensión del poder de gestión sobre los trabajadores, y así es como lo han descrito algunos críticos y observadores.⁶⁹ También se ha descrito como la progresiva eliminación de los puestos de trabajo y la consiguiente creación de una masa permanente de desempleados e infraempleados.⁷⁰ Esta última consideración remite a otro conjunto de cuestiones más allá del alcance de este libro. Sin embargo, para los trabajadores en activo, la informatización de sus puestos de trabajo puede significar una situación más compleja y ambigua de lo que la noción de taylorismo electrónicamente expandido podría sugerir. Para muchos trabajadores, un ordenador conectado a una red representa mayor capacidad y facilidades en el trabajo diario. Si sólo

68. Véase el capítulo 2.

69. Heather Menzies, *Whose Brave New World? The Information Highway and The New Economy*, Toronto, Between The Lines, 1996, págs. 125-128.

70. David F. Noble, *Progress Without People: New Technology, Unemployment, and the Message of Resistance*, Toronto, Between The Lines, 1995.

se tratara de una cuestión cuantitativa, de un simple aumento de la velocidad en que pueden resolverse los problemas y las transacciones, la informatización conllevaría sencillamente un incremento de la productividad, y por lo tanto un incremento del taylorismo. Así puede ocurrir con muchos trabajadores que se ven obligados a asumir la velocidad de su ordenador en una red informática, lo que sustituiría a las clásicas cadenas de montaje. Pero en muchos otros casos, la informatización significa un cierto traspaso de responsabilidades hacia abajo, desde los gestores hasta los trabajadores menos cualificados.

Un ejemplo entre otros: la introducción de terminales de ordenador conectadas a extensas bases de datos en los coches patrulla de la policía ha coincidido con el inicio de la «policía comunitaria» en tanto que un nuevo modelo popular que, entre otras cosas, permite a los agentes tomar mayores decisiones en el lugar de los hechos. El agente tiene, mediante la terminal informática de su coche patrulla, una cantidad impresionante de datos a su disposición, a partir de la simple matrícula de un vehículo: identidad, residencia, trabajo, número de la seguridad social, ficha policial y antecedentes, si existen, e incluso, quizás, datos financieros; todo ello con sólo teclear unos números. Al mismo tiempo, los informes sobre cualquier incidente pueden ser rellenados sin necesidad de volver a la comisaría. Tales desarrollos tienen un efecto doble. Inevitablemente, diluyen la jerarquía y descentralizan las estructuras tradicionales de supervisión. Según Richard Ericson y Kevin Haggerty, «las tecnologías comunicativas permiten la dispersión de las estructuras policiales y de sus tareas en una miríada de microcentros de saber y de poder».⁷¹ Sin embargo, según los mismos autores, «cada tecleo en su terminal también “teclea” al agente en términos de cantidad y calidad respecto de sus actuaciones y saber hacer y, por lo tanto, disciplinan al agente en tanto que trabajador útil, sin la necesidad de una supervisión directa y tradicional [...] la terminal de su ordenador en el coche patrulla es una vigilancia permanente e ininterrumpida de su tiempo y de sus movimientos».⁷² En relación con las nociones tradicionales de poder y autoridad, este doble resultado podría parecer profunda-

71. Richard V. Ericson y Kevin D. Haggerty, *Policing the Risk Society*, Toronto, University of Toronto Press, 1997, pág. 445.

72. *Ibíd.*, pág. 432.

mente contradictorio pero, a la luz de las nuevas tecnologías, y de la consiguiente transformación tanto de las comunicaciones como de las estructuras de autoridad, no existe contradicción. Los trabajadores están más estrechamente vigilados que nunca, pero la dispersión de la información reorganiza simultáneamente la verticalidad y la horizontalidad de las estructuras de supervisión. Los ordenadores, en cierto sentido, permiten a los trabajadores supervisarse ellos mismos.

Otro efecto espectacular de la informatización es la dispersión física de los puestos de trabajo. En empresas completamente informatizadas, especialmente aquellas que no producen bienes materiales, ya no es necesario mantener una sede centralizada, de ahí el «teletrabajo» y la «oficina en casa» periférica. Por una parte, los trabajadores disponen de una mayor capacidad de decisión y de ciertas ventajas respecto al lugar de trabajo, además de reducirse los costos y el tiempo de numerosos viajes y transportes. Por otra parte, sólo se trata del reflejo de una extensión de las capacidades de vigilancia empresarial, que ahora pueden introducirse en su casa y registrar con precisión sus horas de trabajo y su productividad. Tal y como corresponde a las empresas líderes en alta tecnología, Silicon Valley ha llevado este proceso un paso más allá:

El teletrabajo internacional ha permitido a las empresas de tecnología [de Estados Unidos] crear un nuevo ámbito de comercio internacional, exportando su trabajo y contratando a programadores de todo el mundo para hacerlo. Tras haber reclutado tantos programadores norteamericanos como podían, ofreciéndoles la posibilidad de navegar por Internet para trabajar desde sus casas en Jakson Hole, Wyoming, o en Boulder, Colorado, tales empresas están ahora introduciéndose en lugares como Suráfrica o Filipinas. Cada vez más, el comercio en el mundo ya no sólo remite a camiones cisterna repletos de crudo Brent o a transbordadores cargados con mercancías, sino también a cables por los que circulan códigos de programas informáticos, diseños de producción, diagramas de ingeniería y fórmulas.⁷³

Sin embargo, la industria de las tecnologías de la información ha pedido al gobierno norteamericano cambios en las regulaciones de

73. Allen R. Myerson, «Virtual Migrants: Need Programmers? Surf Abroad», *New York Times*, 18 de enero de 1998.

inmigración con el objetivo de permitir a más programadores emigrar a Estados Unidos. Parece que la emigración virtual no es suficientemente buena, por lo que la anticuada pero real emigración es aún necesaria cuando hacen falta trabajadores con ciertas habilidades, lo que señala un cierto límite en el concepto de teletrabajo: las personas empleadas alrededor del mundo como teletrabajadores sólo cumplen funciones rutinarias o regulares, como el mantenimiento de programas y ordenadores pero, para la innovación, sigue siendo necesaria una cierta concentración humana, de modo que pueda crearse la sinergia adecuada para la creatividad. De ahí los núcleos alrededor de lugares como Silicon Valley con empresas de alcance internacional.

Incluso a escala regional, el teletrabajo es menos efectivo en las clases ejecutivas y de investigación y desarrollo que en los puestos más bajos de la jerarquía laboral. Los trabajos realmente descentralizados resultan ser el equivalente electrónico del trabajo obrero, como los mensajeros que entregan pizzas a domicilio. Desde el punto de vista de la gestión empresarial, este traspaso de los puestos de trabajo fuera de las oficinas disminuye el coste de mantenimiento infraestructural, que es asumido por los trabajadores, elimina muchas preocupaciones sanitarias y médicas, así como problemas de seguridad, y, al aislar a los trabajadores, disuade a los sindicatos y dificulta la solidaridad. Hay algunos trabajos en los que la vigilancia remota podrá efectuarse con eficiencia al mismo tiempo que los empleados tendrán una mínima capacidad de decisión. Pero este tipo de taylorismo extremo funcionará mal, en general, en las grandes empresas, y sin duda será inadecuado para los cargos medianos y superiores, en los que la gente tendrá más libertad para trabajar con mayor flexibilidad y movilidad, pero tenderá a agruparse y a mantener una cierta proximidad física.

Los «cibersiervos» trabajando sin descanso en sus casas a cambio de una comisión no se insertan generalmente en un sistema comunicativo bidireccional, sino que más bien forman la parte terminal de un sistema de gestión aún no automatizado totalmente, pero que sin duda tiende hacia esa dirección. El correo electrónico en tanto que instrumento de gestión manifiesta una naturaleza muy distinta, ya que elimina los indicios de jerarquía que infectan la comunicación cara a cara: las mujeres ya no serán tan silenciadas por voces masculinas dominantes, las discusiones podrán prescindir más fácil-

mente de los aspectos raciales y étnicos, etc. Los estudios sobre el impacto del correo electrónico en las comunicaciones laborales de las multinacionales y grandes empresas sugieren una cierta disminución del orden jerárquico y una cierta democratización moderada. Desgraciadamente, esta evolución también tiene su lado oscuro: la gente padece mayores grados de inseguridad y de duda al tener que enfrentarse con los dilemas que provoca trabajar en empresas que, al fin y al cabo, son jerárquicas y carecen de indicaciones claras o de protocolos de conducta. La democratización también tiene una faceta volátil. A veces, incapaces de conseguir con buenas maneras la obediencia mediante el lenguaje corporal del estatus y del privilegio, o incapaces de apreciar indicios de conformidad y sumisión, los participantes recurren a la violencia verbal: el fenómeno de «encender» al oponente con agresiones verbales desagradables.⁷⁴

Es muy difícil generalizar sobre el impacto de las nuevas tecnologías de la información en el mundo laboral. David Lyon sugiere que el término «vigilancia desorganizada» puede ser una caracterización adecuada.⁷⁵ Las nuevas tecnologías están transformando a las empresas y al trabajo, pero aún estamos en un periodo de transición y la salida no está clara. La paradoja central, sin embargo, es evidente: en todo este proceso descentralizador de la vigilancia, el aumento de las capacidades está íntimamente vinculado al incremento de la vulnerabilidad.

74. Lee Sproull y Sara Kiesler, «Computers, Networks and Work», *Scientific American*, septiembre de 1991.

75. Lyon, *The Electronic Eye*, págs. 119-135.

5. Las torres oscuras: bases de datos y alienación

De los informes secretos a las bases de datos comerciales

Tras repasar las nuevas tecnologías de vigilancia, examinaremos los *usos* a los que puede someterse la información recopilada por dichas tecnologías, que no sólo facilitan la adquisición de la información, sino también su almacenamiento, su recuperación y su procesamiento. Tales procedimientos convergen en una base de datos, es decir, la sistemática concentración de información organizada en tanto que posesiones relativamente seguras de gobiernos, empresas u otras organizaciones, para fines institucionales específicos. A diferencia de las bibliotecas, en las que se recopilan libros, revistas, diarios y otros materiales mediáticos de los que los lectores pueden disponer según sus intereses e intenciones, las bases de datos se crean y

se organizan para propósitos muy concretos, siguiendo un diseño específico: se escogen y se archivan aquellos datos que responden a ciertas preguntas, y la misma estructura de la base de datos —su clasificación, su orden y los mecanismos de recuperación de la información— reflejan este diseño previo.

En su estructura y propósito, las bases de datos se asemejan a los archivos e informes de los servicios de inteligencia y de seguridad: se crean y se organizan intencionalmente, y se diseñan para ser operativos. Ambos son acumulativos y ampliables y, además, ambos *se alimentan a sí mismos*: cuanto mayor y más detallada es una base de datos o un informe, mayor es la capacidad de extraerle aún más información útil. Las bases de datos son como una investigación en curso de los servicios de inteligencia: cuanta más información se recoja, más indicios habrá que señalarán hacia otros datos. En ambos casos, las nuevas tecnologías de la información aceleran todos los procesos implicados, ya que tanto la recopilación como el almacenamiento y la recuperación pueden automatizarse.

Existen al menos tres diferencias importantes entre las bases de datos y los informes de los servicios de inteligencia. En primer lugar, la información de los servicios de seguridad consiste básicamente, aunque no exclusivamente, en información secreta, que se esconde intencionadamente del dominio público. Las bases de datos muy pocas veces contienen información recopilada de forma encubierta, aunque pueda constituir una parte de ciertas bases de datos (antecedentes penales o datos de Hacienda, por ejemplo). En la mayoría de los casos, sin embargo, las bases de datos, especialmente en el sector privado, remiten a una información recogida libremente o de forma consensual. Se trata de una diferencia importante. Sin embargo, los usos que recibe esta información adquirida de forma consensuada se vinculan muy imperfectamente con tales bases consensuales, otra distinción importante sobre la que volveremos.

Una segunda diferencia entre las bases de datos y los informes de los servicios de inteligencia es que estos últimos, al adquirirse en secreto y por medios encubiertos, tienden a ser celosamente guardados y compartidos sólo, de forma cuidadosa y calculada, con otros servicios de seguridad, en intercambios secretos y para fines de colaboración concretos. Los operadores de bases de datos, por el contrario, acostumbran a considerar sus datos como productos comerciales que pueden y deberían venderse. Los obstáculos para su

comercialización provienen generalmente de fuera: leyes y regulaciones gubernamentales, normas de conducta impuesta por la empresa e incluso, en algunos sectores del mercado, presiones resultantes de la competencia. A menudo los servicios del gobierno también están restringidos, por la ley y en la práctica, respecto al uso que pueden hacer de sus datos, aunque esto también está cambiando a medida que los gobiernos pretenden recuperar el coste de sus inversiones o privatizan sus archivos para obtener beneficios. Generalmente, la dinámica tiende hacia la comercialización de los datos, y esta tendencia es tan fuerte que ya se ha generado una nueva profesión: los agentes de información; incluso los operadores de las bases de datos actúan cada vez más como tales agentes.

La tercera diferencia, muy vinculada a la segunda, es que los informes de seguridad están fuertemente centralizados en un lugar, y presentan una estructura de control jerárquico de los datos. No es de extrañar que, históricamente, hayan servido como contrafuertes de potentes Estados centralizados. Las bases de datos, por el contrario, tienden a una dispersión horizontal y a la descentralización. Su misma emergencia ha coincidido con la descentralización del Estado, un relativo declive de su poder, y con la supremacía del mercado respecto a la política.

He insistido en los contrastes entre los informes de los servicios de inteligencia y las bases de datos por razones concretas: ambos contienen información personal sobre los ciudadanos que ha sido recogida en función de su posible uso. Ambos procesos de recopilación se basan en la asunción de que tal información es valiosa y constituye un cierto *poder*. Pero tal poder es interpretado de modo muy distinto en cada uno de estos dos procesos de recopilación y organización de la información. El modelo centralizado y secreto ha sido en parte sustituido por el modelo descentralizado y comercial, pero ambos siguen funcionando en paralelo, utilizando las mismas tecnologías, pero de manera algo diferente. Sin embargo, existen importantes similitudes. Ya sean públicas o privadas, gubernamentales o empresariales, las bases de datos contienen generalmente información que puede ser interpretada por máquinas y que está conectada a una red, y se han diseñado los datos a partir de uno o ambos de estos dos objetivos generales: a) evaluación del riesgo y su exclusión; y b) identificación del consumidor y su inclusión. Las bases de datos remiten a una estructura informativa que es inferencial y permite ha-

cer predicciones, razón por la cual son tan útiles tanto al gobierno como a las empresas: pueden decir a quién excluir para evitar riesgos, y a quién dirigirse en tanto que cliente potencial.

De la vigilancia a la infovigilancia

El término «infovigilancia» ha sido acuñado para «describir las prácticas de vigilancia facilitadas por la recopilación masiva y el almacenamiento de grandes cantidades de información personal».¹ La clave para poder gestionar y coordinar un sistema de información aparentemente disperso, descentralizado y desorganizado, radica en la digitalización, el lenguaje universal que permite establecer la comunicación entre las distintas bases de datos. La digitalización es como una moneda universal que permite el flujo de los datos. Aunque la organización de las bases de datos responde a principios específicos, la información puede trasladarse fácilmente de una base de datos a otra, facilitándose asimismo su comercialización. Uno de los aspectos fundamentales para comercializar la información es la coincidencia y la vinculación de datos, gracias a la cual distintos archivos de información, recopilados por separado y organizados de distinto modo, pueden presentar diversas coincidencias, así como vincularse para producir información nueva y valiosa. Las compañías de seguros, por ejemplo, pueden buscar coincidencias, entre los datos de sus pólizas y diversos archivos médicos para comprobar si existen riesgos adicionales que harían aumentar las cuotas. O una compañía de marketing puede proponer nuevos espacios de publicidad a sus clientes, tras encontrar coincidencias entre los consumidores de un canal televisivo de venta directa y los productos que ofrecen sus empresas a los clientes. La vinculación de datos ha hecho posible los agentes de información, y permite la recopilación cruzada de datos, mediante la cual se exploran múltiples bases de datos para extraer toda la información que pueda utilizarse para obtener beneficios. Los datos relativos a los nacimientos, por ejemplo, pueden ser utilizados por empresas que venden productos para bebés,

1. Colin J. Bennett, «The Public Surveillance of Personal Data: A Cross-national Analysis», en David Lyon y Elia Zureik (comps.), *Computers, Surveillance, and Privacy*, Minneapolis, University of Minnesota Press, 1996, pág. 237.

ofreciendo además una información socioeconómica que permitirá estrategias concretas de publicidad y venta. Todas estas prácticas de infovigilancia apuntan a la siguiente realidad: *a pesar de su estructura dispersa y descentralizada, las bases de datos forman un sistema funcional más o menos unificado.*

Oscar Gandy ha identificado once categorías de información personal que ya residen rutinariamente en bases de datos públicas y privadas, interpretables por las máquinas y conectadas a la Red. Tales categorías son:

1. *información personal para identificar y cualificar,*
que incluye certificado de nacimiento, permiso de conducir, pasaporte, censo electoral, registros de vehículos, libro de escolaridad y expediente académico, libro de familia...
2. *información financiera,*
que incluye historial bancario, cuentas bancarias, tarjetas de débito y de cajeros automáticos, tarjetas de crédito [de financiación, monedero, de conexión a la red bancaria], financiaciones actuales y pasadas, impuestos, inversiones y bonos, cheques de viaje...
3. *información sobre pólizas de compañías de seguros,*
que incluye seguros de salud, del automóvil, de la casa, del negocio, con cobertura general o específica, individuales o colectivos...
4. *información sobre servicios sociales,*
que incluye seguridad social, mutuas de salud, ingresos y privilegios laborales, subsidios de desempleo, de incapacidad, pensiones, cupones de servicios gubernamentales, subsidios y privilegios para veteranos...
5. *información sobre servicios domésticos,*
que incluye teléfono, electricidad, gas natural, calefacción, televisión por cable [conexión a Internet], limpieza e higiene, escombros y basuras, seguridad, entregas a domicilio...
6. *información sobre propiedades inmobiliarias,*
relacionada con compras, ventas, alquileres, *leasing*...

7. *información sobre entretenimiento y tiempo libre.*

que incluye itinerarios de viajes, perfiles de esparcimiento, vehículos y alquileres, reservas de alojamiento, de billetes de avión, de barco, de tren, reservas para espectáculos, suscripciones a diarios y revistas, suscripciones a programas de televisión por cable...

8. *información sobre consumo.*

como tarjetas de créditos comerciales, cuentas comerciales, financiaciones, arrendamientos y alquileres, compras e información sobre productos, suscripciones a catálogos, tallas de ropa y zapatos...

9. *información laboral.*

que incluye solicitudes laborales, exámenes médicos, referencias, logros y éxitos laborales, currículum e historial profesional, solicitudes a empresas de colocación laboral...

10. *información educativa.*

que incluye solicitudes de ingreso en escuelas e universidades, libro de escolaridad, expediente académico, referencias, estudios no reglados y actividades extracurriculares, asociación a clubes y a otras organizaciones, premios y sanciones, graduación...

11. *información judicial.*

que incluye expedientes judiciales, servicios de abogados, artículos e informes de prensa, servicios de indexación y resumen...²

¿Cómo se recopilan todas estas categorías de información? Gran parte se obtiene mediante las respuestas facilitadas a formularios, encuestas y cuestionarios. En algunos casos la información es de carácter obligatorio: puede uno acabar en la cárcel si no entrega a Hacienda los datos requeridos. En otros casos es casi obligatoria, como en una solicitud de empleo: si no se facilitan ciertos datos uno puede quedar excluido del trabajo y de sus beneficios. En ciertos casos se

2. Oscar H. Gandy, Jr., *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, Colorado, Westview Press, 1993, pág. 63; y Gandy, «Coming to Terms With the Panoptic Sort», en Lyon y Zureik (comps.), *op. cit.*, pág. 139. He añadido algunos elementos entre corchetes.

trata de información facilitada voluntariamente: el estilo de vida y las preferencias del consumidor remiten generalmente a cuestionarios rellenos en la suscripción a servicios. En muchos casos, ya sea voluntaria u obligatoriamente, la información recogida remite a unos propósitos específicos, pero no existe ninguna garantía de que no se usará para unos propósitos muy distintos, a menudo por instancias muy diferentes de las que recogieron originalmente la información. Cada vez ocurre más que la persona que transmite tal información no sabe que irá a parar a una base de datos, y aún menos cuáles serán los usos a que dará lugar. Es lo que ocurre generalmente con los datos derivados de transacciones comerciales con tarjetas de crédito: el simple hecho de pagar con tarjeta transmite inmediatamente, pero de forma invisible, datos a la empresa de crédito, por un lado, y a la empresa que efectúa la venta, por otro lado. A partir de aquí, los datos podrán circular en muchas otras direcciones. Hay que resaltar que cada nuevo dato añade un nuevo valor gracias a las coincidencias, repeticiones o variaciones que provoca, pero tales valores añadidos nunca vuelven hacia la persona interesada. Aunque sea personal, tal información no tiene un valor de renta para su propietario original; es muy valiosa, sin embargo, para las diversas entidades que se la apropian para su uso e interés particular.

Las bases de datos pueden basarse en categorías de personas y/o en individuos concretos. Las bases de datos gubernamentales tienden a ser muy personalizadas; los datos de Hacienda, por ejemplo, se individualizan con precisión mediante un número de identificación, como el de la seguridad social, gracias al cual se registran todas las transacciones del individuo en cuestión, lo que permite describir su perfil personal y financiero de forma detallada, localizando incluso el momento y el lugar de cada transacción. Cualquier ciudadano declara sus ingresos y patrimonio, pero tal declaración puede comprobarse punto por punto gracias a la base de datos gubernamental, que ya dispone de toda esta información independientemente del declarante; en el caso de que los datos no coincidan, pueden llevarse a cabo audiciones o investigaciones sobre el declarante. A pesar de esta precisa individualización, los datos personales de Hacienda también se insertan en categorías más amplias que remiten a los diversos tipos de contribuyentes. Los datos relativos al nivel de ingresos permiten clasificar a los contribuyentes individuales en grupos impositivos, que son evaluados de forma diferente a medida que au-

menta el valor impositivo de cada grupo. Un contribuyente puede pertenecer a uno o varios grupos, lo cual le puede conllevar exenciones o devoluciones, entre otras posibilidades. En cierto sentido, la personalización de los datos sólo es un requisito para conseguir una categorización más precisa. Lo que realmente interesa al Estado no es el contribuyente X como tal, sino en qué categoría se inserta según sus criterios impositivos; pero para conseguir esta clasificación, el Estado debe «conocer» al contribuyente X y todos sus datos financieros de forma realmente precisa.

En algunos casos en los que los contribuyentes, por ejemplo, se hacen célebres por su actividad y conducta, o tienen un perfil que sugiere evasión de impuestos, la investigación estatal puede orientarse hacia una personalización cualitativa, y no sólo cuantitativa: algunas figuras mafiosas que han conseguido salir airoso de todas sus operaciones y actividades «profesionales» son a veces atrapadas por evasión de impuestos. En algunas ocasiones, personas consideradas detestables por ciertas figuras prominentes del mundo político, se encuentran de pronto envueltos en una investigación impositiva sobre sus asuntos financieros. Cuando esto ocurre, los implicados se quejan generalmente de ser víctimas de una conspiración de sus enemistades políticas o personales, y la opinión pública simpatiza con ellos, o no, según las circunstancias. Una excesiva personalización por parte del Estado dispara señales de alarma y hace pensar que el Estado no es imparcial en la administración de los asuntos públicos. Se supone que una de las características del moderno Estado burocrático es que no se centra en los ciudadanos individuales, sino que los trata en tanto que insertados en categorías más amplias, despersonalizadas y orientadas a la gestión administrativa. La paradoja radica en que para llevar a cabo minuciosamente esta tarea, el Estado necesita una información muy detallada que le permita categorizar eficientemente a sus ciudadanos. Con este objetivo, las nuevas tecnologías de la información permiten conseguir unas bases de datos personalizadas aún más detalladas. Las limitaciones sobre su uso y los controles para evitar posibles abusos han sido una de las preocupaciones de las democracias liberales durante un cierto tiempo, generalmente bajo la forma de leyes de protección de datos y comisiones para investigar cómo resguardar la intimidad de los ciudadanos. Sin embargo, los Estados están claramente interesados en conseguir cada vez más información, en vincular y contrastar los datos

provenientes de distintas fuentes, y en almacenarlos de forma centralizada. La protección de la información confidencial de los ciudadanos, en tanto que una función especializada del Estado, está pues en tensión permanente con el impulso contrario, inherente al Estado, de recopilar datos con el menor número de obstáculos posible, y de usarlos para sus múltiples intereses. Además, aquellos que tienen la función de proteger los datos están en una posición más débil y desaventajada que los burócratas encargados de buscar y usar tales datos.³

Los augurios respecto al control gubernamental de las bases de datos se hacen aún más sombríos con el desarrollo cada vez más importante de conexiones mediante interfaz con el sector privado, lo que conlleva diversas transferencias de datos. Ericson y Haggerty, por ejemplo, concluyen, tras su investigación sobre la institución policial, que la cantidad de información que entra en sus bases de datos, así como la velocidad de acceso a las mismas, han transformado su naturaleza: de ser uno de los servicios más reservados del gobierno ha pasado a convertirse, gracias a las nuevas tecnologías, en un servicio de información para instituciones como las compañías de seguros, las mutuas de la salud u otros servicios de asistencia social. El interés común que comparten tanto la policía como estas organizaciones privadas consiste en la eliminación del riesgo.⁴

Tanto para el sector público como para el privado, evitar el riesgo es la actitud más racional y económica pero, para aquellas personas implicadas de manera adversa por el uso de tal información, las consecuencias pueden variar desde la molestia al desastre. Las consecuencias de unos elevados precios en los seguros automovilísticos pueden fastidiar a los conductores adinerados, pero serán realmente perjudiciales para los más pobres, que dependen del uso de sus coches para ganarse la vida. ¿Qué ocurre cuando una información errónea se introduce en una base de datos y penaliza injustamente a ciertas personas? Las grandes organizaciones burocráticas tienden a ser indiferentes ante quejas individuales, y se resisten a que unos desconocidos puedan revisar sus bases de datos, incluso si estos descono-

3. David H. Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*, Chapter Hill, The University of North Carolina Press, 1989.

4. Richard V. Ericson y Kevin D. Haggerty, *Policing the Risk Society*, Toronto, University of Toronto Press, 1997.

cidos son las personas afectadas. Un hombre de California llamado Bronti Kelly, por ejemplo, perdió en 1990 su trabajo como vendedor en unos grandes almacenes y cada vez que volvía a ser contratado era despedido a los dos días. Esto le ocurrió una docena de veces. ¿La razón? Habían robado la cartera a Kelly con su carnet de identidad y un hombre fue arrestado poco después por robo con sus papeles: durante un cierto tiempo, circuló públicamente por las cortes judiciales una orden de arresto contra Kelly. Todos los posibles empleadores de Kelly comprobaban su currículum en una base de datos para minoristas y mayoristas que está conectada a los archivos judiciales. Aunque la policía de Los Ángeles ha entregado a Kelly un «certificado de inocencia», tal información no está disponible para los buscadores *on-line* de los bancos de datos de las cortes judiciales, por lo que el informe falso de su arresto continúa apareciendo en la base de datos de los mayoristas y minoristas. Kelly se ha arruinado y no puede conseguir un trabajo dentro de su profesión: «Me siento como si estuviese en la Dimensión Desconocida —comenta Kelly— Desearía poder evitar que la gente se encontrase con ese archivo cuando van a contratarme, pero no puedo hacer nada. Es indignante».⁵

Los Pequeños Hermanos desalojan al Gran Hermano

Las leyes de protección de las bases de datos y las comisiones de vigilancia se centrarán más probablemente en el sector público que en el privado. El sector público no sólo se desdibuja dentro del privado sino que, en Estados Unidos, las bases de datos del sector privado están eclipsando a las estatales, tanto por sus dimensiones como por su alcance en la vida cotidiana de los ciudadanos. Gracias a la sofisticada tecnología de vigilancia actualmente disponible, y con las posibilidades actuales de vincular horizontalmente los datos, los agentes y servicios privados de información están haciendo negocios muy rentables. Los Sistemas Geográficos de Información (GIS), por ejemplo,

5. Rajiv Chandrasekaran. «Doors Flung Open to Public Records». *Washington Post*, 8 de marzo de 1998.

disponen de una tecnología punta para ofrecer detallados mapas y fotografías de alta resolución en formato informático [...] Tal tecnología ha demostrado ser una herramienta impresionantemente poderosa, así como muy comercial y lucrativa. El GIS recoge información de los registros públicos y de los bancos de datos del sector privado, proporcionando luego a los domicilios particulares, casa por casa, cualquier información requerida, desde el cálculo de los impuestos a una fotografía del permiso de conducir del ocupante de un vehículo, o detalles del comportamiento de un consumidor [...] El GIS empezó como un servicio que ofrecía mapas terrestres, marinos y espaciales, en cualquier lugar y momento; ha ofrecido innumerables servicios de gran beneficio social, como la identificación del origen de la enfermedad del legionario, o su ayuda a las comunidades del sur de Florida para coordinar los planes de emergencia después del huracán Andrew.

La comercialización de toda esta tecnología ilumina las bases de datos de un modo bastante diferente. En una aplicación, «una empresa puede cargar los números de matrícula de un garaje dentro de un programa, y obtener así el nombre de sus clientes, su dirección, información del censo electoral y otras características demográficas [...] Otro programa transforma un número de teléfono en el perfil detallado de todos los clientes potenciales que llaman a números 900». El seguimiento electrónico de espacios públicos, por razones de seguridad o control del tráfico, pueden ser usados por GIS para rastrear individuos y vehículos. Tal información puede correlacionarse con gran cantidad de otros datos extraídos de registros públicos informatizados. Cada vez hay más servicios gubernamentales con problemas financieros que venden paquetes de información pública a las empresas, o que introducen conexiones de información con el sector privado para hacer aún más atractiva su oferta en el mercado. Hace sólo una década, cuando el FBI solicitó permiso para centralizar todas las bases de datos nacionales, el Congreso lo denegó: «Ahora, el mercado financiero lo ha hecho por ellos». Los servicios gubernamentales como el FBI «simplemente tienen que pagar, como cualquiera».⁶ La tecnología del GIS ha engendrado una industria floreciente que ofrece informes de personas y hogares, para el

6. Nina Bernstein, «Lives on File: Privacy Devalued in Information Economy», *New York Times*, 12 de junio de 1997.

marketing fundamentado en bases de datos, a mutuas de salud, compañías de seguros, agencias inmobiliarias y servicios financieros. Las nuevas fusiones y asociaciones entre empresas de crédito y servicios de datos e información han dado lugar a gigantescos bancos de datos que son «constantemente puestos al día y analizados, produciendo una impredecible cantidad de detalles sobre prácticamente todos los ciudadanos del país».

En este próspero mundo del poder de las bases de datos, podemos mencionar la empresa Acxiom, un nombre no muy familiar, pero descrita por el *New York Times* como una nueva fuerza en este nuevo territorio:

Si la información es como el dinero, una empresa llamada Acxiom es una de las mayores instituciones bancarias de la época [...] Su corazón se esconde tras unas puertas blindadas, que un guía describe como «estancias de producción bélica»: búnkers con techos muy bajos en los que seis robots, dentro de pequeños silos enlazados, contrastan datos a 100 kilómetros por hora, mientras veinte ordenadores centrales tragan mil millones de bits de datos por segundo. El GIS es sólo una parte de la infraestructura informativa. Los ingresos de Acxiom crecieron casi el 50 % durante el año fiscal 1997, hasta 402 millones de dólares. Entre sus principales clientes destacan empresas líderes en información como AT&T, los almacenes Waal-Mart, Citibank, Citicorp, IBM, Allsat y Automatic Data Processing (ADP), que maneja la mitad de las nóminas en Norteamérica...⁷

Acxiom acumula y clasifica información sobre unos 196 millones de norteamericanos. Tiene unos 350 trillones de caracteres de datos sobre consumidores en sus bancos de datos. Dos veces al mes recibe del servicio postal de Estados Unidos todos los cambios de dirección, para no perder el ritmo de la actualidad. Un ejecutivo de Acxiom dijo que «los datos siempre han estado aquí, lo que ocurre es que ahora, con la tecnología, podemos acceder a ellos [...] Actualmente, nuestra capacidad para recoger, clasificar y dar sentido a grandes cantidades de datos es casi ilimitada».⁸

7. Bernstein, *op. cit.*

8. Robert O'Harrow, Jr., «Are Data Firms Getting too Personal?», *Washington Post*, 8 de marzo de 1998.

Las consecuencias para la vida privada de toda esta concentración de datos son múltiples. Una mujer de Ohio aprendió con horror una de ellas cuando recibió por correo una carta de doce páginas escrita a mano por un extraño que parecía saberlo todo de su vida, «desde el día de su nacimiento hasta los nombres de sus revistas favoritas, desde su divorcio hasta el jabón que utilizaba en la ducha». Tales detalles se entretejían con una fantasía sexual, que amenazaba con llevar a la práctica en cuanto tuviese la ocasión de hacerlo.

El autor de la carta era un violador y ladrón convicto, que cumplía condena a tiempo parcial en la cárcel estatal de Texas. Extrajo su nombre, dirección y otros datos personales de un cuestionario que ella y otros millones de consumidores habían recibido por correo, relleno inocentemente, y reenviado a las oficinas postales de Nebraska y Nueva York, esperando recibir cupones y ejemplares gratuitos. Sus respuestas fueron entregadas por camiones de carga a las prisiones estatales de Texas, que tenían un contrato para ocuparse de las encuestas de Metromail, una empresa líder en marketing informativo directo. Cientos de prisioneros que no eran pagados, muchos de los cuales habían sido encarcelados por agresiones sexuales, introdujeron la información en disquetes informáticos para Metromail, que posee una base de datos muy detallada sobre más del 90% de los hogares norteamericanos.⁹

La mujer emprendió un pleito contra Metromail. Su historia, con todo su desagradable sabor, representa un ejemplo extremo de los riesgos que acechan la intimidad de las personas; pero, a largo plazo, aún es más significativa la inmensa cantidad de datos, personales y muy detallados, que pueden ser utilizados por intereses privados para su propio beneficio, y sin tener que rendir cuentas a nadie.

¿La «muerte de la intimidad»?

En 1984, los ciudadanos de Oceana no disponen de ningún espacio libre para su intimidad que escape a la vigilancia y a la intromisión del Gran Hermano. El Estado poseía una base de datos masiva y centralizada en la que acumulaba todo lo que podía saberse de

9. Bernstein, *op. cit.*

cada sujeto. Los Estados actuales tienen una capacidad tecnológica para ejercer una vigilancia, así como para vincular y recuperar datos, muy superior a la que Orwell pudiese imaginarse, y ciertos aspectos del Estado en tanto que Gran Hermano se han hecho efectivamente realidad. Pero son los Pequeños Hermanos del sector privado los que recogen más datos personales de los ciudadanos y los que saben, por ejemplo, qué marca de jabón usa la mujer de Ohio en la ducha. Además, la información que se introduce en tales bases de datos es entregada voluntariamente (como en el caso de la mujer de Ohio), o es adquirida silenciosa e invisiblemente, sin que el sujeto implicado lo sepa. El Gran Hermano exige información, como las declaraciones de renta o las preguntas relativas al censo, por lo que tiende a suscitar resentimiento e incluso, ocasionalmente, resistencia. Los Pequeños Hermanos, por el contrario, casi no inciden en la población, mientras acumulan y clasifican información privada y personal. No disponemos de ningún término consensuado para denominar estas bases de datos dispersas pero centralizadas del sector privado, mientras que el Estado es personificado en tanto que líder y, en regímenes democráticos, se considera que debe legitimarse ante la población, al menos en teoría. Irónicamente, la transparencia monodireccional característica del Estado orwelliano se ha realizado mucho más efectivamente en el sector privado que en el público, en el que la transparencia, al menos hasta un cierto grado, es bidireccional. Tal y como sugería recientemente un periodista del *New York Times*, «quizás estábamos tan concentrados en evitar al Gran Hermano totalitario de Orwell, que no percibimos la llegada de millones de chismosos entrometidos».¹⁰

Joshua Quittner, autor del artículo «The Death of Privacy» («La muerte de la privacidad»),¹¹ publicado en el número de agosto de 1997 de la revista *Time*, sugiere algunos modos para protegerla: usar menos las tarjetas de crédito, no rellenar los formularios de garantía y desconectar los *cookies*. Sin embargo, rechaza la idea de una intervención y regulación del Estado, adoptando el individualismo anti-Estado tan popular y predominante en Estados Unidos. Pero conceptualizar la intimidad exclusivamente en términos de valor o

10. Peter H. Lewis, «Forget Big Brother», », *New York Times*, 19 de marzo de 1998.

11. Joshua Quittner, «Invasion of Privacy», *Time*, 25 de agosto de 1997.

de interés individual refuerza el individualismo atomístico, y sitúa al individuo en conflicto inevitable con la sociedad. De este modo, la intimidad sólo puede definirse negativamente como el «derecho a que nos dejen estar solos». Tal concepción, como ha argumentado Priscilla Regan, aporta una base teórica muy poco consistente para desarrollar una política pública en esa aérea.¹² La autora propone volver a pensar la intimidad como un valor positivo, social y colectivo: el dominio público en una democracia se beneficia de la participación de sujetos libres y en igualdad de condiciones, cuya autonomía se enraíza en un sentimiento auténtico de autoestima que se aporta a una comunidad de semejantes. A pesar de lo atractiva que es su argumentación, sigue manteniendo una posición individualista, ya que es realmente difícil concebir cómo individuos aislados, aunque constituyan un pequeño grupo con ideas semejantes y con el propósito de emprender diversas acciones, podría realmente oponerse a los efectos de la infovigilancia, teniendo en cuenta todo el dinero que la mueve y el poder de las grandes empresas que la promueven.

Quizás la noción de intimidad, como dice Calvin Gotlieb, «ha emergido, ha tenido su época de esplendor, y ha desaparecido».¹³ Gotlieb cree que «a pesar de que generalmente no se admita, la mayoría de la gente no valora suficientemente la intimidad cuando otros intereses entran en juego [...] Los tratos y las transacciones comerciales en los que la intimidad se ha sacrificado son tan comunes y normales que, a efectos prácticos, la intimidad ya no existe». Además, añade Gotlieb, la intimidad no es un asunto político importante, y sin duda en esto tiene razón: la intimidad no aporta votos en las campañas electorales, por lo que los políticos no la incluyen en sus programas y promociones electorales. Por otro lado, cualquier político se apresura a ampliar la vigilancia con la excusa popular de mantener el orden y la seguridad públicas.

En última instancia, la debilidad de los movimientos en contra del abuso de las bases de datos personales quizás resida en los beneficios que la mayoría de la gente percibe al entregar datos personales a grandes firmas y empresas. En el próximo capítulo exploraremos nuestra propia participación en el panóptico. Por ahora es suficiente

12. Priscilla Regan, *Legislating Privacy: Technology, Social Values, and Public Policy*, Chapter Hill. University of North Carolina Press. 1995.

13. Calvin C. Gotlieb. «Privacy: A Concept Whose Time Has Come and Gone», en Lyon y Zureik (comps.). *op. cit.*, págs. 156-171.

recordar que, como señalábamos más arriba, las bases de datos sirven para dos fines muy generales: la evaluación del riesgo (que pretende excluirse) y la identificación del cliente (que pretende incluirse). La exclusión es percibida por la mayoría como algo que ocurre a una minoría de gente marginada, mientras que los beneficios de la inclusión en la economía del consumo son ampliamente apreciados.

Tal apreciación aumenta cuando los beneficios aparecen claramente personalizados, tal y como ocurre en las estrategias *niche*, muy orientadas a ciertos perfiles de clientes, del actual marketing: estrategias que dependen de las nuevas tecnologías de la información. El marketing masivo, que evidentemente aún se practica, es un instrumento muy tosco, un poco como las bombas lanzadas por aviones en la Segunda Guerra Mundial: desde una altura de cientos de metros, apuntando al objetivo a simple vista o por radar, se abrían las compuertas dejando caer las bombas y esperando que ocurriera lo mejor. Las estrategias *niche* del marketing actual se parecen más a las armas inteligentes que los militares usan actualmente: se apunta al objetivo con máxima precisión, y el disparo es controlado y orientado durante toda su trayectoria, hasta el impacto. La clave del nuevo marketing inteligente radica en la información. Los clientes son identificados no como una masa indiferenciada, sino a partir de subgrupos con patrones muy específicos de compra y poder adquisitivo. La acumulación de datos sobre el consumidor, cuando es percibida, tiende a considerarse como algo que facilita y simplifica el consumo. Los alquileres de películas en vídeo mediante cajeros automáticos, por ejemplo, que aceleran sin duda el proceso, también permiten ir perfilando automáticamente los gustos del consumidor a cada alquiler, aspecto del que pocos clientes son conscientes.¹⁴ Para aquellos clientes muy fieles o con un alto poder adquisitivo, el micromarketing puede convertirse en algo realmente muy personalizado. Algunas cadenas de alimentación en Estados Unidos controlan semanalmente los patrones de consumo de sus clientes, y pueden incluso contactar con ellos personalmente para averiguar cómo prefieren ser servidos y atendidos. La conclusión que parece imponerse es que, si se perciben vínculos

14. Robert Bork, candidato republicano a la Corte Suprema, lo aprendió con consternación cuando, hace algunos años, esperaba la confirmación del Senado: sus enemigos basaron sus críticas en el alquiler de películas pornográficas que había hecho en el pasado.

entre la revelación de información personal y las bases de datos de los consumidores, tales vínculos serán valorados en términos positivos y no como algo potencialmente negativo.

Para todos aquellos que quedan excluidos, es difícil que puedan apreciar cualquier aspecto positivo en el ejercicio de tal vigilancia. Pero incluso para todos aquellos incluidos, los beneficios, aunque suficientemente tangibles, esconden aspectos preocupantes. Si la intimidad se conceptualiza negativamente como la defensa de individuos aislados y solitarios frente a la sociedad, su muerte no implica quizás ningún luto o duelo demasiado importante. Pero si pensamos tanto la vigilancia como la intimidad en términos sociales, en tanto que factores complejos que moldean al individuo en sociedad, el resultado es más preocupante.

Ahora todos somos Owen Lattimore

Los lectores quizás recuerden que, en un capítulo precedente,¹⁵ describimos el papel de los servicios de seguridad interna en las democracias liberales, y los mecanismos de encubrimiento para evitar riesgos de seguridad. Nos referimos al caso del académico Owen Lattimore, que se convirtió en un blanco fundamental de la caza de brujas anticomunista de la era McCarthy. Lattimore, que sobrevivió al calvario, escribió sus memorias relatando cómo los archivos de los servicios de seguridad habían construido el retrato de un hombre «que pudo haber existido».

Actualmente todos somos, en cierto sentido, Owen Lattimore. Las bases de datos públicas y privadas que residen en las torres oscuras del ciberespacio contienen oscuras réplicas personales de casi todos los ciudadanos y consumidores. Estos perfiles de datos, u oscuras réplicas personales, están eclipsando de distintas maneras, pero de un modo importante, nuestras personalidades reales.¹⁶ «Somos realmente fantasmas», afirma Don Goldhammer, un administrador de la red informática de la Universidad de Chicago, «cada uno de nosotros está perseguido por un perfil informativo invisible que

15. Véase el capítulo 1.

16. Mark Poster fue uno de los primeros en señalar la existencia de este oscuro mundo, así como algunas de sus consecuencias: *The Mode of Information*, op. cit.

pretende ser lo que somos.»¹⁷ Las personas que han protestado por el alcance nefasto e injustificado de su crédito, por ejemplo, han descubierto que incluso errores sencillos de identificación son casi imposibles de rectificar. Del mismo modo que los guardianes del Estado de seguridad siempre han defendido que cualquier duda debe resolverse en favor del Estado, el poderoso motivo de la aversión al riesgo por parte del capital significa que cualquier duda debe resolverse en favor de los intereses empresariales o corporativos. Las empresas no se preocupan por los errores cometidos o las injusticias perpetradas contra individuos (excepto en los casos en que se genera suficiente publicidad negativa como para dañar su imagen pública), ya que la atención a tales casos no es *rentable*. El objetivo empresarial es evitar el riesgo en nombre de los accionistas; las bases de datos señalan categorías de riesgo, y las acciones se ponen a disposición de todos aquellos cuyo perfil no se sitúe en tales categorías. El resultado es una especie de selección social: algunas personas son efectivamente excluidas de su plena ciudadanía, no del Estado, pero sí de la sociedad civil.

Las máscaras ciberespaciales tienden a eclipsar a las personas reales, con resultados buenos y malos. Las bases de datos reflejan el mundo real, pero imperfectamente, lo cual es una condición estructural e inherente de este mecanismo. Así como un modelo científico y matemático del universo material que estableciese una perfecta y completa correspondencia con cada uno de los elementos del universo sería, sencillamente, absurdo, también las bases de datos personales son siempre simplificaciones de la realidad. Los puntos clave son: ¿quién hace las preguntas? ¿Quién establece los criterios y parámetros en la búsqueda de datos? ¿Cuáles son los propósitos e intereses en juego? Las respuestas, desde luego, señalan a aquellos con el poder y la riqueza suficiente para moldear las preguntas, y obtener así las simplificaciones que emergen en tales bases de datos. Las bases de datos privadas, del mismo modo que las públicas a las que el sector privado compra el privilegio de acceder, existen para responder a intereses y preguntas del sector privado. Tales perfiles de datos simplificados, o quizás simplistas, se fundamentan en patrones que responden a necesidades empresariales. Las personas reales son

17. John Schwartz y Robert O'Harrow, Jr., «Databases Start to Fuel Consumer Ire», *Washington Post*, 10 de marzo de 1998.

incorregiblemente desordenadas, exasperadamente complejas, irri-tantemente inconsistentes y llenas de contradicciones: en una pala-bra: difíciles. Esto es lo que significa ser humanos, después de todo, y la razón por la cual nos pillamos los dedos tan a menudo en nues-tras relaciones personales, escribimos poemas y novelas, leemos biografías, y tratamos vanamente, en tanto que científicos sociales, de explicar la conducta individual mediante teorías generales. Pero nuestras oscuras réplicas personales, insertadas en el ciberespacio, no son desordenadas, ni complejas, ni inconsistentes, ni contradicto-rias: son simples, de fácil construcción, elaboradas con rapidez y a bajo precio a partir de bases de datos, y usadas de modo muy renta-ble por el cliente que las paga. Estas caricaturas eclipsan la desorde-nada realidad porque el mundo de las transacciones económicas se estructura de tal modo que sólo permite la entrada a un cierto tipo de información. Si los datos no se adaptan al programa, habrá que re-cortar, reducir, o cualquier otro mecanismo que permita la entrada de la información según los requerimientos del programa. Es como la Fiesta del Té del Sombrero Loco: si el lirón no puede meterse en la tetera, tendrá que ser excluido: se convierte en *riesgo*.

Las nuevas tecnologías de la información han prometido muchas cosas, y han abierto incluso un nuevo universo paralelo: el ciberes-pacio. Tal universo paralelo es apasionante, pero también puede ser un espacio amenazador: oscuras torres de datos que generan el hori-zonte, en posesión de sombrías réplicas distorsionadas de las perso-nas, réplicas que pueden poner en peligro a las personas reales, o ri-diculizarlas en sus vidas cotidianas. Se trata de un mundo alienado, en el que los frutos de nuestra invención pueden volver para atormentarnos.

6. El panóptico participatorio

«Confecciona una lista, la comprueba un par de veces...»

Los Reyes Magos son un cuento de hadas para los niños que pretende, como muchos otros mitos similares, ser ejemplar y enseñar a los niños a ser buenos. También conlleva un elemento crucial de la cultura capitalista contemporánea: el castigo comporta la exclusión de las auténticas ventajas de la sociedad de consumo. En el panóptico de Bentham, la vigilancia absoluta y la consiguiente amenaza de castigar cualquier transgresión de las reglas conllevan la docilidad de todos los sujetos, así como su interiorización y asunción de las reglas, sustituyendo de ese modo al ejercicio real de las sanciones. Pero el panóptico actual añade nuevas dimensiones a esta vieja idea: la pone al día y la mejora. El problema de los panópticos de Bentham, Taylor o Orwell residía en el engaño que se infiltraba con re-

lación a la coacción y al consenso: todos reivindicaban que la coacción era sustituida por un consenso activo, pero todos ellos fundamentaban tal consenso en la coacción, que seguía en el trasfondo porque *era* el trasfondo. El panóptico contemporáneo es sorprendentemente distinto. Se trata de un panóptico consumista basado en ventajas y beneficios efectivos cuya peor sanción es la exclusión. Los prisioneros de Bentham soñaban con escapar; los disidentes, en 1984 de Orwell, desean ardientemente huir hacia algún lugar mejor, pero no pueden, y no existe tal lugar. Nuestro panóptico, por el contrario, es el manantial de los bienes.

El Gran Hermano se despide: el panóptico descentralizado y consensual

El nuevo panóptico difiere del antiguo en dos aspectos fundamentales: está descentralizado y es consensual. La primera característica parece paradójica, ya que en el mismo corazón de la idea de Bentham residía un poder rigurosamente centralizado: la materialización arquitectónica de una autoridad divina y soberana que irradiaba desde el centro de mando y control del inspector. Pero tal concepción ya es tecnológicamente obsoleta a finales del siglo xx. Bentham necesitaba esta estructura arquitectónica porque no disponía de ninguna tecnología de vigilancia que no fuera el ojo humano al desnudo: se requería un elaborado artificio para engañar a los prisioneros y hacerles creer en la omnisciencia del inspector. Las nuevas tecnologías de la información ofrecen una omnisciencia real y no fingida, al mismo tiempo que sustituyen al inspector por una multitud de inspectores que pueden actuar tanto al unísono como competitivamente entre ellos.

Las nuevas tecnologías hacen a los individuos «visibles» de un modo que Bentham no podría haber concebido, pero tal visibilidad está expuesta a una multitud de miradas desde direcciones muy diferentes, y en busca de cosas distintas. Imaginemos un complejo entramado entrecruzado de proyectores rotativos que iluminan constantemente a diversos individuos, momentáneamente encendidos como luciérnagas, para desaparecer luego en la oscuridad y volver a iluminarse, periódicamente. Es una imagen evanescente, sin la tosca simplicidad de la arquitectura de Bentham, pero mucho más próxi-

ma a la compleja realidad actual. Cada vez que hacemos una compra o emprendemos una transacción financiera, cada vez que adquirimos acciones, en algún lugar (y el registro de tales actividades es cada vez más completo) quedamos brevemente iluminados por el ahora ubicuo y descentralizado panóptico. Esta transparencia momentánea, junto a todos los otros momentos en que somos registrados mediante un procesamiento electrónico de datos o por vinculación y coincidencia de datos, configuran un modelo unificado. Ya se sabe que las nuevas tecnologías de la información han acabado con muchos puestos de trabajo; lo que se sabe menos es que el primer desempleado de esta nueva era es el inspector/Gran Hermano. El Centro de Mando y Control o el Ojo Único ya no son necesarios, puesto que puede conseguirse el mismo efecto mediante una multitud dispersa, incluso competitiva, de ojos que, en su totalidad, forman un sistema de vigilancia más dominante y penetrante que el de Orwell. La fuerza de este nuevo panóptico reside en la participación voluntaria de la gente gracias a los beneficios y ventajas que puede apreciar, con lo cual es menos propensa a percibir los inconvenientes y las amenazas. No es necesariamente erróneo pensar de este modo, puesto que los beneficios son directos, reales y tangibles. Los inconvenientes son menos tangibles, más indirectos y complejos. Sin embargo, no deberían ser ignorados.

El panóptico participatorio expande su mirada seductora pero insidiosamente. Las tarjetas del cajero automático son cómodas, permitiendo hacer las gestiones bancarias según la conveniencia de cada cual. El teléfono y la conexión bancaria *on-line* ofrecen todavía una mayor comodidad, permitiendo transacciones financieras desde casa a cualquier hora y cualquier día. Las tarjetas de crédito, de financiación o de débito ofrecen una mayor extensión de tales comodidades, permitiéndonos comprar sin preocuparnos de llevar dinero en efectivo y, cada vez más, tales tarjetas funcionan a distancia, mediante el teléfono o Internet, lo que evita tener que desplazarse. Las tarjetas inteligentes amplían tal comodidad aún más, y añaden otra ventaja: la seguridad, puesto que contienen información personal que impedirá usos desautorizados de la tarjeta.

Las tarjetas de salud inteligentes pueden codificar una gran cantidad de información sobre la salud personal, lo que presenta diversas ventajas. Imagínese, por ejemplo, que está usted implicado en un accidente de tráfico, tendido en el suelo, inconsciente y sangrando.

Al llegar los servicios médicos de urgencias al lugar del accidente, localizan su tarjeta inteligente, la descodifican inmediatamente y leen toda una serie de datos pertinentes: tipo sanguíneo, alergias conocidas a ciertos medicamentos, condiciones que pueden causar complicaciones, médico de familia, etc. ¿Quién podría poner objeciones a tales ventajas?

Generalmente, la vigilancia para la seguridad pública es bienvenida. El predominio de la vigilancia videográfica en espacios privados es cada vez menor respecto a la misma en espacios públicos. Los sucesos criminales son menos probables en espacios bajo una vigilancia permanente, y sucesos como el tráfico de drogas o la prostitución, que hacen decaer un barrio, tienden a desaparecer bajo una activa vigilancia. La vigilancia constante por un gobierno represivo («el Gran Hermano te vigila») despierta profundos resentimientos pero, ¿qué ocurre si el eslogan se transforma en «el Gran Hermano vigila por ti»?

Estos elementos panópticos facilitan la vida diaria, aumentan la seguridad y dan más poder al consumidor. ¿Qué ocurre si cada compra es minuciosamente registrada para elaborar el perfil del comprador y de sus preferencias de consumo para el uso de varios directores de marketing? No todo el mundo objetará a tal eventualidad, si pueden ver como resultado que sus necesidades y deseos son mejor atendidos. Puede considerarse como una lista de deseos para los Reyes Magos, para que nos atiendan mejor. El panóptico consumista recompensa la participación.

Pero siempre hay, desgraciadamente, un precio que pagar. Las tarjetas de salud inteligentes pueden ofrecer ventajas, pero también pueden contener información sobre la póliza de seguros o su ausencia, sobre el crédito disponible o sobre el riesgo de otorgarlo, así como cualquier otra información que pueda llegar a cerrar las puertas de los hospitales privados de urgencias: ¿qué ocurre si también contiene datos sobre el SIDA, los trastornos y enfermedades mentales, un historial de drogadicción o cualquier otra información que pueda llegar a ser devastadora en ciertos contextos para el sujeto portador? Y, saltando hacia adelante en el siglo XXI, ¿qué ocurrirá a medida que se descifre cada vez más el genoma humano y dispongamos de la información genética de cualquier persona?

La vigilancia videográfica aporta más seguridad a los ciudadanos y, en conjunción con otras técnicas sofisticadas de rastreo, ofre-

ce mayores posibilidades de encontrar a gente desaparecida, especialmente niños. En su libro *The Missing* («Los desaparecidos»), el escritor inglés Andrew O'Hagan reflexiona sobre la terrible repercusión en la vida de padres, esposas y amigos ante el miedo y el misterio de una desaparición. Sin embargo, también reconoce que en algunos casos se trata de casos de fuga o evasión:

El problema de los desaparecidos puede ser complejo y endemoniado. Puede en parte resolverse con un sistema nacional de vigilancia, que evitará la propagación de todo tipo de delincuencia; pero también impedirá que se pierdan todos aquellos que pretendan hacerlo: éste, quizás, es el precio que hay que pagar.¹

Siempre hay, parece ser, un precio que pagar.

Existe una parte todavía más oscura y que se mantiene invisible para el usuario cotidiano de estos servicios. Los que usan constantemente los servicios bancarios pueden disponer de amplias autorizaciones de crédito en sus distintas tarjetas bancarias, pero todo ello depende de las restricciones a las que otros se ven sometidos. La capacidad para otorgar crédito a los adinerados depende de la capacidad para identificar y excluir el riesgo. El mismo panóptico que otorga ventajas y beneficios inclusivos, castiga con la exclusión. La misma vigilancia minuciosa que personaliza los privilegios y ventajas, selecciona a los que excluye. Además, y en esto la seducción es realmente insidiosa, los consumidores son disciplinados *por el mismo consumo* para obedecer las reglas, y aprenden a ser «buenos» no porque sea moralmente preferible a ser «malos», sino porque no existe ninguna opción concebible, más allá de la exclusión.

De Maquiavelo a Mickey Mouse

En una brillante metáfora de hace algunos años, los criminalistas Clifford Shearing y Philip Stenning usaron Disney World como la encarnación contemporánea del poder panóptico. Mucha gente visita Disney World, y hay a menudo colas y largas esperas para acce-

1. Andrew O'Hagan. *The Missing*. Nueva York. New Press. 1997; citado por Neal Ascherson. «Lost». *The New York Review of Books*. XLV. 1. 15 de enero de 1998, pág. 31.

der a las diversas atracciones. Siempre hay, además, un ambiente ordenado y pacífico que se mantiene de un modo aparentemente tranquilo y perfecto, sin ningún signo visible de coerción. Todo ello es posible gracias al deseo, compartido tanto por el equipo de gestión como por los clientes, de que haya un máximo consumo en Disney Productions:

Dentro de Disney World, el control es encubierto, preventivo, sutil, cooperativo y aparentemente sin coerciones, consensual [...] La vigilancia es penetrante, pero es la antítesis del descarado control del Estado orwelliano: su principio no es el gobierno, ni su medio es el Gran Hermano. El orden de la disciplina instrumental no es el orden unitario de un Estado centralizado, sino órdenes difusos y separados, definidos y controlados por las autoridades privadas responsables de los dominios de Disney World, semejante a un feudo, con sus bloques de apartamentos, sus centros comerciales, y otras urbanizaciones similares. En la disciplina contemporánea, el control es tan minucioso como pensaba Orwell, pero con unas características muy distintas [...] Actualmente, la gente es seducida para conformarse con los placeres del consumo de bienes que puede ofrecerles el poder corporativo y empresarial.²

Disney World es un recinto con una gestión que tiene un propósito unificado, que se infunde a todas las exposiciones, atracciones y lugares que configuran la variada arquitectura y geografía de todo el complejo lúdico. En este sentido, Disney World tiene una estructura orwelliana, pero el mismo principio puede extenderse a la economía más amplia del capitalismo, incluso cuando las múltiples vigilancias panópticas no se encuentran bajo la misma gestión empresarial y compiten entre ellas. La competición, sin duda muy real en el ámbito de la producción y de las ventas, y lo que recompensa a los accionistas, también sirve para consolidar y desarrollar la cultura del consumo, y por consiguiente el mercado potencial de todos los competidores. Como si se tratase del reconocimiento de un interés compartido, casi toda la información personal acumulada por distintas empresas competidoras proviene de las mismas empresas de in-

2. Clifford D. Shearing y Philip C. Stenning. «From the Panopticon to Disney World: The Development of Discipline», en Anthony N. Doob y Edward L. Greenspan (comps.), *Perspectives in Criminal Law: Essays in Honour of John Ll. J. Edwards*, Toronto, Canada Law Book, 1984, pág. 347.

formación, que la ponen a disposición de todo aquel que quiera y pueda comprarla. El panóptico descentralizado es al mismo tiempo fragmentado y unificado.

Aislamiento vertical y solidaridad horizontal

El antiguo panóptico, centralizado y jerárquico, dependía de su capacidad para aislar a los sujetos entre ellos. La cárcel de Bentham fue diseñada con la intención de eliminar la comunicación entre los prisioneros, por lo que cada uno de ellos quedaba reducido a una relación individual con el inspector. La gestión «científica» intentó controlar el trabajo para romper los gremios y los sindicatos, ya que generaban solidaridad entre los trabajadores. Los regímenes distópicos de Zamiatin y Orwell sustituían sistemáticamente las relaciones horizontales entre los sujetos por órdenes, mediante un sistema vertical de comunicación, jerárquico y monodireccional. En ambas novelas, la resistencia del héroe se derrumba cuando es forzado, mediante el horror, a traicionar su relación más íntima; es justamente la traición de Winston Smith a su amante, Julia, lo que le permitirá finalmente amar al Gran Hermano sin reservas.

El nuevo panóptico evita con remilgo las crudezas y brutalidades de su predecesor. Ya no es necesaria la habitación 101 al final del largo pasillo. Pero a pesar de todo, se mantiene una semejanza estructural: las nuevas tecnologías de la información individualizan progresivamente al nuevo sujeto consumidor. Además, la investigación en marketing se orienta cada vez más hacia una diferenciación progresivamente más minuciosa de los gustos y preferencias de distintos grupos sociales y, ocasionalmente, hacia la identificación de las preferencias personales de un consumidor (que pague). La solidaridad social se debilita a medida que la conciencia de tales diferencias es constantemente evaluada, puesta en juego y vendida por el mercado panóptico. Los sujetos están aislados y la sociedad civil fragmentada, pero esto ya no remite a los antiguos métodos de la porra y del aro de metal: actualmente, cuando la vigilancia panóptica se dirige e interpela a sujetos individuales, lo hace mediante la comprensión de sus necesidades y la satisfacción de sus deseos. El sistema es tan flexible que una multitud de productores compiten entre ellos para captar la atención y el dinero del consumidor soberano. La

vigilancia participatoria es, desde luego, un mecanismo mucho más poderoso que el que existía antes.

Diversas transformaciones de los medios de comunicación han facilitado todo este proceso. El desplazamiento desde transmisiones en abierto de programas televisivos a las emisiones codificadas ofrece incluso unos medios especializados de entretenimiento que permiten diferenciar perfiles de marketing. En 1950, los telespectadores podían seleccionar entre CBS, NBC y ABC. En otros países la elección era incluso más limitada, y así se mantuvo durante mucho más tiempo. Los programas tenían una audiencia de masas, y los publicistas se dirigían a un mercado tan amplio para sus productos como el de dichas audiencias. La llegada de la televisión por cable y de las emisiones por satélite ha transformado este panorama. Mientras la televisión se desplaza hacia un universo de quinientos canales, los canales especializados salen a flote. Un canal que sólo transmita golf tendrá una audiencia relativamente limitada, pero estará muy controlada por ciertos publicistas que reconocerán en el perfil informativo de los entusiastas del golf el perfil adecuado para los productos que promocionan. Cuanto más sepan los publicistas sobre tales telespectadores, mejor podrán servir este pequeño mercado *niche*, y cuanto más les sirvan, más les conocerán.

La misma tendencia puede apreciarse en los medios de comunicación impresos. Los periódicos con tiradas masivas han ido decreciendo en los últimos años, absorbidos y consolidados bajo la propiedad de grandes empresas o multinacionales, y existen crisis periódicas sobre el margen de sus beneficios. Al mismo tiempo, la década de los noventa ha sido una época dorada para las revistas, no tanto para el viejo mercado de masas, con revistas que contienen de todo para todo tipo de gente, como *Life* o *Saturday Evening Post*, muchas de las cuales han desaparecido, sino para revistas más especializadas o definidas. En cualquier revistero actual pueden hallarse lámparas de Aladino repletas de tesoros para posibles compradores: cada revista ofrece un tesoro particular para un segmento específico de la población. Las revistas atraen a los aficionados a la música *hip-hop*, a la pesca, a las armas, a los coches, al baile, al sadomasoquismo, a los caniches, al mercado de antigüedades, etc. Puede nombrarse cualquier cosa: casi seguro que existirá una o dos revistas especializadas para proveer sus deseos y fantasías. Los anuncios atraen aún más la atención de los lectores que los artículos, ya que

tales lectores saben que los productos que se anuncian en su revista favorita son justamente los que despiertan su interés.

También la radio ha seguido este modelo. El fenómeno de los 40 Principales ha sido sustituido por cadenas que ofrecen una mayor especialización de los gustos musicales: rock, *rap*, música ambiental, viejas melodías, *country* y *western*, música étnica y otras categorías, cada una de ellas con un apropiado surtido de anuncios. Mediante Internet tal especialización llega a su máximo, puesto que el número de páginas *web* o de direcciones especializadas sólo está limitada por el ingenio y la energía de los usuarios de la Red. Por el momento no parece que los publicistas hayan aún capitalizado realmente las oportunidades que ofrece la Red para un marketing dirigido a audiencias especializadas, pero sin duda se trata de una demora que tarde o temprano será subsanada.

Mientras prosigue la fragmentación de las audiencias masivas, también decrecen los programas orientados a este tipo de público. Ciertos acontecimientos exageradamente promocionados, como la Super Bowl anual, pueden aún atraer a una audiencia relativamente grande, así como las primeras emisiones de ciertos anuncios dirigidos a esta audiencia (y que siguen emitiéndose mientras dura la retransmisión del partido). Pero incluso la Super Bowl y otros acontecimientos mediáticos de carácter deportivo o lúdico atraen cada vez menos concentraciones de espectadores en relación con el pasado. Algunos espectáculos, generalmente comedias de situación, pueden conseguir una gran audiencia durante un cierto tiempo, recogiendo un espectro demográfico o un determinado sentimiento público, tal y como ocurrió con *Seinfeld*, que tuvo una destacada trayectoria antes de que su creador cerrara el grifo, quizás anticipándose a su inevitable declive. Pero podemos esperar una cada vez mayor fragmentación de la audiencia según determinadas clases de programas, a su vez seguidos por determinados tipos de publicidad. La misma economía del panóptico dicta esta necesidad pero, ¿qué ocurre con el impacto cultural que esta fragmentación provoca en las democracias de masas? Se trata de una pregunta de una gran complejidad de la que sólo podemos dar, y nunca mejor dicho, fragmentos de una respuesta.

El panóptico multicultural

Consideremos el modo en que los negocios de Norteamérica han identificado, perfilado y se han dirigido hacia diversos grupos sociales. Las feministas han criticado con justicia la imagen de la mujer en la publicidad en tanto que objeto sexual o accesorio masculino. En una época en que los hombres controlaban casi todo el poder discrecional de compra del país, la avenida Madison decidió que «el sexo vende», lo que significaba que «las mujeres *sexys* venden». Tradicionalmente, en las áreas en las que las mujeres hacían compras —artículos del hogar, ropa, etc.— se lanzaban ciertos reclamos a la mujer que eran, de hecho, la imagen refleja de los anuncios centrados en la masculinidad, es decir, mujeres ocupadas con su labores y su maternidad que intentan ser atractivas para sus esposos. En la época del marketing de masas, una sola talla tiene que ser la adecuada para todos. A medida que las mujeres se adentraron más y mejor en el mundo laboral, la publicidad empezó a cambiar. Al coincidir tales cambios con la rápida proliferación de las nuevas tecnologías de la información y con las nuevas estrategias de marketing, ya no hubo una simple equiparación ni una mera inversión de roles. En su lugar, el marketing empezó a concentrarse en categorías particulares de la «nueva» imagen de la mujer con poder adquisitivo tan pronto como podían ser identificadas. Empezaron a aparecer mujeres jóvenes y atractivas con carrera en diversas situaciones laborales y profesionales, siempre elegantemente vestidas, decididas, ofreciendo consejos inteligentes a sus viejos jefes masculinos o tomando decisiones por su cuenta. Una variación de esta tendencia es la nueva imagen de la mujer en el mundo laboral que busca agresivamente hombres atractivos. El mensaje: puedes tenerlo todo, éxito y también sexo. Pero tales imágenes no sustituyen a las más antiguas, muchas de las cuales también han adoptado diversas variaciones, como los anuncios de comida congelada orientados a mujeres trabajadoras, preocupadas por servir la comida en sus casas pero sin disponer del tiempo necesario para cocinar ellas mismas, tal y como lo hacían las madres que sólo se ocupaban de sus hogares. Tales anuncios reafirman a las mujeres que intentan combinar ambos roles: puedes hacer ambas cosas, dice el mensaje, trabajar durante el día y ocuparte del marido y los niños en casa. Sin embargo, también siguen vigentes imágenes más tradicionales, como la mujer en tanto que objeto sexual del marido (bebe

tal cerveza y tiene una mujer; conduce tal coche y también conduce a una mujer) o la mujer en tanto que devota esposa que se ocupa del hogar; imágenes que encienden la ira de feministas rigurosas que consideran que nada ha cambiado realmente, después de todo, mientras siguen promoviéndose modelos de mujer con tales roles.

Las críticas con tales motivos políticos, por más loables que sean en su contexto, tienden a errar el tiro. Desde una perspectiva empresarial la clave reside, volviendo a enderezar la célebre frase de Marx, en entender el mundo, y no en cambiarlo. El mundo ofrece actualmente una imagen mucho más variada y diversificada de la mujer para la mirada panóptica: estas mujeres, ¿se dedican ante todo a conseguir el éxito empresarial? Identifiquémoslas, descubramos cómo atraer su atención, cómo se ven a sí mismas, cuánto pueden gastar y qué quieren comprar. Diseñemos entonces los productos y los anuncios que llamarán su atención. Del mismo modo, ¿existen mujeres trabajadoras ambivalentes respecto a su papel, que se sienten inseguras en relación con la imagen que tienen de ella su marido y sus hijos? Diseñemos entonces los productos adecuados para conectar con tal inseguridad, y alimentémosla, para asegurarnos de que seguirán comprando nuestros productos. Al mismo tiempo, a pesar del cambio de papeles sexual, aún se puede convencer a muchos hombres para que compren ciertos productos si se asocian a la sensual figura de una mujer, por lo que el paisaje publicitario hace convivir bebés y mujeres objeto con decididas mujeres profesionales y con honestas pero preocupadas madres trabajadoras. El capitalismo no se ocupa de encabezar cambios sociales, pero tal ausencia también contribuye a que su mirada panóptica sea muy pronta en detectar indicios de los cambios sociales que realmente ocurren; su propósito consiste en recogerlos y darles forma en tanto que demandas sociales del consumidor, que pueden ser acogidas por el sistema. Al diferenciar la imagen de la «mujer», la clasificación panóptica también ayuda a dispersar y fragmentar la potencial circunscripción política de la «mujer» en una multitud de circunscripciones con distintos tipos de mujer, con afinidades y objetivos diferentes. El capitalismo, desde luego, no crea tales circunscripciones pero, al animarlas y recompensar su diferenciación e individualización, acelera tales tendencias de fragmentación presentes en la sociedad.

Recientemente, el capitalismo norteamericano ha empezado a darse cuenta del potencial de un «mercado gay». Esto sólo podía

ocurrir después de que los homosexuales y las lesbianas empezaran a salir de sus guetos sociales y culturales para mostrarse claramente al mundo. Las reacciones homofóbicas continúan produciéndose en todas las sociedades, sin duda, y tanto el sida como las manifestaciones de la mayoría moral y evangélica de Estados Unidos están a la orden del día. En tal contexto de cambios sociales, cargado aún de ansiedades sociosexuales, de amenazas de proseguir con las sanciones públicas y de diversos actos de violencia antigay, la identificación y conquista del mercado gay es un proceso repleto de tensiones. La mirada panóptica, que tan a menudo aparece benévola y beneficiosa para con sus sujetos, se muestra en este caso peligrosamente ambigua, incluso intimidante. En el pasado más reciente, un pasado que infunde al presente un aire amenazador, había muchas más tendencias de la vigilancia panóptica buscando cualquier «desviación» sexual en tanto que riesgo o inseguridad laboral, o con el objetivo de chantajearla (a menudo no podían distinguirse claramente ambas amenazas).

Un caso de 1998 que cautivó la atención pública en Estados Unidos ilustra perfectamente la continuidad del problema. Bajo la política del «no preguntes, no contestes» que se derivó de los fracasados intentos del presidente Clinton para erradicar la discriminación antigay en el ejército norteamericano, un veterano oficial de la marina, con diecisiete años de honorable servicio, fue despedido. El oficial usó el término «gay» para describir su estado civil en un formulario de American Online (AOL, el mayor proveedor de servicios de Internet) mientras mantenía correspondencia electrónica con un empleado civil en relación con una actuación de caridad para donar juguetes.³ Aunque en tal formulario no constaba ningún vínculo que permitiese su identificación personal, la Marina la obtuvo de forma ilícita por medio de AOL, que posteriormente se disculpó por haber revelado el dato.⁴ El daño, sin embargo, ya se había consumado.

En un contexto tan potencialmente amenazador, apenas sorprende que la exploración de la mirada panóptica para identificar un mercado gay pueda toparse algunas veces con más suspicacia que bienvenidas. Por otro lado, las empresas tienen que elaborar cuida-

3. Lisa Napoli, «Sailor Says Navy Is Using AOL Profile to Oust Him», *New York Times*, 9 de enero de 1998.

4. Lisa Napoli, «AOL Admits Error in Sailor's Case», *New York Times*, 21 de enero de 1998.

dosamente sus reclamos publicitarios para evitar reacciones antigay en otros sectores del mercado. A pesar de estos percances, la emergencia del mercado gay es sin duda un paso importante en la reestructuración de las relaciones entre los gays y las lesbianas y el resto de la sociedad, quizás incluso hacia una posible eliminación de la discriminación por motivos de orientación sexual. El panóptico consumista puede legitimar a grupos previamente marginados e integrarlos no en tanto que consumidores del montón que esconden o pierden su identidad, sino justamente en términos específicos relativos a aquello que los diferencia de otros grupos y de la corriente mayoritaria. Al dirigirse a ellos *en tanto que gays* y no como consumidores que pueden ser gays en su tiempo libre, la mirada panóptica reconoce y legitima sus diferencias.

Hay una serie de aspectos a resaltar en este proceso de reconocimiento. No debemos olvidar que tal reconocimiento sólo se otorga a cambio de su poder adquisitivo, por lo que los grupos marginados que carecen del mismo permanecen marginados. En el caso del mercado gay, se ha afirmado que las lesbianas no tienen generalmente el mismo poder adquisitivo del que gozan los varones homosexuales, por lo que tal mercado ha sido relativamente ignorado. Podríamos ampliar esta observación dentro del mismo mercado gay, ya que la mirada panóptica iluminará con más frecuencia y más favorablemente a los hombres homosexuales con mayor nivel de ingresos. Se tendrá especialmente en consideración a los profesionales, a los hombres de negocios o la gente dedicada al espectáculo, tanto por su visibilidad como por su riqueza, lo que sin duda acentúa y refuerza la diferencia de clases. El reconocimiento panóptico también exige otras condiciones específicas: una política gay radical, subversiva y directa será difícilmente recompensada, mientras que otra más cordial, conformista y sin diferencias amenazadoras en su «estilo de vida» será, por el contrario, bienvenida. La vigilancia participatoria puede ser consensual y no recurrir directamente a la coerción pero, en última instancia, remite a la disciplina y a la integración, y no a la rebelión ni a la resistencia, por lo que tanto la diferenciación como la fragmentación sirven justamente para tal fin.

El multiculturalismo es actualmente una tendencia en el candelero, impugnada, y claramente política. Hablar de un panóptico multicultural podría parecer algo perverso, ya que se trata de una tendencia generalmente considerada de izquierdas y a la que se oponen

acaloradamente los conservadores. Es intrínsecamente improbable que el capitalismo corporativo lidere los desafíos a su hegemonía, pero las batallas culturales esconden mucho más de lo que iluminan. La sensibilidad de la mirada panóptica a las diferencias, incluso a las más pequeñas y encubiertas, es un atributo esencial de un conservadurismo creativo, adaptable y flexible.

Con la globalización de la economía, la identidad dual del panóptico en tanto que competitivo y unificado al mismo tiempo genera un enorme poder: la competición es el mecanismo mediante el cual se adentra en los nuevos mercados, al mismo tiempo que conlleva una aceptación universal de la cultura del consumo. El panóptico consumista puede expandir su mirada de un modo global precisamente porque puede adaptarse con facilidad a las variaciones locales. Hace algunos años, IBM emitió una serie de anuncios televisivos que representaban «soluciones para un pequeño planeta», con graciosos spots que reunían a gente en lugares tradicionales y exóticos discutiendo sobre la última tecnología de IBM: las monjas de un convento europeo, por ejemplo, se susurran durante los rezos que están impacientes por «navegar por la Red». Microsoft, que emplea un número considerable de programadores informáticos y de analistas de sistemas de nacionalidad india, organizó un concurso interescolar en la India para que los niños propusieran soluciones técnicas a problemas informáticos concretos. Los ganadores eran presentados en un acontecimiento televisivo por el mismo Bill Gates, con sus premios, y junto a sus orgullosos padres y familiares, algunos vestidos con la tradicional ropa india. La campaña intencionadamente multirracial y multicultural de Benetton (los «United Colors of Benetton») llevó tan lejos esta estrategia que provocó incluso diversos estallidos de indignación xenófoba por sus sugerencias de sexo interracial o, en un caso muy comentado, por su representación de una reina de Inglaterra negra. Benetton también ha sido acusada de emplear mano de obra barata en fábricas del Tercer Mundo que explotan a los obreros, demostrando así claramente que el marketing multicultural puede basarse en una explotación multirracial: en ambos casos, el beneficio económico es el criterio fundamental. En las décadas de los cincuenta y los sesenta, diversos críticos señalaron la «Cola-colonización» norteamericana del mundo. En los inicios del marketing de masas, un producto como la Coca-Cola, tan típico como el modelo T de Ford, parecía el emblema de un imperialismo en el que una cultura de masas ho-

mogeneizada corría tras la bandera de las multinacionales. En la práctica, la Coca-Cola ha sabido desarrollar con habilidad diversas adaptaciones de sus productos a las necesidades de distintas culturas.⁵ Tal y como escribe Ronald Diebert a propósito de las nuevas tecnologías de la información, los llamados «hipermedios de comunicación»:

Los hipermedios de comunicación, mediante sistemas de publicidad y mecanismos de producción organizados informáticamente y diseñados digitalmente, permiten fabricar productos *niche* adaptados a las condiciones locales. Mediante perfiles informáticos y otros mecanismos de control del marketing, las firmas pueden mantener una vigilancia permanente a escala mundial, en lugares y poblaciones muy diferentes, consiguiendo diversas respuestas adaptadas a las condiciones locales. Gracias a ello, han sabido efectuar rápidos ajustes de sus campañas publicitarias, con el propósito de influenciar los gustos más idiosincrásicos del consumidor. Incluso McDonald's —un símbolo de la homogeneización capitalista, si tal cosa existe— cambia regularmente muchos de sus productos y campañas publicitarias para que se ajusten al perfil de los consumidores locales. En Japón, por ejemplo, cambió el nombre de su mascota Ronald McDonald por el de Donald McDonald, así como la pronunciación de su nombre por el de «Makudonaldo», facilitando ambos cambios la pronunciación por parte de los hablantes japoneses.⁶

Las multinacionales no tienen ningún problema con el multiculturalismo, ya sea en tanto que parte de su fuerza de trabajo, o en sus estrategias de marketing internacional. El entramado de proyectores panópticos ilumina las particularidades culturales, lingüísticas, étnicas y de cualquier otro tipo, en tanto que objetivo de sus ofertas en el mercado; y una producción flexible puede adaptarse rápidamente mediante una adecuada diferenciación de sus productos y de sus servicios, lo que sin duda exige capital disponible. Algunos rincones

5. Una película australiana de hace algunos años, *The Coca-Cola Kid*, describía a un ejecutivo de ventas norteamericano de esta empresa que se lanzaba en paracaídas a Australia con el objetivo de eliminar a una marca de refrescos local muy competitiva. Inmediatamente, decide explotar la música aborigen en locales que asocian e identifican dicha música, así como otros aspectos de la cultura indígena, con los productos Coca-Cola.

6. Ronald J. Diebert, *Parchment, Printing and Hipermedia: Communications in World Order Transformation*. Nueva York, Columbia University Press, 1997, págs. 144-145.

acaloradamente los conservadores. Es intrínsecamente improbable que el capitalismo corporativo lidere los desafíos a su hegemonía, pero las batallas culturales esconden mucho más de lo que iluminan. La sensibilidad de la mirada panóptica a las diferencias, incluso a las más pequeñas y encubiertas, es un atributo esencial de un conservadurismo creativo, adaptable y flexible.

Con la globalización de la economía, la identidad dual del panóptico en tanto que competitivo y unificado al mismo tiempo genera un enorme poder: la competición es el mecanismo mediante el cual se adentra en los nuevos mercados, al mismo tiempo que conlleva una aceptación universal de la cultura del consumo. El panóptico consumista puede expandir su mirada de un modo global precisamente porque puede adaptarse con facilidad a las variaciones locales. Hace algunos años, IBM emitió una serie de anuncios televisivos que representaban «soluciones para un pequeño planeta», con graciosos spots que reunían a gente en lugares tradicionales y exóticos discutiendo sobre la última tecnología de IBM: las monjas de un convento europeo, por ejemplo, se susurran durante los rezos que están impacientes por «navegar por la Red». Microsoft, que emplea un número considerable de programadores informáticos y de analistas de sistemas de nacionalidad india, organizó un concurso interescolar en la India para que los niños propusieran soluciones técnicas a problemas informáticos concretos. Los ganadores eran presentados en un acontecimiento televisivo por el mismo Bill Gates, con sus premios, y junto a sus orgullosos padres y familiares, algunos vestidos con la tradicional ropa india. La campaña intencionadamente multirracial y multicultural de Benetton (los «United Colors of Benetton») llevó tan lejos esta estrategia que provocó incluso diversos estallidos de indignación xenófoba por sus sugerencias de sexo interracial o, en un caso muy comentado, por su representación de una reina de Inglaterra negra. Benetton también ha sido acusada de emplear mano de obra barata en fábricas del Tercer Mundo que explotan a los obreros, demostrando así claramente que el marketing multicultural puede basarse en una explotación multirracial: en ambos casos, el beneficio económico es el criterio fundamental. En las décadas de los cincuenta y los sesenta, diversos críticos señalaron la «Cola-colonización» norteamericana del mundo. En los inicios del marketing de masas, un producto como la Coca-Cola, tan típico como el modelo T de Ford, parecía el emblema de un imperialismo en el que una cultura de masas ho-

mogenezada corría tras la bandera de las multinacionales. En la práctica, la Coca-Cola ha sabido desarrollar con habilidad diversas adaptaciones de sus productos a las necesidades de distintas culturas.⁵ Tal y como escribe Ronald Diebert a propósito de las nuevas tecnologías de la información, los llamados «hipermedios de comunicación»:

Los hipermedios de comunicación, mediante sistemas de publicidad y mecanismos de producción organizados informáticamente y diseñados digitalmente, permiten fabricar productos *niche* adaptados a las condiciones locales. Mediante perfiles informáticos y otros mecanismos de control del marketing, las firmas pueden mantener una vigilancia permanente a escala mundial, en lugares y poblaciones muy diferentes, consiguiendo diversas respuestas adaptadas a las condiciones locales. Gracias a ello, han sabido efectuar rápidos ajustes de sus campañas publicitarias, con el propósito de influenciar los gustos más idiosincrásicos del consumidor. Incluso McDonald's —un símbolo de la homogeneización capitalista, si tal cosa existe— cambia regularmente muchos de sus productos y campañas publicitarias para que se ajusten al perfil de los consumidores locales. En Japón, por ejemplo, cambió el nombre de su mascota Ronald McDonald por el de Donald McDonald, así como la pronunciación de su nombre por el de «Makudonaldo», facilitando ambos cambios la pronunciación por parte de los hablantes japoneses.⁶

Las multinacionales no tienen ningún problema con el multiculturalismo, ya sea en tanto que parte de su fuerza de trabajo, o en sus estrategias de marketing internacional. El entramado de proyectores panópticos ilumina las particularidades culturales, lingüísticas, étnicas y de cualquier otro tipo, en tanto que objetivo de sus ofertas en el mercado; y una producción flexible puede adaptarse rápidamente mediante una adecuada diferenciación de sus productos y de sus servicios, lo que sin duda exige capital disponible. Algunos rincones

5. Una película australiana de hace algunos años, *The Coca-Cola Kid*, describía a un ejecutivo de ventas norteamericano de esta empresa que se lanzaba en paracaídas a Australia con el objetivo de eliminar a una marca de refrescos local muy competitiva. Inmediatamente, decide explotar la música aborigen en locales que asocian e identifican dicha música, así como otros aspectos de la cultura indígena, con los productos Coca-Cola.

6. Ronald J. Diebert, *Parchment, Printing and Hypermedia: Communications in World Order Transformation*, Nueva York, Columbia University Press, 1997, págs. 144-145.

del mundo se mantienen relativamente oscuros: la mayor parte de África, diversas partes de Asia y gran parte de América Latina. En otros lugares, como las antiguas economías del bloque soviético, hay una media luz intermitente: no está claro si se iluminarán del todo o recaerán en la oscuridad. Pero allí donde se desarrolla el mercado, la mirada panóptica lo explora sin cesar.

En un influyente artículo de hace algunos años, el filósofo político canadiense Charles Taylor escribió acerca del multiculturalismo en tanto que política sobre el reconocimiento de la diferencia.⁷ Contrariamente al antiguo liberalismo universal que luchaba por erradicar las diferencias raciales, sexuales, etc., el multiculturalismo político busca el reconocimiento y la validación de las diferencias culturales en tanto que fundamento de una comunidad compartida. La mirada panóptica del capitalismo busca y se adapta a las diferencias pero, ¿qué tipo de «multiculturalismo» conlleva tal adaptación? Sin duda, las críticas que describen un mercantilismo puramente «blanco, masculino y eurocéntrico», que pretende imponerse a las jerarquías raciales y genéricas existentes, así como implantar una estructura cultural homogénea en todo el mundo, pasan por alto la capacidad de las prácticas panópticas para adaptarse e integrar entornos múltiples y diversos. Al mismo tiempo, existe una profunda diferencia entre el multiculturalismo del capitalismo de la información, por un lado, y el desarrollado en tanto que filosofía del cambio social y político. El capitalismo reconoce y constituye a las personas en tanto que *consumidores*, pero no en tanto que *ciudadanos*. El consumo multicultural no es lo mismo que la ciudadanía multicultural: entre uno y otra hay un mundo de diferencias.

Las formas tempranas del panóptico siempre han provocado resistencias pero, actualmente, es más sutil, más flexible, más abierto a participaciones heterogéneas y más consensual. El consenso de ingeniería genética que Huxley describe en *Un mundo feliz* puede parecer más cercano a la brutalidad del sombrío Estado policial de Orwell, pero tal proximidad es superficial. Los encantos del consumo son seductores, pero existen demasiadas personas —millones en el Tercer Mundo, pero también demasiadas en el mundo «desarrollado»— totalmente excluidas de tales beneficios, y por lo tanto de la

7. Charles Taylor, «The Politics of Recognition», en Amy Gutmann (comp.), *Multiculturalism and the Politics of Recognition*, Princeton University Press, 1997, págs. 25-74.

mirada panóptica. La mayoría no tiene el pasaporte que permite la entrada en tal recinto: el dinero. Otros han sido excluidos de tales encantos a causa del «riesgo» que representan y, a medida que se incrementa internacionalmente la aceptación de la agenda neoliberal, se les excluye incluso del cinturón de seguridad del sistema de bienestar. Algunos sienten instintivamente las limitaciones políticas y el empobrecimiento cultural de la realidad que subyacen al título de «consumidor soberano». La resistencia toma algunas veces la forma de *luchas por la ciudadanía*, que no pueden contenerse ni gestionarse como un simple reconocimiento de los consumidores. Irónicamente, las mismas tecnologías que sostienen e intensifican la mirada panóptica del capitalismo también aumentan la capacidad de lucha por la ciudadanía. Volveremos a las promesas democráticas de las nuevas tecnologías en el último capítulo.

La época de la vigilancia multidireccional

Aunque la vigilancia con alta tecnología aumenta la capacidad de vigilancia jerárquica de arriba abajo, también intensifica el movimiento contrario de abajo arriba. La televisión empezó como un medio de arriba abajo, unidireccional, en el que la única participación efectiva de la audiencia remitía a una minuciosa y rígida selección para sus estudios televisivos (a menudo reemplazada por risas automáticas registradas previamente) o a los sistemas despersonalizados y masivos de índices de audiencia. La televisión también se ha adaptado a los mecanismos de vigilancia y seguridad, con circuitos cerrados que exploran cualquier lugar mediante cámaras, desde los vestíbulos de los apartamentos y los garajes hasta los pasillos de las oficinas. Esta misma tecnología de cámaras, fácilmente manejables, también se ha convertido en un instrumento económico y móvil para ciertas guerrillas urbanas de contravigilancia. La mayoría de tales usos remiten a formas triviales, apolíticas y rápidamente absorbidas y utilizadas por los medios de comunicación en tanto que productos de entretenimiento, como *America's Funniest Home Videos*.^{*8} Pero

* *Los vídeos domésticos más divertidos de América*, programa de televisión similar a *Videos de primera*. (N. del t.)

8. En la década de los sesenta, la misma idea fue utilizada en un contexto más

también existen ejemplos de algunos usos políticamente explosivos del vídeo: la paliza que recibió Rodney King por parte de la policía de Los Ángeles, capturada en vídeo por un testigo solitario, se convirtió en el motor de un conflicto racial mucho mayor, y de numerosas manifestaciones en todas las ciudades norteamericanas. En Canadá, los vídeos que grabaron ciertos participantes en las sesiones de entrenamiento de un regimiento de aerotransportación de elite de las fuerzas militares de Canadá, transmitidos por televisión, conmocionaron de tal modo a la opinión pública por la exhibición de racismo, brutalidad y denigración que contenían, que el regimiento fue disuelto por el ministro de Defensa. En otro caso canadiense, las prisioneras de un centro correccional femenino, internadas por causas diversas de disturbios sociales, eran forzadas a desnudarse y a coquetear con los guardas; todo el proceso fue captado por un vídeo que consiguió llegar a los medios de comunicación, desatando una investigación oficial y provocando finalmente la dimisión del responsable del correccional. En todos estos casos, el comportamiento de ciertos funcionarios que antes se mantenía oculto y fuera de toda consideración, llega de pronto a la opinión pública, con importantes consecuencias. No siempre se trata de guerrillas de contravigilancia desde abajo: la tendencia de Richard Nixon a registrar encubiertamente las conversaciones del Despacho Oval se volvió contra él en el fiasco de las cintas de la Casa Blanca, que le condujeron finalmente a la dimisión ante su inminente destitución. La misma tecnología, más que las intenciones o planes humanos, puede ser la responsable, como en el caso del correo electrónico que implicó a varios funcionarios administrativos de Reagan en el Irangate: los conspiradores fracasaron al no informarse adecuadamente sobre los mecanismos de registro automático que caracterizan el sistema de correo electrónico de la Casa Blanca, por lo que la frenética acti-

controlado y jerárquico: en *Candid Camera* se planeaban y ejecutaban bromas visuales en las que se engañaba a personas inocentes para hacer reír a una audiencia televisiva cómplice de la farsa. Por otro lado, el contenido de *America's Funniest* depende de la contribución de videoaficionados, que muy a menudo envían material casual y divertido de sus películas domésticas, filmadas para uso privado y no público. En muchos casos, puede tratarse de material planificado y ensayado, pero aun así se trata de un artificio popular y democrático, en contraste con los mecanismos manipuladores y bastante autoritarios de la generación anterior. La diferencia se basa simplemente en la amplia difusión de las cámaras de vídeo domésticas.

vidad de eliminación de archivos que siguió a tales intercambios no consiguió borrar todas las copias generadas. Finalmente, gracias a un pleito emprendido por un grupo civil, cientos de casetes informáticos e incluso 135 discos duros del Consejo de Seguridad Nacional fueron conservados como testimonios públicos.⁹

Uno de los efectos inmediatos de esta era de vigilancia multidireccional consiste en colocar a las figuras públicas bajo una constante mirada publicitaria y sin remordimientos, orientada tanto a sus vidas privadas como a sus roles públicos, alimentada por las ansias mediáticas por destapar asuntos de sexo y mezquindades entre los poderosos. Por ejemplo, el absurdo espectáculo que ha mantenido cautiva a la presidencia de Estados Unidos durante tanto tiempo, intentando saber si el presidente había mantenido o no relaciones sexuales en la Casa Blanca con una becaria adulta y muy dispuesta. El asunto salió a la luz gracias a las cintas registradas clandestinamente a dicha becaria, que se lo exponía todo a una supuesta «amiga», y hechas públicas posteriormente. El caso de Monica Lewinsky (que quizás podríamos considerar «virtual») representa una especie de *reducción al absurdo* de los mecanismos de legitimación democrática. La precipitada mediatización de este supuesto escándalo hasta la cima de los medios de comunicación (eclipsando incluso, por ejemplo, la histórica visita del papa a Fidel Castro) fue en parte conducida por una impresionante proliferación de rumores funcionando como noticias en Internet. Se trata de un medio de comunicación que puede parecer democrático y animar a la participación ciudadana, en contraste con la pesada carga institucional, rígidamente estructurada, de los medios de comunicación tradicionales. La misma Red que ha desarticulado las estructuras empresariales tradicionales está invadiendo también la comunicación dentro y entre empresas, provocando lo que ha sido denominado «desintermediación». Tal y como explica Jack Shafer:

En el mundo del comercio electrónico, se oye hablar cada vez más de «desintermediación»: la eliminación de intermediarios y distribuidores gracias a la Red, que conecta directamente a los productores con los consumidores. Sería prematuro proclamar la «desintermediación»

9. Tom Blanton (comp.), *White House E-Mail: The Top Secret Computer Messages the Reagan/Bush White House Tried to Destroy*, Nueva York, The New Press, 1995.

de los nuevos medios de comunicación, con cibernautas independientes que actúan como editores, denuncian a abogados y critican las convenciones periodísticas. Pero [...] cualquiera que esté conectado a Internet y tenga algo original que transmitir puede llegar a una audiencia internacional. Al percibir esta «desintermediación», los antiguos medios de comunicación se han introducido en la Red [...] Los expertos en comercio electrónico ya están hablando de «reintermediación», lo que supondría la emergencia de una nueva hornada de intermediarios en la Red para organizar el caos que ha provocado la «desintermediación». A medida que la tecnología de la Red evolucione, los dispositivos de Internet serán tan ubicuos como el teléfono. Incluso los periódicos tendrán la capacidad de transmitir las noticias con la misma velocidad que una cadena televisiva, y éstas tendrán la capacidad de convertirse en periódicos.¹⁰

El mayor inconveniente de tal dinámica es que, actualmente, existen muy pocas normas y convenciones tanto profesionales como éticas en el periodismo de Internet, ya que es justamente su aspecto *amateur* y su fácil acceso lo que dan a Internet su peculiar atracción popular. Pero el anverso de una actividad de aficionados es la irresponsabilidad. Así como el dinero negro puede blanquearse y generar dinero legal, los rumores sobre el asunto Lewinsky que circulaban por la Red acabaron imprimiéndose en periódicos e invadiendo los telediaros, capitaneados por las noticias por cable, con su consabida avidez de noticias instantáneas, y a menudo con rumores añadidos de cosecha propia, muchos de los cuales tenían que ser desmentidos a los pocos días, incluso horas más tarde.

Hay algo de inherentemente desagradable en la intensa vigilancia a que son sometidas diversas personalidades del sector público, en comparación con el escrutinio mucho menos minucioso que se desarrolla sobre la riqueza y el poder en el sector privado. A causa de la legitimidad que los políticos deben a sus votantes, a menudo se considera su vida privada como propiedad pública. Grandes figuras del mundo empresarial, que sólo rinden cuentas a sus accionistas, pueden permitirse una vida privada que sería recriminada por los medios de comunicación en una figura política. En una época en que

10. Jack Shafer, «The Web Made Me Do It», *The New York Times*, 15 de febrero de 1998.

los Estados parecen retraerse ante el desarrollo de un sector privado internacional, la trivialización del espacio público como una comedia del arte o basura televisiva podría acelerar la denigración del sector público a favor del privado, así como la sustitución de los políticos por mercados y de los Estados por multinacionales. De hecho, cada vez es más difícil distinguir entre el mundo «real» de la política y el mundo «fantasioso» de la televisión, confusión que se acentúa por el afán de los políticos por aparecer en cualquier «paisaje» televisivo. Ronald Reagan pasó ocho años en la Casa Blanca interpretando su último papel al estilo de Hollywood, pero esta vez como presidente de Estados Unidos y, según las encuestas, realizó un trabajo convincente. Dan Quayle, el anterior vicepresidente, criticó al personaje de Murphy Brown, de la famosa comedia de situación, por tener un hijo sin estar casado (como si tal personaje fuera un oponente político del partido demócrata) y, para completar el círculo, el propio Dan Quayle interpretó luego un personaje en la serie de Murphy Brown. Así que Bill y Hillary, en vez de ser el presidente y la primera dama, se convierten en personajes de una comedia de enredos, y Monica, la «otra mujer» que proviene de Beverly Hills, tiene una dirección que se asocia a otra comedia con jóvenes actores y frenéticas infidelidades. El asunto Lewinsky saltó a la opinión pública poco después de que una comedia de Hollywood alcanzase el éxito en todo el país: *Cortina de humo*. En ella, un presidente con problemas de faldas en la Casa Blanca acude a un médico y a un productor de cine que le proponen desplegar una falsa guerra con el objetivo de desviar la atención, y el remedio funciona. Como si estuviese siguiendo el mismo guión, el presidente Clinton empezó a incrementar el conflicto con el eterno rival de Estados Unidos, útil para cualquier propósito, Saddam Hussein; estreno inminente en las mejores salas: *Tormenta del desierto; la secuela*. Las noticias se transmiten como entretenimiento y el entretenimiento como noticias. A medida que nos adentramos cada vez más en el corazón encantado del reino de Nunca Jamás, existen menos y menos espacios disponibles en la televisión para los sesudos y aburridos políticos que pretenden hablar de la pobreza, de la seguridad social o de la protección medioambiental. Cuando Clinton huyó del abrumador escándalo de la Casa Blanca para hacer una gira en el corazón del país y hablar de las buenas noticias económicas respecto al bajo desempleo, la baja inflación y los bajos tipos de interés, un periodista

de la CNN comentó que sería interesante... ¡ver si el presidente conseguiría «distraer» la atención de los votantes!

Bajo el brillo de la autofelicitación populista, la contravigilancia «democrática» esconde una paradoja en su propio corazón. El liberalismo sugiere que la solución a la intromisión de la vigilancia radica en la defensa de la *intimidad*, en crear barreras legales y morales que protejan al individuo de la miríada de ojos fisgones o, por lo menos, en reducir todo lo que sea razonablemente posible su capacidad de intromisión. De tales premisas derivan mecanismos burocráticos como las comisiones y comisarios dedicados a la «intimidad», los códigos deontológicos y voluntarios del sector privado y los dispositivos legales para bloquear o ralentizar el flujo de información, sus vínculos y su recuperación. Se aprueban leyes que restringen el acceso a los datos íntimos de los ciudadanos al mismo tiempo que se proclama la libertad de información, tal es la paradoja, ya que la protección de la intimidad está en intrínseca contradicción con la libertad de información. Además, en la práctica, muchos de los que han intentado acceder a ciertos archivos gubernamentales se han encontrado que las barreras más infranqueables se legitiman ahora mediante la denominada «protección de la intimidad» de la sociedad civil, irónico recurso si tenemos en cuenta que tanto las leyes que protegen la libertad de información como las que protegen la intimidad de los ciudadanos han sido promovidas por grupos de la sociedad civil para limitar el poder de vigilancia del Estado burocrático. La contravigilancia para fines democráticos tiende a ser tan intolerante con la intimidad como lo es la vigilancia estatal y empresarial. Aunque la contravigilancia sea llevada a cabo por periodistas investigadores, por académicos o por grupos y movimientos de la sociedad civil, y sean cuales sean sus resultados políticos específicos, siempre tiende al paradójico resultado de incrementar el interés hacia la vigilancia así como de aumentar la tolerancia hacia la misma. Al mismo tiempo, la protección de la intimidad es vista a menudo como una respuesta reaccionaria o inherentemente sospechosa: sólo aquellos que tienen algo que ocultar pretenderán protegerse de la mirada pública; sin duda, ésta es precisamente la defensa conservadora de la vigilancia.

La vigilancia descentralizada y multidireccional puede aumentar las oportunidades de resistencia, pero también puede contribuir al declive de la legitimidad de grandes organizaciones, entre las cuales

el Estado estará sin duda en primera línea, aunque probablemente no sea la última. Otra cuestión es la indeterminación de la frontera entre realidad y fantasía, entre noticias y entretenimiento. Si todo el mundo y todas las cosas fluyen por cámaras y casetes a disposición de cualquier curiosidad lasciva, la misma idea de una vida dedicada puramente al servicio público no sólo se hace sospechosa, sino incluso difícil de entender conceptualmente. J. Edgar Hoover escuchó clandestinamente y espió en habitaciones de hotel frecuentadas por Martin Luther King, Jr., recopilando informes sobre sus infidelidades sexuales con el objetivo de desacreditar su histórica campaña a favor de los derechos civiles. Hoover fracasó, y se convirtió él mismo en la presa póstuma de *voyeurs* que alegan que era homosexual e incluso —con muy pocas pruebas, si es que hay alguna— que se travestía en la intimidad. Pero cuando la vigilancia se vuelve multidireccional y deja de ser una prerrogativa del FBI, la intimidad empieza generalmente a considerarse poco más que un obstáculo al derecho público de saber. No tiene sentido pensar que tal atención indecente se dedicará exclusivamente a los ricos y famosos. Andy Warhol comentó que todo el mundo tendría sus quince minutos de fama en los medios de comunicación, aunque quizás ahora pueden condensarse en quince segundos. Pero, ¿y si estos quince minutos no son de fama sino de infamia? ¿Quince minutos en que uno es desnudado en toda su intimidad en *Los vídeos más censuradores de América*? La transparencia bidireccional en la ciudad de cristal puede haber sido en el siglo XVIII un sueño de Rousseau, que creía ingenuamente que la pureza de las almas, tan evidente para él, lo sería también para el resto,¹¹ podría tratarse de la pesadilla del siglo XXI.

Tal y como escribió con cierto humor Russell Baker, columnista del *New York Times*:

Georges Orwell, creador del Gran Hermano en su novela 1984, imaginó al monstruo que siempre nos vigila como un tirano político [...] Al vivir en una época de tiranos, imaginó que la tecnología del siglo XX podría engendrar dictadores políticos indestructibles. Se equivocaba en ello: las nuevas tecnologías han convertido en obsoleta la tiranía del modelo soviético.

11. Jean Starobinski, *Jean-Jacques Rousseau: La transparence et l'obstacle*, París, Gallimard, 1971.

Sin embargo, hay tiranías y tiranías. Un mundo en el que no hay escapatoria a la vigilancia no es lo que se puede desear como paraíso democrático. Y la vigilancia no se limita a las autoridades oficiales como el FBI, el fiscal Kenneth Starr o el policía local con su pistola radar. Hubo una vez un ciudadano privado que, con su cámara de videoaficionado, filmó a la policía de Los Ángeles pegando a Rodney King. Actualmente, hay cámaras de este tipo por todas partes: si se hurga la nariz, puede acabar saliendo en el *National Inquirer*; si en su patio trasero azota a su desobediente hijo de 5 años, puede acabar pasándolo mal por abuso de menores...

He oído decir que las personas que no tienen nada que ocultar no deben temer esta sofocante tecnología de vigilancia pero, ¿dónde está esta gente que no tiene nada que ocultar?¹²

Se trata de una espinosa pregunta y, en la época de la vigilancia multidireccional y descentralizada, hay otra pregunta igualmente espinosa: ¿qué ocurre cuando ya no hay donde esconderse?

12. Russell Baker, «Quiet, Quiet, Louie, There's a Bug in That Martini Olive», *The New York Times*, 13 de febrero de 1998.

7. El consultorio del Gran Hermano: el panóptico internacional

Hemos descrito a lo largo de este libro algunos de los impactos que las nuevas tecnologías han provocado en el poder y en su ejercicio. Hemos examinado las transformaciones del concepto del panóptico y de la vigilancia en tanto que mecanismos de control social. Hemos discutido la emergencia de la sociedad de la Red como un nuevo paradigma de organización política, social y económica, así como algunas de las implicaciones culturales que conllevan tales cambios. La mayor parte de nuestras investigaciones se han centrado en las democracias liberales de Norteamérica y de Europa occidental, pero las nuevas tecnologías de la información son universalizantes, y las técnicas panópticas, pioneras y desarrolladas en Occidente, seguirán expandiéndose. La sociedad de la Red o de las redes se está haciendo internacional, ya que se trata justamente de su

propia dinámica interior: ¿qué podemos prever sobre la configuración del poder en dicha sociedad de redes teleinformáticas?

¿Un feudalismo virtual?

Abbe Mowshowitz ha descrito el posible futuro de un mundo de redes teleinformáticas, al que ha denominado «feudalismo virtual»: ¹ tras analizar las tendencias tecnológicas subyacentes que han facilitado la «organización virtual» en tanto que una nueva y eficiente forma de organización, prosigue examinando los cambios estructurales de esta nueva revolución, a la que equipara, por su profundidad e importancia, con las transformaciones que derivaron del paso del feudalismo al capitalismo. También señala ciertas tendencias ya evidentes en las estructuras tradicionales de la autoridad, especialmente la familia y el Estado-nación. Respecto a este último, postula su «declive» o su «final»: si el Estado no desaparece, parece sugerir, perderá virtualmente toda su pertinencia y se convertirá en una institución insignificante.

Muchos otros han predicho de forma similar el declive y la caída del Estado-nación, pero lo que distingue a la visión del futuro propuesta por Mowshowitz es la sorprendente descripción de una irónica «repetición» histórica: la «nueva» era postestatal, sugiere, se parecerá mucho al mundo precapitalista del feudalismo. Del mismo modo que la emergencia del mercado erosionó, y en última instancia derrumbó desde el interior, el sistema de autoridad feudal, también las capacidades económicas de la flexible organización virtual erosionarían, y en última instancia derrumbarían desde el interior, las relaciones de autoridad entre los diversos Estados nacionales. Con el declive de los recursos del Estado y, en consecuencia, del mismo poder estatal, los núcleos privados del poder económico asumirían cada vez más el poder político y, al igual que en el feudalismo medieval, el sector privado asumiría y ejecutaría las funciones básicas del gobierno. No se trata de un simple cambio nominal de los proveedores de servicios públicos: con el desplazamiento de las funcio-

1. Abbe Mowshowitz. «Virtual feudalism», en Peter J. Denning y Robert M. Metcalfe (comps.), *Beyond Calculation: The Next Fifty Years of Computing*, Nueva York, Springer-Verlag, 1997, págs. 213-231.

nes también se desplazarían el poder y su legitimidad. El sector privado ejercería la autoridad en su propio nombre en vez de hacerlo en virtud de una ley que le trasciende: tal es la esencia del feudalismo.²

La imagen que ofrece Mowshowitz de este nuevo feudalismo no es muy agradable, y conlleva el empobrecimiento general de millones de personas que quedan excluidas de los beneficios y ventajas de la economía de la información; en muchos casos ya ni tan sólo serían necesarias para los trabajos menos deseados y peor pagados, ni tampoco serían amparadas por los cada vez más agónicos servicios sociales de los ahuecados y endeudados Estados nacionales. Incluso una moderada redistribución de la riqueza no podría aliviar las grotescas y exageradas disparidades sociales, ya que la lógica del máximo beneficio vinculada al poder político excluye cualquier consideración global sobre el conjunto de la sociedad, a favor de una racionalidad microeconómica. En consecuencia, es probable que el desorden se extendiese y tuviera que ser contenido por la fuerza mediante servicios de seguridad privada.³ Núcleos relativamente seguros coexistirían con áreas desprovistas de toda ley, una geografía quizás ya anticipada en Norteamérica a finales de este siglo por los contrastes entre los desolados centros urbanos y los adinerados y cercados barrios residenciales de la periferia. En el peor de los casos, habría probablemente un prolongado periodo de desorden y anarquía similar a la Edad Oscura que precedió la Edad Media, cuando las relaciones feudales ya se estabilizaron y ordenaron un poco.

Mowshowitz no despliega toda la lógica de esta analogía feudal, e incluso retrocede ante algunas de sus implicaciones más sombrías, ya que la evocación del feudalismo tiene una fuerza que va mucho más lejos del uso deliberadamente delimitado que hace de ella en tanto que mecanismo heurístico. La memoria histórica de la Edad Media que prevalece en Occidente se asocia a una jerarquía opresi-

2. Mowshowitz, pág. 226.

3. Se trata del mismo futuro, aunque sin la etiqueta de «feudal», que describen con gran deleite y entusiasmo James Dale Davidson y William Rees-Mogg en *Sovereign Individual: The Coming Economic Revolution, How to Survive and Prosper in It*, Londres, Macmillan, 1997. Mowshowitz parece mantener una amoralidad imparcial respecto a la pauperización de todos aquellos que quedan fuera de la revolución informática; Davidson y Rees-Mogg, en tanto que Thatcheristas ingleses, le dan la bienvenida como una justa confirmación para los pobres que habían tenido la temeridad, en el pasado, de esperar transferencias de bienestar de los ricos.

va, al oscurantismo y a la superstición, a la brujería, a los tiranos agresivos, a la Inquisición y a la peste negra. Imaginar que el siglo XXI pueda volver a las condiciones de hace mil años es como imaginar un descenso a la locura y a la senilidad. En este sentido, más allá de las intenciones de Mowshowitz, la visión del «feudalismo virtual» es una distopía del siglo XXI tan vívidamente amenazadora como lo fueron las distopías de 1984 o *Nosotros* para el siglo XX. La concentración definitiva de todo el poder político y económico en el Estado totalitario imaginario es sustituida por la descentralización definitiva de dicho poder en el feudalismo virtual, y ambas situaciones son igual de escalofriantes. Pero, ¿se trata de una visión realista? Después de todo, los Estados totalitarios se han hecho realidad en este siglo infligiendo violencia y sufrimiento, pero sin llegar a alcanzar nunca el ideal totalitario y, además, tampoco pudieron sobrevivir. ¿Cómo puede emerger el feudalismo virtual en tanto que sistema internacional o principio organizador global?

El modelo de Mowshowitz tiene muchos elementos a su favor. Al observar las tendencias que emergen de esta sociedad de redes teleinformáticas internacionales, podemos aislar la descentralización del poder y de la autoridad, la separación entre soberanía y territorio, la disolución de muchas de las prerrogativas del Estado-nación y de la frontera entre lo público y lo privado, la transformación del trabajo y la creación de una subclase social de desempleados permanentes y de «inempleables», el aumento de las disparidades entre riqueza y pobreza no sólo a escala internacional, sino también al interior de los países considerados ricos, y el aumento de los servicios de seguridad y de justicia en el sector privado. Tales tendencias, y otras parecidas, podrían avalar la posibilidad de que emergiese un nuevo feudalismo. Siempre existe el peligro de considerar que las tendencias del presente continuarán simplemente de modo lineal, pero Mowshowitz ha tenido la precaución de elaborar sus proyecciones del futuro no sólo sobre tales tendencias, sino considerando asimismo la base estructural que les subyace, especialmente las nuevas formas de organización que posibilitan y promueven las nuevas tecnologías de la información. Estas nuevas formas de organización también conllevan la descentralización, la dispersión y la privatización. Todo ello puede apuntar hacia un cierto «feudalismo», con centros de poder económico y político dispersos, y con una jerarquía desmesurada en la base pero algo más plana en su cima, tendencia

que seguramente aumentaría a medida que las poderosas y cambiantes congregaciones de «barones» (¿las multinacionales?) desafiaran la autoridad relativamente débil de los «reyes» (¿los Estados?).

Aunque al principio parezca convincente, tal imagen del futuro pierde consistencia y claridad cuando la examinamos más detenida y minuciosamente. Tal y como señala el propio Mowshowitz, el auténtico feudalismo se basaba en los recursos sedentarios de la tierra, mientras que el feudalismo virtual se basa en unas formas de organización que derivan de la transformación de la información en una mercancía que fluye y circula a escala internacional:

El feudalismo virtual comparte los aspectos políticos del feudalismo clásico, pero su base económica es la riqueza abstracta, y el sistema social derivado puede ser muy fluido. La institución central del feudalismo virtual será el feudo virtual, y no el castillo ni el territorio señorial del feudalismo europeo. La distribución de bienes y privilegios dependerá de los «recursos virtuales» a escala internacional, es decir, la base concreta de la riqueza abstracta puede variar según las variaciones temporales de las necesidades financieras institucionales y de las condiciones del mercado.⁴

Tales consideraciones confunden más de lo que Mowshowitz parece dispuesto a aceptar. Era justamente la permanencia de la tierra como recurso económico fundamental lo que permitió consolidar la estructura de una autoridad descentralizada en el feudalismo, aportando las condiciones para una relativa estabilidad de las relaciones sociales durante los siglos que perduró. Pero es muy difícil imaginar incluso el grado mínimo de estabilidad suficiente para que pudiese perdurar el feudalismo virtual en tanto que un nuevo sistema social cuando la fluidez, la flexibilidad y los flujos internacionales en tiempo real de la riqueza abstracta están en el mismo corazón de las formas de organización emergentes. El «feudalismo» como metáfora se muestra especialmente inepto cuando pretendemos comparar un sistema enraizado en la permanencia y la inmovilidad, en la tradición y en las costumbres, con otro basado en el cambio febril, en la liquidación y recreación constantes, en el movimiento casi por el movimiento mismo. Quizás Mowshowitz nos esté ofreciendo un

4. Mowshowitz, pág. 227.

ejemplo involuntario de lo que Marshall McLuhan nos advertía que debíamos evitar: conducir hacia el futuro mirando exclusivamente por el espejo retrovisor.

El regreso del Estado

Los análisis de Mowshowitz sobre la transición al feudalismo virtual contienen otros aspectos problemáticos. No toma en consideración lo que los economistas llaman «efectos externos», especialmente los efectos medioambientales generados por la producción de sectores privados organizados «feudalmente» y, tal y como sugiere, sin ningún tipo de control o regulación. La riqueza «abstracta» está muy bien, pero incluso una economía de la información mediante redes teleinformáticas tiene que atender una producción que no es abstracta, sino material: productos que nutren, cobijan, calientan, enfrían, visten, transportan, entretienen, curan, etc. La producción material y el consumo de tales recursos tienen unas consecuencias de las que cada vez somos más conscientes y que son a menudo acumulativas y muy graves, incluso fatales. Un mundo futuro en el que todo el poder y todos los mecanismos de regulación están efectivamente dispersos en una multitud evanescente de empresas privadas en pos de sus beneficios, con identidades corporativas limitadas, a menudo de corta vida, y cada una de ellas defendiendo sus propios intereses económicos e inmediatos, tal perspectiva es sin duda una vía hacia la degradación medioambiental del planeta que amenaza las mismas condiciones de vida terrestre: una macroirracionalidad de proporciones desmesuradas.

Aunque todo esto no implica que tal perspectiva no pueda realizarse, al no tener en cuenta el impacto medioambiental, Mowshowitz deja abierta una inmensa grieta en la funcionalidad de su modelo. Cabe señalar que esta misma grieta ya está siendo identificada por la economía política internacional actual, lo que ha empujado a ciertos Estados, en retirada en tantos otros asuntos, a afirmar su presencia, su autoridad y su capacidad de decisión. En un sentido muy general, la degradación medioambiental no interesa a nadie; incluso en el sentido más reducido de la microeconomía, son «racionales» todas las actividades que generan beneficios, aunque sea a costa de devastar el medioambiente. Pero si la regulación de comportamien-

tos autodestructivos es universal, de modo que nadie pudiese perder ventajas competitivas frente a otros competidores sin regulación, no existe pérdida real, sólo una mejora general: esto significa que tal regulación debe ser internacional.

Sólo existe, sin embargo, un espacio efectivo para poder instaurar regulaciones medioambientales: el Estado-nación. Una regulación internacional requeriría acuerdos y compromisos entre gobiernos: Estados individuales con el poder y la voluntad para hacer cumplir tal regulación a los organismos y agentes privados que operan en su jurisdicción. De aquí proviene la tentativa de la década de los noventa para establecer una cooperación interestatal, con el objetivo de controlar la perjudicada capa de ozono y la emisión de gases de efecto invernadero. Sin duda puede debatirse hasta qué punto funcionan, en la práctica, tales acuerdos específicos, pero el inicio de una cooperación entre Estados (relativamente fuertes) para instaurar una regulación medioambiental a escala internacional es probablemente sólo el principio de otros acuerdos, en distintos ámbitos y áreas de interés común y de peligro planetario. La ausencia de cualquier referencia a esta dimensión en el modelo del feudalismo virtual es una carencia importante. El feudalismo clásico, después de todo, entró en una crisis terminal en el siglo XIV tras siglos de explotación agrícola sin ninguna consideración ecológica, lo que culminó en hambrunas masivas seguidas de la devastadora peste negra. Las instituciones feudales no podían contener ni gestionar tales catástrofes «naturales», por lo que se desataron amargas luchas sociales con constantes revueltas de campesinos y artesanos, que ayudaron a acelerar el declive y la caída del modo de producción feudal. No hace falta ni decir que el capitalismo contemporáneo empequeñece al feudalismo en su capacidad de amenazar el equilibrio ecológico planetario y, en consecuencia, su propia seguridad y pervivencia.

Otro gran defecto del modelo del feudalismo virtual, así como de otras extrapolaciones sobre el futuro con redes teleinformáticas internacionales, es el papel asignado inherentemente a la marginalidad en la economía internacional. Como mucho, los empobrecidos o perseguidos son considerados delincuentes o criminales, de los que se ocuparía un servicio de seguridad (básicamente privado). Es como si hubiera algo irracional en esta precipitada pulsión de los neoliberales para reducir e incluso eliminar cualquier programa de bienestar social. A fin de cuentas, con tantos desempleados perma-

nentemente alejados de cualquier disciplina laboral (especialmente los varones jóvenes), los programas de subsidio de desempleo, mediante su estricto control burocrático, permiten instaurar una especie de sistema secundario de vigilancia y disciplina. Cuando el panóptico, a causa de su aversión al riesgo, sigue recortando los créditos y ayudas a los ciudadanos más desvalidos e indigentes, también pierde otro mecanismo de control sobre los márgenes de su sistema. No es, por lo tanto, ninguna sorpresa que tales ciudadanos acaben, muy fácilmente, bajo la disciplina coercitiva —y mucho más costosa— de las cárceles, un área en constante expansión y crecimiento en Estados Unidos. Aunque en dicho país el sistema de prisiones se traslada cada vez más hacia el sector privado, sigue dependiendo de las licencias y regulaciones del Estado; es evidente que el sector privado no puede asumir aún, por medio de empresas privadas, la totalidad de los gastos policiales, judiciales y carcelarios de la sociedad.

Del mismo modo que la aplicación de regulaciones es uno de los eslabones ausentes en el modelo del feudalismo virtual, también lo es la cuestión de la seguridad (y por consiguiente de la soberanía), que Mowshowitz asigna con mucha labia al sector privado; ambos aspectos se tambalean ante un examen minucioso. Es cierto que, en Norteamérica, la seguridad privada ya ha superado a la seguridad pública respecto a la asignación de recursos y personal, y que la justicia privada también ha sustituido, hasta un grado sorprendente, la justicia pública al interior de organizaciones privadas, que pueden llegar a prescindir de la intervención de la policía y de los procesos judiciales formales.⁵ Pero tales tendencias siempre se han desarrollado en los confines de las fronteras nacionales, dentro de un armazón público de seguridad y de justicia que otorga ciertos grados de autonomía a la seguridad privada, pero en última instancia ésta sigue dependiendo de licencias y delegaciones (limitadas) de la autoridad pública.

El problema de los costes sociales del crimen y de la delincuencia entre las endémicas subclases sociales no es sólo un punto ciego de los programas neoliberales. La idea de que la economía internacional procederá hacia sus conclusiones lógicas y definitivas sin ninguna resistencia efectiva, excluyendo a la marginalidad de todos

5. C. D. Shearing y P. C. Stenning, *Private Security and Private Justice: A Review of Policy Issues*, Montreal, Institute for Research on Public Policy, 1983.

los beneficios del sistema, es una idea bastante absurda que se opone a cualquier lección histórica. Tampoco existe ninguna razón para imaginar, junto a los sosos teóricos de la hegemonía corporativa, que sólo la empresa capitalista será capaz de comprender y explotar con éxito las nuevas formas de organización promocionadas y recompensadas por las nuevas tecnologías de la información.

«¡Te vigilamos, Gran Hermano!»

A principios de 1998 se reseñó que «en su mayor acción informática hasta la fecha [...] los rebeldes [zapatistas del EZLN] piratearon unas páginas *web* del gobierno mexicano, rellenándolas con imágenes del rebelde revolucionario que da nombre a su organización, Emiliano Zapata. Una parte del mensaje revolucionario, enviada a la *homepage* del Ministerio de Economía, decía: “¡Te vigilamos, Gran Hermano!”».⁶ Los zapatistas han sido descritos como «la primera guerrilla informática».⁷ Esta acción particular tiene un hermoso contenido simbólico, pero quizás poca sustancia. Señala, sin embargo, la destacada capacidad del movimiento revolucionario para comunicarse a escala internacional, mediante Internet, la televisión u otros medios, mientras prosigue su rebelión campesina contra el gobierno mexicano y su política neoliberal de acuerdo con los cánones internacionales. Es posible que los vínculos y conexiones internacionales que los zapatistas han establecido a escala internacional mediante las nuevas tecnologías de la información hayan impedido al gobierno mexicano tratar tal rebelión sólo con las consabidas represiones masivas, permitiendo en cambio la opción tan inusual de una negociación. Tal y como explica Castells, «su estrategia no consistía en la guerra efectiva. Los zapatistas usaban armas para hacer una declaración, luego exponían la posibilidad de su sacrificio ante los medios de comunicación internacionales con el objetivo de forzar una negociación y conseguir una serie de demandas razonables que, como pa-

6. «Zapatista Rebel Supporters Wage Virtual War», *Wired News*, 4 de febrero de 1998.

7. Manuel Castells, *The Information Age: Economy, Society and Culture*, vol. 2: *The Power of Identity*, Oxford, Blackwell, 1997, págs. 68-83 (trad. cast.: *La era de la información: economía, sociedad y cultura*, vol. 2, *El poder de la identidad*, Madrid, Alianza, 1998).

recen indicar los sondeos de opinión, tenían un amplio respaldo en la mayoría de la sociedad mexicana [...] La habilidad de los zapatistas para comunicarse con el mundo y con la sociedad mexicana, así como para llamar la atención de la gente y de los intelectuales, han propulsado un grupo insurgente local y débil a la vanguardia de la política internacional». ⁸ También han sido importantes los respaldos que se han desarrollado en diversas direcciones públicas de Internet establecidas en México. El Chase Manhattan Bank señaló a sus inversores que el gobierno mexicano tendría que acabar con el movimiento rebelde para recuperar la confianza de los inversores: inmediatamente, unas páginas *web* norteamericanas de apoyo a la causa zapatista introdujeron todo el texto en la Red, movilizando a poderosos inversores contra el banco, aquellos que consideran a la democracia tan importante como sus beneficios de inversión. ⁹

Otro caso menos conocido en el que las redes teleinformáticas jugaron un papel importante en un movimiento de resistencia es el de los indios cree de James Bay, al norte del Quebec: su exitosa campaña contra el megaproyecto hidroeléctrico «James Bay Dos» o «Gran Ballena», ávidamente promovido durante años por el gobierno del Quebec y sus compañías hidroeléctricas. HydroQuébec tiene una importancia crucial y enorgullece el nacionalismo quebequés. El anterior proyecto «James Bay Uno» se desarrolló como un recurso básico para tales aspiraciones nacionalistas: un proyecto vasto y de sofisticada tecnología, que conectaba al Quebec con los mercados de exportación de energía hidroeléctrica internacionales; todo un símbolo de la capacidad del Quebec para construir un Estado moderno y consolidar una economía *quebequesa*. El proyecto «James Bay Dos» sería la continuación de tal desarrollo y, después de que el partido secesionista tomara el poder en 1994, también sería un símbolo de la decisión y capacidad del Quebec para romper con las constricciones del federalismo canadiense y poder ocupar su lugar en la economía internacional.

Desde la perspectiva de las tribus aborígenes del norte del Quebec, el desarrollo de los proyectos «James Bay» se muestra de modo muy diferente: se trata de una arremetida agresiva e imperialista de la «civilización» capitalista y europea en el mismo corazón de las

8. Castells, *op. cit.*, pág. 79.

9. «A Rebel Movement's Life on the Web», *Wired News*, 6 de marzo de 1998.

tierras y la economía nativas. Las presas hidroeléctricas transforman radicalmente el paisaje y el equilibrio ecológicos, inundando antiguas tierras, desviando ríos y riachuelos, cortando y rompiendo los senderos migratorios de la vida salvaje autóctona y perturbando los hábitos de caza y aprovisionamiento. Era necesario desplazar y «reubicar» a comunidades enteras. A primera vista, este proceso parece remitir al paradigma de la modernidad, inmiscuyéndose agresivamente en las formas de vida tradicionales. Las cuadrículas hidroeléctricas avanzan sin descanso por los paisajes agrestes, sometiendo todo, hombres y animales, árboles y ríos, a medida que prosigue su camino. Mediante la alquimia tecnológica, la naturaleza se transforma en poder, y así alimenta las máquinas de la industria capitalista. Las particularidades, las tradiciones y las irregularidades son sometidas a las rígidas e inflexibles directrices del imperio que transporta este poder a los mercados extranjeros, conectando y subordinando de este modo las tierras de los indios a las redes de la economía internacional.

Los proyectos de «James Bay» movilizaron una resistencia mucho mayor en los planes de la segunda fase. No se trataba de una desesperada y última resistencia final de indios en peligro. Se desarrolló una sofisticada campaña publicitaria internacional para convencer a la opinión pública, con el apoyo de la destacada figura política de Robert Kennedy, Jr., y de una importante agencia de publicidad norteamericana. Los indios *se conectaron a la Red*, asociándose a grupos medioambientales internacionales con experiencia y competencia en los sistemas de comunicación internacionales, lo que generó una publicidad muy desfavorable para el gobierno del Quebec en los medios de comunicación, tanto de Norteamérica como de Europa occidental. La legislatura de Nueva York (el mayor mercado para la exportación de la energía hidroeléctrica del Quebec) fue convencida para rechazar la compra de esta energía generada por el proyecto «Gran Ballena». El gobierno del Quebec, ante las voces que llegaban de Washington, en donde los cree se enfrentaban a los portavoces del Quebec en un ambiente generalmente hostil a este último, desistió finalmente del proyecto «Gran Ballena».

Los indios aborígenes del norte del Quebec, amenazados por los lazos asfixiantes del capitalismo internacional (el entramado del poder), se defendieron conectándose a las redes teleinformáticas de los grupos medioambientales internacionales. Sin duda, la batalla por

los derechos de los aborígenes apenas ha progresado gracias al éxito de esta escaramuza, pero su estrategia de resistencia es interesante y ofrece un modelo para la nueva era de la información.

Otro ejemplo reciente de resistencia mediante la conexión a las redes teleinformáticas es la exitosa campaña contra el Acuerdo Multilateral en Inversiones (MAI). Tal acuerdo, alcanzado tras largas negociaciones secretas de los gobiernos bajo la égida de la Organización por la Cooperación y el Desarrollo Económico (OCDE), hubiera instaurado una regulación obligatoria respecto al tratamiento de los inversores extranjeros.¹⁰ Todo se desarrollaba suavemente puertas adentro, hasta que un grupo de apoyo a los intereses comunes del Canadá puso sus manos sobre un anteproyecto del acuerdo. Un periodista ha descrito los acontecimientos posteriores del siguiente modo:

Políticos con mucho poder tenían un montón de estadísticas para demostrar por qué una regulación internacional de las inversiones mejoraría el mundo. No estaban contrastadas, sin embargo, con otros datos de entidades y grupos de la sociedad civil que, con poco más que sus ordenadores y el acceso a Internet, derrumbaron el acuerdo. Sin duda, las negociaciones internacionales se han transformado después de la exitosa anulación del Acuerdo Multilateral en Inversiones (MAI), gracias a la oposición de grupos civiles que, alarmados por la tendencia de una economía global, usaron otros mecanismos internacionales para defenderse.¹¹

Las organizaciones no gubernamentales canadienses, muchas de las cuales ya habían estado implicadas en campañas sin ningún éxito contra la instauración del Acuerdo de Libre Comercio entre Estados Unidos y Canadá de 1989, así como contra el subsiguiente Acuerdo de Libre Comercio de Norteamérica (ACLAN), aprendieron de los nefastos resultados de sus campañas previas y preciberespaciales. Esta vez, se conectaron con otros grupos *on-line* de distintos países, como por ejemplo la Red del Tercer Mundo localizada en

10. Tony Clarke y Maude Barlow, *MAI: The Multilateral Agreement on Investment and the Threat to Canadian Sovereignty*, Toronto, Stoddart, 1997.

11. Madelaine Drohan, «How the Net Killed the MAI: Grassroots Groups Used Their Own Globalization to Derail Deal», *The Globe & Mail*, Toronto, 29 de abril de 1998.

Malasia. Disponían inmediatamente de cualquier nueva noticia o dato relativo al anteproyecto del acuerdo secreto, y desarrollaron análisis críticos de todas las implicaciones del MAI para los diversos gobiernos nacionales que circularon rápidamente alrededor del mundo. La información acumulada en un país, que podía ser comprometedora para otro, se hacía inmediatamente pública. Atrapados en su propio secretismo, los gobiernos nacionales quedaron paralizados en su capacidad de respuesta. Sin duda, muchas de las organizaciones no gubernamentales estaban más informadas sobre los detalles e implicaciones del MAI que la mayoría de los ministros a los que se enfrentaban. Una ola de protestas internacional barrió las negociaciones de la OCDE, que admitió su derrota a principios de 1998. «Ésta es la primera campaña exitosa de las organizaciones no gubernamentales mediante Internet», afirmó un diplomático involucrado en las negociaciones, «ha sido muy efectiva.» Tras haber bloqueado el anteproyecto del acuerdo, las mismas organizaciones ya están impacientes por jugar un papel más positivo en el futuro; para ofrecer, por ejemplo, propuestas constructivas de lo que debería constar en los acuerdos comerciales, en lugar de mantener una simple oposición a las negociaciones gubernamentales. Tal y como lo expresó uno de los activistas canadienses a lo largo de esta campaña: «Estamos en contra de este modelo de economía global, pero la idea de una comunidad global en la que podríamos trabajar todos juntos es un ideal estupendo».¹²

El obispo de ningún sitio y de todas partes

Para ofrecer otro ejemplo de cómo las nuevas tecnologías de la información están impulsando nuevas formas de resistencia, podríamos recurrir a la estructura de autoridad jerárquica más antigua y continuista del mundo: la Iglesia católica. Ninguna otra organización se acerca ni tan siquiera remotamente a su longevidad; originada en los tiempos del imperio romano, la Iglesia se expandió durante la época feudal y prosigue a finales del segundo milenio sin ninguna disminución de sus proporciones, todo lo contrario, se extiende actualmente más que nunca. A lo largo de estos dos mil años, su jerar-

12. *Ibíd.*

quía de poder ha aprendido algunas cosas para mantener su autoridad. Al enfrentarse a curas turbulentos y molestos, el Vaticano ha aprendido que existen técnicas más efectivas que la represión inmediata. Una de ellas consistía en nombrarlos obispos de una diócesis inexistente llamada «Partenia», supuestamente situada en la cordillera del Atlas, en medio del desierto del Sahara, al norte de África. Partenia no estaba literalmente en ningún sitio, una diócesis sin iglesia y sin fieles, un producto de la imaginación de la jerarquía eclesiástica muy útil para desembarazarse de curas molestos que podían ser consignados en ella, desvaneciéndose sin dejar rastro y sin el fastidio de una inquisición o un castigo. Así fue usada durante siglos, hasta que llegó el obispo Jacques Gaillot en 1995.

Gaillot era el antiguo obispo de Evreux, en Francia, un cura con una marcada tendencia de izquierdas que discrepaba de la doctrina papal en numerosos aspectos. En vez de mantener sus posiciones en privado, Gaillot las expresaba públicamente, en solidaridad con organizaciones y causas de las que el Vaticano se había mantenido oficialmente distante. El papa asignó a Gaillot la diócesis de Partenia, y sin duda esperaba no volver a saber nada más de él. Había funcionado durante siglos, pero aparentemente la era del ciberespacio marcaba su final. Jacques Gaillot construyó una Partenia simplemente en tanto que una dirección pública en Internet. La diócesis de ningún sitio había encontrado su hogar en un medio de comunicación que tampoco está en ningún sitio pero que llega a todas partes. Una diócesis en las áridas montañas del Sahara era, en el pasado, tan silenciosa como la arena del desierto, pero una diócesis virtual en el ciberespacio otorga al obispo una voz que puede escucharse desde todas partes, y un grupo de fieles que se reparte por todos los rincones del mundo. Así que, a principios de 1998, cualquier visitante de las páginas *web* de Partenia podía leer los pensamientos del obispo a favor de las manifestaciones de los desempleados contra el gobierno francés, y también podía mandarle sus opiniones por correo electrónico. Un autor francés reivindicó ramificaciones religiosas del ciberespacio: «La mente de Dios es imitada por la estructura virtual de Internet, en donde la diferencia entre la realidad física y la existencia real ha sido finalmente eliminada».¹³ Para no confundirnos: la Iglesia católica

13. Edward Rothstein, «Finding Utopia on the Internet», *New York Times*, 27 de octubre de 1997.

apenas ha sido afectada en su fundamento por esta peculiar disidencia *on-line*, aunque exista un desafío implícito a la autoridad jerárquica en el uso de las nuevas tecnologías que, quizás, pueda provocar uno o dos pequeños escalofríos en la jerarquía eclesiástica.

Existen muchos otros ejemplos de resistencia política mediante las nuevas tecnologías de la información. La lucha popular contra el régimen serbio de Slobodan Milosevic recibió un fuerte estímulo mediante las conexiones a Internet, que no sólo aportaron un mayor respaldo a los disidentes, sino que además les permitía seguir comunicándose con la opinión pública cuando el régimen censuraba los medios de comunicación tradicionales, estrategia que Milosevic no podía controlar. Los sindicatos en lucha en Corea del Sur y el movimiento estudiantil de China que conllevó la masacre de la plaza de Tiananmen (en aquel tiempo dependían básicamente del fax) constituyen otros ejemplos. Menos espectaculares pero quizás más importantes a largo plazo son los movimientos populares en diversos países del Tercer Mundo que han empleado la Red como un instrumento de organización, descubriendo que las redes internacionales pueden aportarles una conexión en tiempo real con una multitud de organizaciones no gubernamentales involucradas en la asistencia para el desarrollo, así como a grupos de campesinos, trabajadores e indígenas que se enfrentan a problemas similares en otros países. Incluso en aquellos países que disponen de muy pocos ordenadores y de escasas líneas telefónicas, un pequeño grupo de activistas con acceso a tal tecnología puede canalizar la comunicación para el resto del movimiento en una doble dirección: consiguiendo información del resto del mundo para sus intereses locales, y enviando su propia información local a todos los rincones del planeta.

Ninguna reseña sobre las implicaciones políticas de la Red estaría completa sin reconocer el papel que ha jugado en el impulso de la propaganda de extrema derecha neonazi o de grupos racistas, tanto en Norteamérica como en Europa. Algunos se especializan en la negación del Holocausto, otros en transmitir información práctica sobre bombas letales y otros dispositivos terroristas. Grupos como las Milicias Americanas mantienen contacto entre sí mediante la Red, así como con otros grupos neofascistas de diversos países europeos. A finales de 1997, en Génova, en una conferencia patrocinada por las Naciones Unidas, se señalaba que «el número de direcciones públicas en Internet con apología de la violencia o del racismo se ha

doblado casi hasta seiscientas en el último año [...] Existen al menos 94 direcciones que defienden la jerarquía racial y que clasifican a los europeos por el color de su piel, por su religión, sus características étnicas e incluso por su lenguaje preferido [...] [en aquel momento podían contarse] 87 direcciones neonazis, 35 de apología a la supremacía blanca y 51 con apología del terrorismo».¹⁴ No es ninguna sorpresa que este tipo de apología de la violencia y del racismo hayan provocado demandas de censura en la Red, con la habitual perplejidad ante el reto de llevarla a cabo sin socavar la libertad de expresión y sin frenar la libre espontaneidad que ha caracterizado el desarrollo de Internet. Ya existen leyes en funcionamiento que permiten controlar la propaganda y apología de la violencia contra grupos identificables y que, en teoría, podrían invocarse contra los autores de tales páginas *web* tan prontamente como en los medios impresos. En la práctica, tanto la autoría como la localización de una dirección en la *web* internacional son aún difíciles de conseguir dentro de los límites legales de cualquier jurisdicción. Para aquellos que consideran que las nuevas tecnologías ofrecen la oportunidad de avanzar en programas políticos progresistas, el predominio de una agitación racista y fascista devuelve una lección que sin duda hace reflexionar: la Red no tiene inherentemente ningún color político. También ofrece una irónica demostración del potencial subversivo de las nuevas tecnologías, ya que tanto el fascismo como el racismo son ahora expresiones ideológicas excluidas de la corriente legitimada del discurso político occidental. La habilidad que han manifestado tales grupos para explotar las nuevas tecnologías para sus intereses políticos es simplemente el testimonio de las oportunidades abiertas por el nuevo panóptico descentralizado para las redes subversivas, así como para cualquier otra opción política.

¿Cerrar la puerta trasera?

Las implicaciones potencialmente subversivas del ciberespacio no han pasado desapercibidas por los regímenes cerrados y autoritarios. Singapur ofrece un ejemplo especialmente intrigante de una so-

14. Elizabeth G. Olson, «Nations Struggle With How to Control Hate on the Web», *New York Times*, 24 de noviembre de 1997.

ciudad capitalista, con ambiciones internacionales y muy favorable a las innovaciones en alta tecnología pero que adopta, sin embargo, una fuerte tendencia autoritaria respecto a la libertad de expresión. Singapur es una sociedad estrechamente controlada, cuya ciudadanía es sometida a una sofisticada tecnología de vigilancia que es quizás más evidente que en cualquier otro lugar. El tráfico, por ejemplo, es intensamente controlado mediante una vigilancia informatizada y electrónica a la que también se somete el tráfico pedestre, e incluso infracciones menores, como ensuciar la calle, son castigadas con prontitud. Singapur quiere y necesita un acceso completo a Internet para potenciar al máximo sus negocios y finanzas internacionales mediante las conexiones en tiempo real pero, al mismo tiempo, pretende controlar y censurar tales accesos a los usuarios locales, para proteger al régimen contra las ideas foráneas, potencialmente perjudiciales. Singapur ha intentado, en efecto, construir un panóptico local, abierto a las oportunidades del capitalismo internacional pero cerrado a las alternativas políticas. Es poco probable, sin embargo, que el Estado pueda realmente mantener a largo plazo su capacidad de controlar selectivamente el ciberespacio: ¿es realmente posible que un Estado relativamente pequeño abra totalmente sus puertas respecto a una área internacional mientras las cierra en otra? El ciberespacio es quizás un medio de comunicación demasiado plástico y proteico como para ser domesticado de este modo tan selectivo. Como los antiguos puertos marinos del pasado, el ciberespacio es una ventana abierta al mundo: los barcos salen cargados de mercancías para la exportación y vuelven con numerosos bienes obtenidos del intercambio, pero siempre es posible que también regresen con elementos extraños y exóticos, con una atmósfera que remite a lo desconocido, e incluso con semillas de subversión. Y, sin duda, los mares son inmensos y los puertos foráneos quedaban muy distantes, mientras que en el ciberespacio todo circula muy rápido, en tiempo real.

China es otro Estado que ha decidido domesticar Internet, aprovechando su potencial pero reduciendo su energía. Según un artículo del *Financial Times*:

China anunció ayer una regulación con una serie de medidas para controlar el uso de Internet, una tentativa de castigar a los usuarios de la Red que, según el líder Beijing, están accediendo a secretos estatales

y difundiendo «información perjudicial». El gobierno chino ha mostrado hasta ahora una actitud ambivalente respecto a Internet, instintivamente asustado ante su capacidad de difundir información subversiva, al mismo tiempo que atraído por el modo en que respalda y acelera la innovación tecnológica.¹⁵

El país más poblado del mundo tiene aún muy pocas conexiones a Internet; cuando se impusieron las regulaciones podían contarse unas 620.000, muchas de ellas quizás compartidas por hasta diez o veinte personas, lo que no alcanza ni siquiera el 1 % de la población. Sin embargo, los disidentes dentro y fuera de China han empezado a utilizar las posibilidades que ofrece este nuevo medio de comunicación para difundir su desacuerdo. Tal y como comentó el *New York Times*:

La lucha de China por domesticar el salvaje y retorcido movimiento tentacular de Internet refleja lo que muchos expertos consideran el enigma central del gobierno: ¿cómo promover la libertad y el crecimiento económicos mientras se mantienen apretados los torniquetes políticos? El agente de seguridad que anunció la nueva regulación no confirmó ningún posible intercambio o trueque, sólo dijo: «La gestión segura y efectiva de las redes teleinformáticas es un prerequisite para su suave instauración, y el camino hacia la modernización tecnológica del país».¹⁶

Quizás el régimen notoriamente represivo de China pueda tener éxito en lo que tantos otros han fracasado, pero es sorprendente la contradicción inherente a este síndrome de atracción y repulsión hacia las nuevas tecnologías.

Podemos buscar una analogía en el impacto de un antiguo medio de comunicación, la televisión, sobre el antiguo régimen de la República Democrática Alemana. Los alemanes del Este podían recibir fácilmente las señales de televisión de Alemania del Oeste, lo que conllevaba una grave amenaza a la frágil legitimación de un Estado artificial e impopular. La televisión de Alemania occidental llevaba

15. James Harding, «China Crackdown on Internet "Subversion"», *Financial Times*, 31 de diciembre de 1997.

16. Eric Eckholm, «China Cracks Down on Dissent in Cyberspace», *New York Times*, 31 de diciembre de 1997.

sus mensajes y valores capitalistas directamente en los hogares de Alemania del Este, sin ningún tipo de barrera lingüística o cultural. El régimen podía sin duda prohibir directamente la venta de televisores, pero no estaba preparada para tal prohibición, ya que la televisión representaba un símbolo de su «éxito» económico y, además, era un importante instrumento de propaganda del que no quería prescindir. Tal propaganda no fue muy popular, como pone de manifiesto un antiguo chiste de la época: «¿Qué es un "Ul'b"? Un Ul'b es la unidad mínima de poder que uno se ahorra al apagar el televisor durante un discurso de Ulbricht», por entonces el jefe del partido. No tenía ninguna sentido encargar a la Stasi la elaboración de informes sobre aquellos que veían las emisoras prohibidas: todos lo hacían, y todos sabían que todos lo hacían; castigar a los infractores aleatoriamente hubiese sido fútil. Así que las imágenes de la vida en el Oeste llegaban puntualmente cada noche a las salones de los hogares de la RDA, erosionando el aislamiento que supuestamente protegía al sistema comunista y atrayendo a un número cada vez mayor de personas a huir hacia el Oeste, a través del muro de Berlín, hasta el colapso final y la posterior reunificación de las dos Alemanias. Existen múltiples causas para la debilidad y el colapso final de la RDA y de su régimen, entre las cuales la televisión del Oeste difícilmente figura entre las principales; pero fue realmente como un incesante goteo, que lenta pero inevitablemente erosiona una superficie dura.

El inspector inspeccionado: el panóptico cibernético

Las implicaciones políticas exactas de las nuevas tecnologías son aún, sin duda, muy poco conocidas. Los optimistas señalan las oportunidades que nos brinda el ciberespacio, así como la flexibilidad de las nuevas fronteras en las redes teleinformáticas. Los regímenes autoritarios sienten su amenaza, que sin duda existe y es importante. Los pesimistas se inclinan por argumentar que tanto la riqueza como el poder dominarán el ciberespacio, del mismo modo que dominan el mundo real, insistiendo en la estructura privada que caracteriza la propiedad de estos nuevos medios de comunicación, así como la concentración corporativa que se desprende de la convergencia entre distintos tipos de empresas (software, hardware, telefonía y cableado, entretenimiento, etc.) y de sus fusiones, aso-

ciaciones, alianzas estratégicas y otras colaboraciones. La pregunta que se desprende de sus críticas es: ¿cómo podemos competir con esta acumulación de poder e influencia en el sector privado? Incluso Orwell pone cara de invitado desconcertado, mientras el gobierno norteamericano pretende insistir en obtener los mismos privilegios en el ciberespacio que obtenía con los antiguos medios de comunicación.

Quizás un antiguo chiste pueda ser apropiado para esta cuestión: El optimista declara felizmente que «vivimos en el mejor de todos los mundos posibles»; el pesimista simplemente responde que, desgraciadamente, el optimista puede sin duda tener toda la razón. Lo que está claro es que las nuevas tecnologías han reestructurado totalmente el ejercicio del poder panóptico, convertido en una entidad descentralizada y «consensual» que se extiende mucho más allá del poder que emana explícitamente de la cima, con la participación de todos los sujetos en su propia vigilancia. También facilitan la comunicación horizontal inmediata entre los sujetos del panóptico, así como la posibilidad de «vigilar al vigilante», de instaurar una posibilidad democrática de vigilancia desde abajo. Se ha destruido el inevitable aislamiento y separación de los prisioneros del panóptico de Bentham, las paredes de las celdas se han derrumbado y, además, el inspector puede ser inspeccionado. Bentham había proyectado un artificio arquitectónico para desarrollar la ilusión de una figura central que lo sabe todo pero es incognoscible: una figura divina. Actualmente, las nuevas tecnologías ofrecen el material y también la ilusión de la omnisciencia, pero tales tecnologías también eliminan incesantemente los velos que antaño oscurecían el rostro del poder. La transparencia monodireccional de la ciudad de cristal es sustituida por una transparencia bidireccional. El modelo cibernético se basa en unas conexiones de realimentación que provocan constantes ajustes y reajustes: el panóptico cibernético se repliega sobre sí mismo.

En 1984, Winston Smith trabaja en el Ministerio de la Verdad y su labor consiste en reescribir constantemente la memoria histórica, enviando los textos antiguos que ya no se consideran políticamente correctos al agujero negro de la memoria. Hubo un tiempo en la antigua Unión Soviética en el que la Gran Enciclopedia Soviética se reescribía constantemente de un modo similar al descrito por Orwell. Un conocido ejemplo es el del artículo que ensalzaba al infame jefe de la policía secreta, Lavrenti Beria, que fue eliminado tras su

ejecución y reemplazado por otro sobre el mar de Bering. También hubo ejemplos notables de fotografías manipuladas para borrar a ciertos personajes indeseables, tal y como ocurrió con la fotografía de Lenin y Trotski en la que este último fue eliminado totalmente. El verdadero Estado totalitario fue, sin embargo, menos eficiente que el imaginado por Orwell: se conservaron diversas copias de las fotos originales que permitieron una comparación crítica con las manipuladas; algunos de los propietarios de la Enciclopedia podían resistirse a eliminar el artículo de Beria y añadir el del mar de Bering. En 1984, todos los medios de comunicación están tan rigurosamente controlados desde lo más alto del poder que, cuando la información es enviada al agujero negro de la memoria, se desvanece para siempre cualquier rastro de su existencia. Ninguna dictadura real ha alcanzado este grado de control pero, con las nuevas tecnologías, incluso el grado de control que antes podía alcanzarse está desvaneciéndose rápidamente de las manos de todos. Consideremos la facilidad con que la información puede buscarse desde cualquier lugar, cargarla como archivo en el ordenador personal y, simultáneamente, reenviarla alrededor del mundo a todas las direcciones de correo electrónico que deseemos. Consideremos que cuando enviamos un correo electrónico a una dirección situada en un país con tendencia a censurar la información que reciben sus ciudadanos, podemos cifrar el mensaje, encriptarlo de un modo suficientemente sofisticado como para convertirlo, si no en invulnerable, al menos en muy difícil de descifrar. Consideremos que si, por lo que sea, la apariencia de un mensaje claramente cifrado puede atraer la atención de indeseables, la misma información puede transmitirse bajo la forma de una fotografía o de una pieza musical que, mediante la clave adecuada, podrá leerse como un mensaje digitalmente codificado.¹⁷ Consideremos finalmente que tales capacidades no son la prerrogativa de un Estado de seguridad secreto y poderoso ni de sus servicios de inteligencia, sino que están abiertas a cualquiera que disponga de una modesta cantidad de dinero y de una mínima competencia tecnológica.

17. Esta técnica de encriptación, denominada Stego, ha sido desarrollada por una de las figuras más exóticas del ciberespacio. Romana Machado, también conocida como Cypherella, una antigua modelo de California que explica sus dotes de encriptación en las páginas *web* de una dirección de Internet, y sus encantos personales en otra dirección, erótica, también de Internet.

Ya hemos señalado las manifiestas habilidades del Tercer Mundo y de los pueblos indígenas para sacar provecho de las oportunidades que ofrecen las nuevas tecnologías, y las redes teleinformáticas globales, para sus estrategias de resistencia. La globalización del capitalismo irá seguramente acompañada de una globalización similar de las redes de resistencia, tales como sindicatos, feministas, ecologistas y otros grupos de la sociedad civil, conectándose a través de cualquier frontera para luchar contra causas comunes, formando, deshaciendo y recreando distintas alianzas para embarcarse en otras causas, exactamente del mismo modo que las flexibles empresas del capitalismo forman y deshacen organizaciones virtuales para operaciones financieras concretas.

Algunas veces, tales grupos de resistencia pueden juntarse con ciertas alianzas de Estados e incluso con ciertas corporaciones privadas para obtener la fuerza necesaria contra otros Estados o empresas. El caso de las minas terrestres es un ejemplo: una alianza internacional de organizaciones no gubernamentales, utilizando figuras tan mediáticas como la difunta princesa Diana, movilizó la opinión mundial y a un grupo de Estados con un poder relativamente fuerte, liderados por Canadá, que consiguió establecer un tratado internacional contra las minas terrestres, a pesar de la desgana, si no la clara oposición, de Estados Unidos.

En otros casos, se considerará a la resistencia como una amenaza para el capital, sometiénola a la represión y a la vigilancia de los servicios de inteligencia y de seguridad, así como de las fuerzas policiales. Ni el coste ni la responsabilidad de un poder de represión internacional podrán recaer exclusivamente en el sector privado. Sea cual sea la forma precisa y la naturaleza de las redes de resistencia, así como las respuestas del capitalismo internacional, es evidente que la configuración de tales fuerzas no se limitará a un nuevo pseudofeudalismo.

Cuando observamos el panorama internacional, lo que más se acercaría a las anárquicas condiciones del feudalismo virtual, vemos algo muy distinto: las multinacionales están amenazadas en sus negocios internacionales por organizaciones «ilegítimas» que también operan a escala internacional: terroristas, algunos con tendencias políticas, otros simplemente criminales, que atacan a los ejecutivos o los raptan para pedir un rescate, o amenazan la seguridad de sus inversiones. El crimen organizado internacional puede negociar con

drogas, comercio ilegal de armas, apuestas ilegales, prostitución, y tener incluso otros negocios legítimos como tapadera; también blanquean grandes cantidades de dinero negro y destinan otro tanto a la corrupción sistemática de los gobiernos más vulnerables. Existen espeluznantes paralelismos entre las actividades criminales y la economía internacional. Las mafias se organizan en clanes que ignoran las fronteras y jurisdicciones nacionales, tal y como tienden a operar también las multinacionales. No sólo utilizan las nuevas tecnologías para hacer sus negocios, sino que también han reestructurado sus tradicionales formas de organización para sacar el mayor provecho a los beneficios que éstas ofrecen: flexibilidad en la búsqueda y obtención de oportunidades, o una mayor habilidad para las alianzas y asociaciones, así como para disolverlas bruscamente cuando ya no sirven para el propósito con el que fueron concebidas. Finalmente, han mostrado una notable capacidad para explotar las nuevas tecnologías según sus intereses mediante las inventivas formas del «ciber-crime».

La «economía criminal internacional», encarnada en el blanqueo de dinero, se ha convertido, en palabras de Manuel Castells, «en un componente muy significativo y perturbador de los flujos financieros internacionales y de las reservas del mercado mundial», pero «el impacto del crimen en las instituciones estatales y en la política nacional es aún mayor. La soberanía del Estado, ya sacudida por el proceso de globalización [...] está directamente amenazada por los flexibles clanes del crimen organizado, que evitan cualquier control y asumen unos niveles de riesgo imposibles de asumir por cualquier otra organización».¹⁸ Pero incluso bajo esta amenaza directa, los Estados se han hecho más necesarios que nunca, y precisamente por esta misma amenaza. Ante estas penetrantes amenazas transnacionales, que podríamos llamar la cara oscura de la globalización, los intereses privados «legítimos» se muestran relativamente indefensos sin la ayuda de los Estados y de sus extensos cuerpos de policía y servicios de seguridad e inteligencia, y también con su experiencia y su poder para imponerse.

18. Manuel Castells, *The information Age*, vol. 3: *End of Millenium*, Oxford, Blackwell, 1998, págs. 201-202 (trad. cast.: *La era de la información: economía, sociedad y cultura*, vol. 3, *Fin de milenio*, Madrid, Alianza, 1999).

El Estado natural mundial: ¿desagradable, brutal y dañino?

Existe otra analogía histórica que puede ser provechosa. En la Inglaterra del siglo XVII, el modo de producción capitalista para la agricultura estaba sustituyendo a las degradadas instituciones feudales, y numerosos campesinos eran eliminados de los campos. Al mismo tiempo, el capitalismo mercantil también aumentaba en importancia, centralizado en ciudades de donde salían a amplias rutas comerciales. Las estructuras políticas se rezagaban algunas veces tras estos desarrollos económicos, y la confusión política conducía a menudo a guerras civiles. En este contexto de revueltas se generó la teoría política inglesa moderna. Hobbes y Locke fueron las figuras preeminentes y, aunque muy diferentes en sus prescripciones, ambos desarrollaron la noción de un contrato social que subyacía y justificaba la función de los gobiernos. Aunque ambos justificaron y racionalizaron el concepto de Estado, ambos eran pensadores «liberales», preocupados por emancipar las nuevas fuerzas productivas del mercado y, al menos en el caso de Locke, liberar y dar una mayor capacidad de expresión a las energías políticas de la nueva clase comercial. Hobbes en particular ha sido un rompecabezas para muchos estudiosos, por su entusiasta descripción del gobierno en tanto que «Gran Leviatán», con su aparentemente extensa y amplia gama de poderes y soberanía, que parecen, a primera vista, curiosamente en tensión con su defensa de las relaciones contractuales que conlleva el mercado, consideradas el fundamento de la sociedad racional.¹⁹ De hecho, las nociones del siglo XVII de un Estado «Leviatán» se convierten en muy poca cosa frente a las realidades del siglo XX: la mayoría de las actividades que actualmente sabemos sujetas a una rutinaria regulación e intervención estatal, Hobbes las consideraba perfectamente capaces de desarrollarse sin el conocimiento del Estado, y desde luego sin su intervención. Sin embargo, en tanto que teórico prominente de la soberanía, Hobbes hizo mucho por establecer los fundamentos de la noción moderna del Estado soberano en tanto que lugar de un poder y de una autoridad sin competidores, inmune a cualquier desafío. La combinación de esta concepción sobre la soberanía del Estado con la emergencia de un mercado libre no es tan

19. C. B. Macpherson, *The Political Theory of Possessive Individualism: Hobbes to Locke*, Oxford. Clarendon Press, 1962.

difícil. Para que las relaciones contractuales puedan sustituir a las antiguas relaciones feudales, los contratos deben ser cumplidos; tal y como Hobbes argumentó lúcida y convincentemente, el mercado sin ningún tipo de regulación no puede garantizar por completo las obligaciones contractuales, ni siquiera la seguridad de las propiedades. Abandonado a sus propios mecanismos como un «Estado natural» sin gobierno, el mercado se convierte en una guerra de todos contra todos, en el que la vida es «solitaria, pobre, desagradable, brutal y dañina».²⁰ La solución de este dilema es el contrato social, en el que todo el mundo acepta transferir sus poderes a la soberanía estatal: un poder común que trasciende a todos los ciudadanos y que puede hacer cumplir de forma imparcial las obligaciones contractuales, y hacer por lo tanto funcionar al mercado. De aquí la coyuntura histórica entre el apogeo del capitalismo y de un Estado-nación relativamente fuerte.

Actualmente, la economía internacional ha liberado al capitalismo de las ataduras del Estado-nación, y el capitalismo transnacional ha sabido sacar el mejor provecho a esta libertad. Pero tal y como Hobbes lo entendía, el Estado no sólo constriñe, también protege y posibilita. La competencia de la economía internacional amenaza con reproducir algunas de las condiciones del «Estado natural» de Hobbes. Sin lugar a dudas no puede y no habrá un Leviatán internacional en las mismas condiciones y posición que conlleva el universal contrato social hobbesiano. Tal y como he tratado de indicar, las condiciones estructurales para una autoridad soberana, absoluta y centralizada han empezado a desvanecerse a escala nacional, no digamos ya a escala internacional. A pesar de la paranoia de algunos respecto a los Derechos Americanos, no existe ningún gobierno dictatorial a escala mundial, ya sea bajo bandera comunista, sionista, de la banca internacional o de cualquier otro color, que aceche en el horizonte, aspecto sobre el que Mowshowitz tiene toda la razón. Pero el salto desde aquí hasta un feudalismo recurrente anterior a la época de Hobbes y a la emergencia de las relaciones del mercado capitalista es un salto demasiado largo. Es mucho más que probable que las condiciones para una competición económica a escala internacional requieran, si no un Leviatán en tanto que tal, al menos un

20. Hobbes, *Leviathan*, Hammondsworth, Middlesex, Penguin Books, 1968, parte II, cap. 13.

equivalente funcional que sea adecuadamente designado para un mundo de redes teleinformáticas, quizás un panóptico internacional: ¿A qué puede parecerse?

El consultorio del Gran Hermano

Ya hemos señalado en un capítulo previo que uno de los primeros desempleados a causa del advenimiento del panóptico participatorio es el Gran Hermano: las nuevas tecnologías de vigilancia convierten sus servicios en obsoletos. Los Hitlers y Stalins de la vida real se han convertido en historia, así como la imagen idealizada de un dictador totalitario, omnisciente y omnipotente. Un mundo de redes teleinformáticas es un mundo con el poder ramificado, difuso, con diversos núcleos situados en intersecciones clave de las redes teleinformáticas internacionales. Como mucho, podemos imaginar a dictadores regionales tripulando algunos de estos núcleos, los Saddam Husseins y Slobodan Milosevics del futuro.

Los despidos por causas tecnológicas a menudo tienen límites: algunos trabajos eliminados de ciertas empresas vuelven a aparecer al exterior de la empresa, como consultorías, contrataciones, etc. Existe incluso un término inglés para describir esta nueva flexibilidad laboral que complementa las reducciones de plantilla y las «re-equilibra»: *outsourcing*. Actualmente, ante los desafíos de la economía internacional, y especialmente ante las amenazas que plantea la inestabilidad inherente a la globalización, así como ante el crecimiento de la sombra paralela del crimen organizado a escala internacional, lo que más arriba hemos denominado la cara oscura de la globalización, el Gran Hermano es introducido de nuevo en tanto que consultor externo, o algo parecido.

¿Por qué deberían las grandes corporaciones transnacionales emprender enormes inversiones en el personal y los recursos materiales requeridos para alcanzar una capacidad que sólo duplicaría la que los grandes Estados ya poseen? Además, las empresas multinacionales también deberían, para llevar a cabo tal duplicación, prepararse para una estrecha cooperación, casi perpetua y muy difícil, con sus competidores, que sin duda sería necesaria para llevar a cabo operaciones de seguridad efectivas a escala internacional. Parece más sencillo que reclamen la estrecha cooperación de sus respectivos Estados para

que actúen en su nombre, y para que vigilen y controlen la emergencia y el desarrollo de esta nueva economía global, gracias a lo cual las multinacionales podrían concentrarse en sus intereses fundamentales: hacer dinero. Esto es exactamente lo que las grandes corporaciones privadas y empresas multinacionales están haciendo a finales del siglo xx: animando a los Estados para que aumenten sus colaboraciones interestatales y puedan intervenir con fuerza en diversas actividades internacionales, algo que sin duda contradice directamente la visión de un mundo de feudos privados ejerciendo su soberanía en áreas delimitadas, tal y como plantea la hipótesis del feudalismo virtual.

Esto no quiere decir que los Estados seguirán pareciéndose a lo que han sido hasta ahora, y de hecho ya se están transformando en entidades más flexibles, menos rígidas. Sin duda no pueden ser todos equiparados a un mismo nivel, siendo muchos los débiles y algunos los fuertes, pero todos los Estados pueden convertirse en entidades mucho más especializadas, conservando aquellas funciones para las que están mucho mejor equipados y preparados que el sector privado, mientras transfieren otras funciones, ya sea totalmente o por delegación, al sector privado.

Uno de los ámbitos en el que los Estados tienen ventaja respecto a cualquier organización privada es en el ejercicio de la coerción. Las tecnologías de vigilancia y represión puede fabricarse en el sector privado en busca de beneficios, pero serán los Estados quienes más las detentarán y usarán, así como las asociaciones entre Estados. Aquí es donde el Gran Hermano reaparece en tanto que consultor externo. Su probada experiencia y efectividad en la interceptación y coerción a escala internacional mediante cooperaciones estatales puede capacitarle para defender el próspero Oeste, con su policía transnacional, sus bases de datos comunes y su sofisticada tecnología de vigilancia y control político, ya sea para enfrentarse a la emigración y a los refugiados, por ejemplo, o para combatir con sus satélites y su tecnología de telecomunicaciones a grupos terroristas o supuestamente terroristas.²¹ Éste es el tipo de cosas que los Estados

21. Respecto a la «Fortaleza Europea», véase: Michael Spencer, *States of Injustice: A Guide to Human Rights and Civil Liberties in the European Union*, Londres, Pluto Press, 1995; Tony Bunian (comp.), *Stewatching the New Europe*, Nottingham, Russell Press, 1993; Steve Right, *An Appraisal of Technologies for Political Control*, Luxemburgo, Parlamento Europeo, Junta Directiva General para la Investigación, 1998.

y las agencias estatales hacen realmente bien, y sin duda se concentrarán y especializarán en ellas. Pero ya no se trata de fines en sí mismos, o de medios dedicados exclusivamente a engrandecer el Estado en pos del antiguo ideal totalitario; se trata más bien de un ejercicio de la coerción, especializado y funcional, que se aplica en un mundo complejo de redes teleinformáticas internacionales.

Empezamos este libro considerando «el siglo de los servicios de inteligencia», y es el momento adecuado para cerrar el círculo volviendo a los servicios de inteligencia en tanto que adquisición sistemática e intencional de información secreta. El Estado se ha descentralizado, el poder se ha dispersado y difundido, y la vigilancia se ha hecho multidireccional pero, aunque el panóptico participatorio prescinde de muchos de los elementos del antiguo poder estatal, también mantiene muchos otros. Tales desarrollos no eliminan, sin embargo, el requisito de un régimen de vigilancia internacional que respalde cualquier intervención coercitiva.²² Tal requisito es necesario porque, en un mundo de redes teleinformáticas, existen numerosos elementos de inestabilidad y contradicción; es necesario porque agentes no estatales, como los terroristas, pueden amenazar la estabilidad del sistema estatal internacional, por no mencionar los simples negocios y las inversiones internacionales; es necesario porque el mundo teleinformático está duplicado y amenazado por un sosia, la cara oscura de la globalización: el crimen organizado a escala internacional, y en consecuencia la corrupción sistemática, el tráfico de drogas ilegal, la venta ilegal de armas, el blanqueo de dinero, etc.

Tras la Guerra Fría, hubo algunas especulaciones infundadas respecto al posible carácter obsoleto de los servicios de inteligencia y seguridad. El hecho de que esto no haya ocurrido ha provocado el cinismo y la burla de algunos críticos, que acusan a la burocracia de tales agencias de mantener vivos sus imperios y privilegios mediante la búsqueda de nuevos enemigos, para subsanar el cese de los predecesores. Sin duda hay algo de cierto en ello, ya que ninguna organización burocrática abandona voluntariamente sus prerrogativas, y tiende en cambio a ser muy creativa para poder perpetuarse. Pero los nuevos enemigos señalados por los servicios de inteligencia no son ficticios, sino que son muy reales, y existe un buen fundamento para

22. Stephen Gill, «The Global Panopticon? The Neoliberal State, Economic Life, and Democratic Surveillance», *Alternatives*, 2, 1995, págs. 1-49.

argumentar que la función de los servicios de inteligencia, así como su tecnología y métodos específicos, son exactamente lo que hace falta para poder controlar, interpretar y elaborar minuciosos mapas topográficos de los clanes de criminalidad y terror que ensombrecen la economía internacional. Las amenazas que prescinden de las fronteras estatales exigirán una mayor cooperación entre Estados, pero los servicios de inteligencia ya tienen una amplia experiencia en alianzas, así como en compartir actividades alrededor de las telecomunicaciones globales, experiencia forjada durante la Guerra Fría bajo la presión de enfrentarse a una amenaza percibida en común respecto al bloque rival. Las amenazas son ahora más difusas, pero la experiencia acumulada antaño para construir, desarrollar y mantener redes de vigilancia internacional, generalmente entre las mismas agencias y no mediante relaciones intergubernamentales, nos ofrece un interesante paradigma de cómo se resolverán y organizarán tales asuntos en el mundo teleinformático del futuro. En la época del ciberespacio, las nuevas tecnologías de la información facilitan a los clanes del crimen internacional proliferar, e incrementar su amenaza no sólo en relación con las instituciones económicas del capitalismo, sino también respecto a las instituciones políticas de los Estados democráticos y, más insidiosamente, a sus sociedades civiles. Los estragos que causa el abuso de drogas en las principales ciudades norteamericanas y europeas es una muestra suficiente para percibir el coste humano que exigen los cuarteles del crimen organizado a escala internacional.

El terrorismo ha sido sin duda mal usado por los gobiernos en tanto que excusa para ciertos excesos represivos, así como para inmiscuirse en comunidades sospechosas, tales como los grupos de emigrantes que provienen de países de los que emana una actividad terrorista internacional. Pero esto no implica que el terrorismo sea una amenaza inventada por los Estados y, cuando existe la posibilidad de que proliferen armas de destrucción masiva, ya sea nucleares, químicas o biológicas, no sólo en manos de los denominados Estados peligrosos como Iraq, sino en manos de agentes no estatales con programas político-religiosos incompatibles con cualquier idea de orden internacional o incluso nacional, entonces existe realmente un problema de la mayor gravedad. Mencionemos, por ejemplo, la milenaria comunidad de culto Aun Shinrikyo, en el Japón, que liberó un gas mortífero en tres vagones del metro de Tokio, causando doce

mueritos y cinco mil heridos. Otros grupos con métodos más convencionales de destrucción se han responsabilizado de actos como la explosión de una bomba en el World Trade Center de Nueva York. El potencial de destrucción al que podrían acceder tales grupos si consiguen adquirir armas nucleares, químicas o biológicas no es algo que se hayan inventado ciertos Estados histéricos. Para intentar adelantarse a tales amenazas, los dispositivos y mecanismos existentes de vigilancia y coerción, ya distribuidos a escala internacional, serán de gran utilidad. El avanzado sistema de interceptación telecomunicativa descrito más arriba²³ forma parte de ello, así como la vigilancia internacional mediante satélites. Pero también será necesaria la ayuda de los métodos más tradicionales de los servicios de inteligencia, tales como la integración de espías u otras fuentes de información en comunidades sospechosas.

Consideremos el problema del blanqueo del dinero negro, que es un punto clave para seguir el filo de muchas de las actividades que constituyen la cara oculta de la globalización. Tanto el capital internacional como los Estados se sienten igual de amenazados por este proceso, que utiliza las nuevas tecnologías y redes teleinformáticas para financiar actividades criminales y corromper a personajes tanto gubernamentales como del sector privado. Trazar el circuito de todos los movimientos de este blanqueo de dinero es algo que remite a los servicios de inteligencia, pero aportar pruebas y cargos compete a las fuerzas policiales. Ninguna de las dos cosas puede lograrse con cuerpos nacionales trabajando aisladamente contra tales actividades transnacionales. Los medios tecnológicos para combatir tal amenaza existen; y no hay ningún límite teórico respecto de su capacidad actual de vigilancia para poder controlar los flujos financieros y las transacciones internacionales, ocurran donde ocurran, asumiendo una asociación internacional con el régimen denunciante. De hecho, una oficina de la Tesorería de Estados Unidos, apodada FinCen, está actualmente coordinando un esfuerzo internacional en esta dirección. Cuando se complete tal sistema de vigilancia financiera, cualquier transacción —desde el uso personal del cajero automático hasta los mayores flujos del capital— podrá ser controlada. El software de inteligencia artificial ha sido y está siendo desarrollado para poder explorar esta vasta e impresionante área de datos con el objetivo

23. Véase el capítulo 4.

de poder reconocer patrones anómalos. Cuando se identifican movimientos financieros sospechosos, el gobierno o los gobernantes del país en que han tenido lugar tales actividades deberán dar su permiso para que prosiga la investigación y pueda llegar a juicio. La tecnología no es el problema, pero la cooperación entre Estados a escala internacional sí que lo es.

Un régimen de vigilancia internacional de este tipo suscita sin duda otros problemas. Los defensores de las libertades civiles objetarán ante esta intromisión de ojos observando detenidamente los asuntos financieros de la ciudadanía; las multinacionales, a pesar de reconocer la importancia de controlar la economía criminal internacional, pueden mostrarse reacias a someter a un escrutinio exterior algunas de sus operaciones menos escrupulosas. Lo que se plantea finalmente, sin embargo, es el problema hobbesiano del orden y, con él, la posibilidad de que otros elementos «legítimos» de inestabilidad a escala internacional puedan ser también vigilados y controlados, tal y como los mercados financieros y los flujos de capital, asuntos que hasta la fecha sólo se han sometido a los mecanismos de vigilancia multilateral como los del Fondo Monetario Internacional. La idea de que los gobiernos carecen actualmente del poder para controlar en tiempo real los flujos del capital es sin duda certera, si los Estados se consideran entidades aisladas que intentan ejercer un poder soberano y autónomo. Pero un mundo de redes teleinformáticas internacionales no impide la posibilidad de una cooperación internacional para instaurar un régimen de vigilancia económica que haga cumplir ciertas prescripciones.²⁴ La tecnología ya está dispuesta para llevarlo a cabo, y el motivo para asegurar la estabilidad contra una ruinosa volatilidad también está disponible, pero la voluntad y la capacidad política son sin duda más problemáticas. El problema, sin embargo, ya ha sido expuesto, y seguirá en la agenda y en el orden del día del futuro.

24. La crisis financiera asiática de 1997-1998 provocó que incluso algunos prestigiosos economistas neoliberales se preguntaran en voz alta si el papel tradicional del FMI, es decir, su presión para que los gobiernos adopten políticas neoliberales, no debería ser reemplazado por el de un organismo preparado para regular los mercados e instituciones financieros, en lugar de sacarles de apuros después de que hayan fracasado.

El poder se transforma

Imaginemos un mundo en el que el Estado-nación, tal y como lo entendemos actualmente, ha perdido efectiva y drásticamente su capacidad e importancia, por lo que las inversiones de la economía privada y las decisiones de producción se hacen con incluso menos consideraciones que las actuales respecto a los efectos (residuales) en los márgenes de la nación; la soberanía política se ha separado casi totalmente, aunque nunca del todo, del territorio, y el poder político se ha dispersado entre múltiples núcleos que se sitúan en la intersección de múltiples redes teleinformáticas, sobre todo, aunque no exclusivamente, económicas, que trazan el esqueleto de la economía política internacional. Tales núcleos no son «nacionales» en tanto que tales, aunque algunos puedan fundamentarse más en una nacionalidad que en otras. Incluso aquellos con una influencia nacional relativamente fuerte deben su fuerza a los vínculos teleinformáticos con otros núcleos que cruzan a menudo por sus líneas nacionales. Las naciones aún existen en un sentido cultural y sociológico, pero el otrora poderoso y potente motor del Estado-nación se ha disgregado casi por completo.

Tal imagen es drásticamente distinta de la del feudalismo virtual, puesto que la propiedad no es fija e inamovible, sino flexible y móvil. Su base institucional es proteica, con organizaciones constantemente formándose y recreándose en alianzas cambiantes y asociaciones con otras organizaciones. También difiere del feudalismo virtual en que los intereses económicos privados *no* se han apoderado del poder político, aunque pueda ser compartido por alianzas entre el sector público y el privado, en las que ciertos aspectos del poder coercitivo son entregados o delegados a partes privadas.

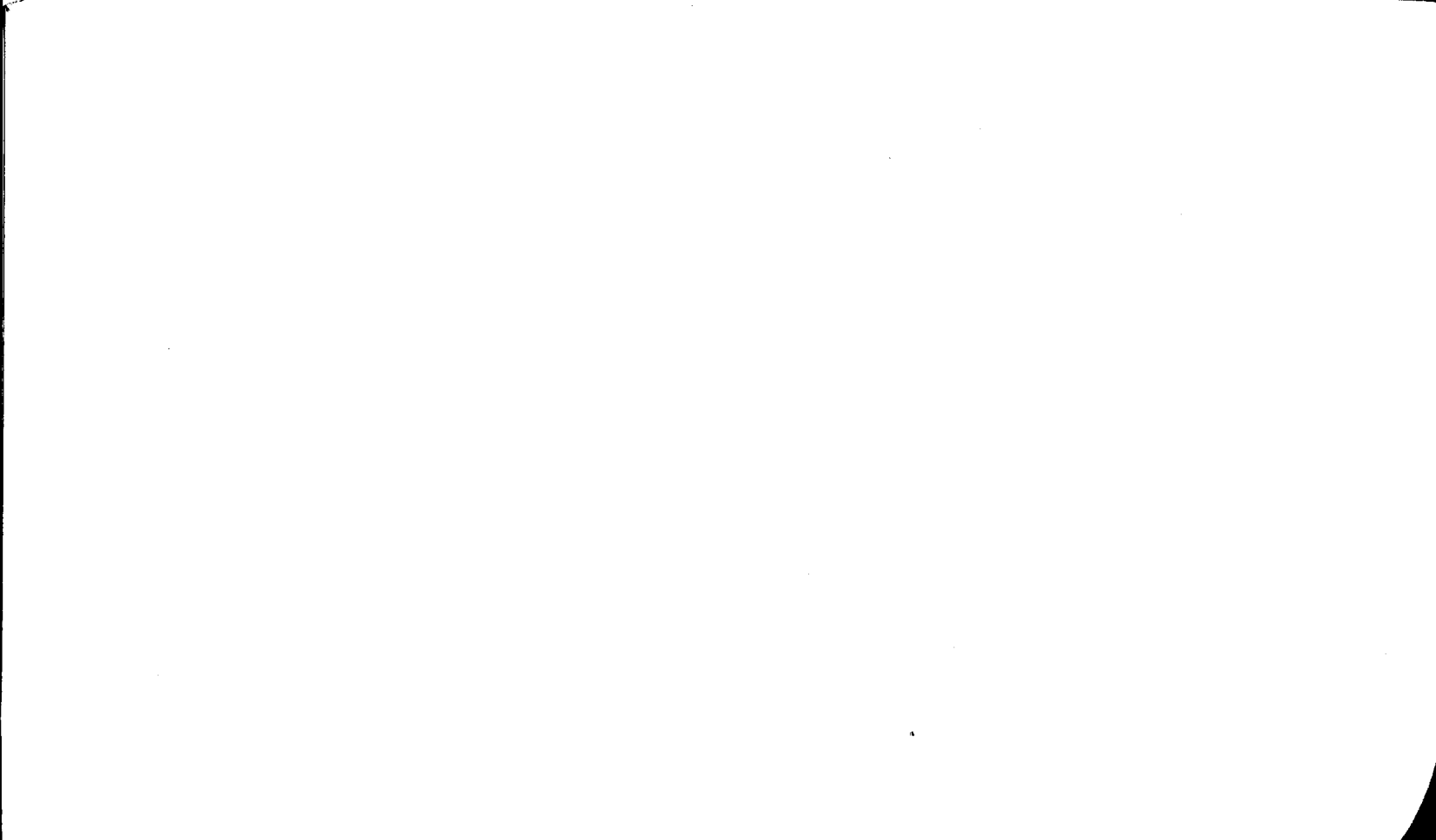
Tal y como sugiere Manuel Castells, un mundo teleinformático provoca «una espectacular reorganización de las relaciones de poder»:

Las conexiones que vinculan a ciertos organismos e instituciones (por ejemplo, los flujos financieros que controlan a los imperios mediáticos para influenciar los procesos políticos) son los instrumentos privilegiados del poder. Así que los agentes de tales conexiones son los poseedores del poder. Puesto que las redes de organismos e institucio-

nes son múltiples, los códigos y conexiones entre tales redes se convierten en el elemento clave para la formación, orientación o desorientación de las sociedades.²⁵

El problema del poder y de sus usos o abusos se mantiene a lo largo de las transformaciones económicas y sociales que nos aportan las nuevas tecnologías y los nuevos modos de producción y distribución de los bienes y de los servicios, así como la organización del saber y de la información. También se mantiene, tan interminable a su propia manera como los procesos de un mundo teleinformático, el potencial para incrementar democráticamente el control de tales conexiones. Las nuevas tecnologías de la información no han cerrado tales trayectorias, sólo han reestructurado el terreno sobre el que se representarán las batallas del futuro.

25. Castells, *Information Age*, vol. 1: *The Rise of The Network Society*, Oxford, Blackwell, 1996, pág. 471 (trad. cast.: *La era de la información: economía, sociedad y cultura*, vol. 1, *La sociedad red*, Madrid, Alianza, 1999).



Índice analítico y de nombres

- Acta para la Decencia en las Comunicaciones, 143-144
- Acuerdo de Libre Comercio de Norteamérica (ACLAN), 206
- Acxiom (empresa), 162
- Agencia Central de Inteligencia (CIA), 16, 20, 23, 25, 31
- Agencia de Seguridad Nacional (NSA), 116, 127, 135, 136
- Alemania:
- nazismo, 16, 23, 35, 41
 - reacciones británicas, periodo anterior a la Primera Guerra Mundial, 33-34
- Alemania del Este:
- Stasi, 33, 35
 - televisión en, 212-213
- America's Funniest Home Videos* (*Los vídeos domésticos más divertidos de América*, programa de televisión), 187
- Ames, Aldrich, 25, 26
- Angleton, James Jesus, 23-24
- Apolo, misión a la luna, 113-114
- Arpanet, 73
- Audiovigilancia, véase Tecnología de escucha clandestina
- Aum Shinrikyo (secta), 223-224
- Aumento de las capacidades, la cuestión del, 89-90, 128-131, 145-149
- resistencia, redes teleinformáti-

- cas de, 203-210. *Véase también* Globalización planetaria
- Aversión al riesgo, 60-61, 187
- efectos de las bases de datos, 159-160, 166, 167-169
- inseguridad en la sociedad te-
leinformática, 99-100
- Aviv, David, 106
- Babbage, Charles, 69
- Baker Russell, 193-194
- Baltimore, 105
- Bases de datos:
- beneficios de la inclusión, 165-167
- categorías de información per-
sonal en las, 155-156
- definición de «datos», 20
- efectos de exclusión, 159-160, 166, 167-169
- fantasmas de nosotros mismos, 167-169
- informes de los servicios de in-
teligencia en contraste con, 151-154
- invasiones del sector privado, 160-167
- muerte de la intimidad, 163-167
- propósito y efectos de evitar el
riesgo, 159-160, 166
- recopilación de datos, 156-157
- réplicas sombrías, 167-169
- Sistemas de Información Geo-
gráfica (GIS), 160-162
- vigilancia de datos, 154-160
- vinculación de datos, 154-157
- Bell (laboratorios), 70
- Benetton, 184
- Bentham, Jeremy, 46-49, 50, 51, 53-54, 171-172, 177, 214
- Beria, Lavrenti, 36, 214-215
- Berlín (túnel), 24-25
- Bhagavad Gita*, 82
- Biblioteca de Babel, 65-66, 69
- Biotechnología, 77-80
- creación de inteligencia, 79-81
- ingeniería genética, 77-81
- Blade Runner* (película), 78-79
- Blake, George, 24, 25
- Blanqueo de dinero, detección del, 29, 224-225
- Blunt, Anthony, 39
- Borges, Jorge Luis, 65-66, 69, 86-87
- Brave New World* (*Un mundo feliz*, Huxley), 186
- Burgess, Guy, 25, 39
- Burke, Edmund, 48
- Burocracia, 58-60
- Cairncross, John, 25, 39
- Canadá:
- campana contra el Acuerdo
Multilateral en Inversiones
(MAI), 206-207
- escándalos videográficos, 188
- resistencia de los indios cree a
los proyectos «James Bay»,
204-206
- Capitalismo, 52-53. *Véase también*
Marketing
- fábrica panóptica, 52-55
- Carnés de identidad, 121-127
- Castells, Manuel, 96, 203, 217, 226
- Caza de brujas, 31-40
- Censura, 140-145
- Centro de Información Íntima y
Electrónica, 139
- Centro para la Democracia y la Tec-
nología, 121
- Chase Manhattan Bank, 204
- CHECA (Commision to Combat
Counterrevolution and Sabota-
ge), 35
- China:
- control de Internet, 211-212
- movimiento estudiantil, 209

Churchill, Winston, 16-19, 135

Ciberspacio:

bases de datos, *véase* Bases de datos

censura, en el, 140-145

clones informáticos (*bots*), 76-78

control autoritario, del, 210-211

creación de, 74-75

espionaje empresarial, en el, 92-94

fantasmas de nosotros mismos en el, 167-169

globalización planetaria, *véase*

Globalización planetaria

«infobombo» *versus* realidad, 87-91

novios virtuales, 75

piratas informáticos, 92-93

realidad económica del, 87-91

robots y ciborgs, 81-86

sociedad red, 96-100

software inteligente, 29, 76-78

virtualidad descafeinada, 89-90

Ciborgs, 83-86

Ciencias sociales, 57-58

Clinton, Bill, 115, 138, 139, 189-192

Clipper chip, 138

Clones informáticos (*bots*), 76-78

Coca-Cola, 184-185

COLOSO (ordenador), 70

Cookies «galletas», 131

Consejo Industrial de las Tecnologías de la Información, 129-130

Consumidor *versus* ciudadano, 186-187

Corea, 17

avión comercial KAL-007, derribo del, 27

sindicatos en Corea del Sur, 209

Correo electrónico:

efectos en la comunicación del, 148-149

vigilancia del, 132-134

Cortina de humo, *La* (película), 191

Criptografía, 15-17, 20-21, 132-133
encriptación de clave pública, 135-140

saber criptográfico, 19, 132-136, 138-139

Cucarachas robot, 113

CyberPatrol, 143-144

Dandeker, Christopher, 45

«Death of privacy, The» (Quittner), 164

Delegados de software, *véase* Clones informáticos

Dell, ordenadores, 98

DES, encriptación, 137

Desencriptación, *véase* Criptografía

Desintermediación, 189-190

Diebert, Ronald, 185

Diffie, Whitfield, 132-133

Digitalización, 67-69, 154. *Véase también* Ordenadores

Disney World, 175-176

2001: Odisea del espacio, 82

Dunn, Ashley, 136

Dyson, Freeman, 80

Early Bird, satélite, 111

East Newark, Nueva Jersey, 105

ECHELON, 118, 133

Einstein, Albert, 18

E-mail, *véase* Correo electrónico

Empleo, *véase* Lugar de trabajo

Encriptación, *véase* Criptografía

ENIAC, ordenador, 70

Escuelas, 58

Espionaje, *véase* Servicios de inteligencia

Espionaje, novelas de, 25-26, 33-34

Estados Unidos:

asunto Lewinsky, 115, 189-192

censura en el ciberespacio, 142-144

CIA, 16, 20, 23, 25, 31

- encriptación de clave pública, posición respecto a la, 138-140
 Guerra Fría, 17, 22-30, 33
 policía internacional, como, 31-32
 sistemas de comunicación de los servicios de inteligencia, 116-117
 Etzioni, Amitai, 133
 Exclusión, 186-187
 consumidor *versus* ciudadano, 186-187
 efectos de las bases de datos, 159-160, 166, 167-169
 evitar el riesgo, véase Aversión al riesgo
 Expertos en eficacia, 54
 Exploración médica, 38
 Especialización de las retransmisiones televisivas, 178-179

 Fábricas, véase Lugar de trabajo
 Falcon, software, 123-124
 FBI, Departamento Federal de Investigación (*Federal Bureau of Investigation*), 33, 36, 40, 44, 90, 121, 123, 138, 161, 193-194
 Feudalismo, metáfora del, 196-203
 Feudalismo virtual, 196-203
Financial Times, 211-212
 FinCen, 224
 FLIR, tecnología de Búsqueda Infrarroja, 108
 Ford, Henri, 53, 145
 Foucault, Michel, 10, 46, 47, 51
 Fragmentación de la audiencia de masas, 177-178
 Fuchs, Klaus, 18

 Gaillot, Jacques, 208
 Gandy, Oscar H., Jr., 46
 Gates, Bill, 184
 Gays y lesbianas, 38, 181-183

 GCHQ, Jefatura de Comunicaciones del Gobierno Británico (*Government Communications Headquarters*), 94, 116, 136
 Genoma Humano, proyecto, 78
 Gestapo, 35
 Gestión empresarial «científica», 53-55, 145-146, 147-148
 Gibbon, Edward, 65
 Gibson, William, 85-86, 91
 Giddens, Anthony, 52
 Gingrich, Newt, 88, 119-120
 GIS, Sistemas de Información Geográfica, 160-162
 Globalización planetaria:
 cara oscura de, 216-221, 222-225
 desalojo y consultoría del Gran Hermano (*outsourcing*), 220-225
 extrema derecha, conexiones te-
 leinformáticas de la, 209-210
 indios cree de James Bay, conexiones te-
 leinformáticas de los, 204-206
 MAI, campaña contra, 206-207
 modelo del feudalismo virtual, crítica del, 196-203
 páginas *web* del obispo Gaillot, 208
 regímenes autoritarios, esfuerzos por controlar la, 210-211
 zapatistas, conexiones te-
 leinformáticas de los, 203-204

 Goldhammer, Don, 167
 Gore, Al, 87, 143
 Gotlieb, Calvin, 165
 GPS, Sistema de Posicionamiento Global, 110
Grid, The (Kerr), 83
 GRU, 25
 Guatemala, golpe de Estado, 31
 Guerra del Golfo, 32, 92

- Guerra Fría, 17, 22-30, 33, 38, 41, 70, 73, 116, 118, 222-223
- Hager, Nicky, 117
- Haggerty, Kevin, 146, 159
- Haraway, Donna, 83-84
- Historia de la decadencia y ruina del Imperio Romano* (Gibbon), 66
- Hitler, Adolf, 23, 41
- Hobbes, Thomas, 218-219, 225
- Homosexuales, 38, 181-183
- Hoover, J. Edgar, 33, 36, 40, 44, 193
- Howard, Michael, 22-23
- Hussein, Saddam, 32, 191, 220
- Huxley, Aldous, 186
- IBM, 184
- Iglesia católica, 207-209
- Impuestos, 55-56, 155, 157-159
- Información estadística, 56-57
- Información sobre vuelos y billetes internacionales, 126-127
- Inglaterra:
- carne nacional de identidad inteligente, 126
 - servicios de inteligencia, 15, 20-21, 34, 38, 94, 116-117, 135
 - vigilancia videográfica, 105-106
- Intel, 137
- Inteligentes, carnés de identidad, 121-127, 173-174
- Intercepción de las telecomunicaciones, 116-117
- almacenamiento de las intercepciones, 117-119
 - teléfonos móviles, 119-121
- Intercepción de teléfonos móviles, 119-121
- Internet (la Red), 64. *Véase también* Ciberespacio
- aumento de las capacidades ofrecido por, 89-90, 128-131. *Véase también* Aumento de las capacidades, la cuestión del
 - censura en, 140-145
 - desarrollo de, 73-74
 - desintermediación, 189-190
 - Cookies* «galletas», problema de las, 131
 - infoguerra, 93-94
 - Plataforma para la Selección del Contenido de Internet (PICS), 143-144
 - realidad económica de, 87-91; 94-96
 - rumores en, 188-189, 200
 - sociedad red, 96-100
 - vigilancia del correo electrónico, 132-134
- Intervención telefónica, 19, 115-116
- Intimidación:
- contravigilancia, paradoja de la, 192
 - muerte de la, 163-167
 - vigilancia videográfica, implicaciones de la, 109-110, 174-175
- Irangate, 134, 188
- Iraq, 32, 92
- Japón, 16-17, 75, 113, 223-224
- Kaldor, Mary, 23
- Kaufman, Irving, 17
- Keegan, John, 16
- Kelly, Bronti, 160
- Kennedy, Robert, Jr., 205
- Kerr, Philip, 83
- KGB, 20, 24-25, 34, 36-37
- King, Martin Luther, Jr., 193
- King, Rodney, 188, 194

- Lattimore, Owen. 40. 167
 Le Carré, John. 25
 Lenin, V. I.. 215
 Lewinsky, Monica. 115, 189-192
 Lexis-Nexis. 125-126
 Ley de Moore. 71
 Locke, John. 218
 Lugar de trabajo:
 comunicación por correo electrónico. efectos de la. 148-149
 descentralización de la supervisión. 145-147
 gestión empresarial «científica». 53-55, 145-146, 147-148
 lugar de trabajo panóptico. 52-55, 145-148
 teletrabajo. 147-149
 Lyon, David. 149
 Lyons, Nueva York. 105

 Maclean, Donald. 25, 39
 Maes, Pattie. 77
 Magnicidios octintados (asesinatos políticos). 31
 Manhattan. Proyecto. 16-17, 18
 Marketing:
 en los medios de comunicación. 177-179
 fragmentación de la audiencia de masas. 177-178
 hombres y mujeres en la publicidad. 180-181
 mercado gay. 181-183
 multicultural. 183-186
 Marx, Karl. 10, 48
 Mary, Alan Nunn. 18
 McCarthy, Joseph. 17, 38, 40. 167
 McDonald's. 185
 McLuhan, Marshall. 200
 Mecanismos de seguridad basados en la ocultación. 37-41
 Megachips. 71
 Metromail, empresa. 163

 México:
 zapatistas. conexión a redes te-
 leinformáticas. 203-204
 Microchips. 70-71
 Microordenadores (PC). 72
 Microsoft. 184
 Midway, batalla de. 16
 1984 (Orwell). 42, 163-164, 171-172, 173, 176, 177, 186, 193-194, 214-215
 Milosevic, Slobodan. 209, 220
 Missing, *The* (O'Hagan), 175
 Módem. 73
 Moisés. 15
 Montsanto, empresa. 98
 Mowshowitz, Abbe. 196-203, 219
 Multiculturalismo. 183-186
 Mundialización. véase Globalización planetaria
Murphy Brown (espectáculo televisivo), 191

 Nanotubos. 72
 Nazismo. 16, 23
 Netanyahu, Benjamin. 92
 NetNanny. 143-144
New York Times. 68, 71, 120, 136, 162, 164, 193-194, 212
 Nixon, Richard. 188
 North, Oliver. 134
Nosotros (*We*, Zamiatin). 42-43, 177
 Nueva York, ciudad. 104
 Nueva Zelanda. 116, 118

 Oficina de Servicios Estratégicos (OSS). 20
 O'Hagan, Andrew. 175
 Oppenheimer, J. Robert. 18, 82
 Ordenadores:
 aumento de las capacidades. 89-90, 128-131, 145-149, 203-210
 biotecnología, y. véase Biotecnología

- capacidad de transmisión, 73-74
- ciberspacio, creación de, 74-75. *Véase también* Ciberespacio
- desarrollo, 69-75
- «infobombo» *versus* realidad, 87-91
- Internet, *véase también* Internet
- microordenadores (PC), 72
- miniaturización de la tecnología, 71-72
- Organización Nacional de Mujeres (NOW), 144
- Orwell, George, 42, 163-164, 171-172, 173, 176, 177, 186, 193-194, 214-215
- Panoptic Sort, The* (Gandy), 46
- Panóptico, 10, 171-172. *Véase también* Sociedad de vigilancia
- alcance metafórico, 47-48
- aversión al riesgo, 60-61, 187. *Véase también* Aversión al riesgo
- Bentham, ideas de, 46-50, 51, 172
- burocracia y vigilancia, 57-60
- carnés de identidad y tarjetas de crédito inteligentes, 121-127, 173-174
- coerción, necesidad de la, 50-51, 171-172
- consideraciones multiculturales, 183-186
- consumo y vigilancia, 175
- descripción del, 46-47
- Estado panóptico, 55-60
- huir de la mirada panóptica, 59
- lugar de trabajo o fábrica panóptica, 52-55, 145-148
- marketing, *véase* Marketing
- metáfora de Disney World, 175-177
- paralelismos religiosos, 49, 50-51
- participación y consenso, 172-175
- planetario, *véase* Globalización planetaria
- sociedad disciplinaria y panopticismo, 51-52
- transparencia del, 214-215
- vigilancia videográfica, *véase* Vigilancia videográfica
- Partenia, obispo de, 208
- Pasaportes, 127
- PGP, software de encriptación, 137
- Philby, Kim, 25, 26, 39
- Plataforma para la Selección del Contenido de Internet (PICS), 143-144
- Pontecorvo, Bruno, 18
- Pornografía y censura, 140-145
- Powers, Francis Gary, 27
- Prensa impresa, 128
- Pruebas nucleares, detección de, 27-28
- Quayle, Dan, 191
- Quittner, Joshua, 164
- Red, la, *véase* Internet
- Reforma protestante, 128
- Regan, Priscilla, 165
- Religión:
 - Dios y la vigilancia, 49, 50-51
 - Moisés y el espionaje, 15-16
- Resistencia, redes teleinformáticas de, 209, 216
 - Acuerdo Multilateral en Inversiones (MAI), campaña contra, 206-207
- indios cree de James Bay, 204-206
- páginas *web* del obispo Gaillot, 208
- propaganda de extrema derecha, 209-210
- zapatistas, 203-204

- Revolución de la información. 64-65. Véase también Ordenadores y ciberespacio
 bombo *versus* realidad. 87-91
 digitalización. impacto de la. 67-69
 historia de la. 69-75
 metáfora de la biblioteca de Babel. 65-66, 69
- Rise of the Network Society, The* (Castells), 96
- Robocop* (película), 84
- Robots. 82-83
- Rosenberg, Julius y Ethel. 17, 29-30
- Rousseau, Jacques. 193
- Satélites. 19, 27-29, 74
 agricultura con. 110-111
 EarlyBird. 111
 «etiquetas» de localización. 111
 interceptación de las telecomunicaciones. 115-121
 Sistema de Posicionamiento Global (GPS). 110
 usos comerciales de los satélites de espionaje. 110-112
- Schwartzau, Winn. 93
- Schwarzenegger, Arnold. 84
- Segunda Guerra Mundial. 16, 23, 69, 135
- Seguridad social. números de la. 125-126
- Seinfeld* (espectáculo televisivo). 179
- Serbia. 209
- Servicios de inteligencia:
 académico y espía. afinidades entre. 20-22
 automatización de los. 26-30
 bases de datos *versus* informes de los. 151-154
 breve historia del espionaje. 15-16, 22-26
 círculo vicioso. 18-20
 conocimiento *versus* información. 19-20
 desinformación. 22-26
 Estado liberal y los. 37-41
 Estado totalitario y los. 41-44
 Guerra Fría. 17, 22-30, 33, 38, 41, 116
humint versus techint. 30
 inteligencia artificial. software. 30
 intervenciones encubiertas en el extranjero. 31
 satélites. 19, 27-29
 vigilancia político-policial internacional. 30-32
 vigilancia político-policial nacional. 32-37
- Shafer, Jack. 189-190
- Shearing, Clifford. 175
- Sindicatos. 53, 209
- Singapur. 210-211
- Sistemas de retransmisión en correo electrónico (*re-mailing*). 134
- Sistemas de visualización con rayos X. 108
- Smith, Adam. 52, 54
- Sociedad de vigilancia. 43-44. Véase también Panóptico
 carnés de identidad inteligentes. 121-127, 173-174
 encriptación. controversia de la. véase Criptografía
 Internet, dilemas de. 129-130
 intimidad, muerte de la. 163-167
 satélites. véase Satélites
 tecnología de escucha clandestina. véase Tecnología de escucha clandestina
 vigilancia de datos. 154-160
 vigilancia del correo electrónico. 132-134
 vigilancia multidireccional. 187-194

- vigilancia videográfica, *véase*
- Vigilancia videográfica
- Sociedad disciplinaria, 51-52
- Sociedad red, 96-100
- Software inteligente, 29, 76-78
- Sony, 137
- Stalin, Joseph, 33, 41, 42
- Starr, Kenneth, 114-115
- Stasi, 33, 35
- Stenning, Philip, 175
- Sunday Times* (Londres), 112
- Tarjetas de crédito, 121-127, 173-175
- Taylor, Charles, 186
- Taylor, Frederick Winslow, 53-54, 145, 148, 171
- Tecnología de escucha clandestina, 114-115
 - interceptación de la telecomunicaciones, 116-121
 - intervención telefónica, 114-116
 - láser y digitalización, 115
 - tecnología TEMPEST, 119
 - teléfonos móviles, 119-121
 - transmisión por fibra óptica (interceptación), 119
- Tecnología de fotocopia estroboscópica, 108
- Tecnología de reconocimiento facial, 106-107
- Tecnología de visión nocturna, 108-109
- Tecnología del «destello» (*flash*), 71-72
- «Tecnioniéras» (*nannycam*), 101-102
- Teletrabajo, 147-149
- TEMPEST, tecnología, 119
- Terminator* (película), 84
- Terrorismo, 38-39, 223-224
- Time*, 164
- Trabajo policial, 146-147, 160
- Transistores de cuantos, 71
- Transistores, 70-71
- Transmisión, capacidades de, 73-74
- Tripp, Linda, 115
- Trotsky, León, 215
- Turing, Alan, 20, 69
- U-2, avión de espionaje, 27
- UKUSA, red, 116, 118, 133
- Unión Soviética, 17, 18, 19, 20, 41, 97, 214
 - avión comercial KAL-007, derribo del, 27
 - KGB, 20, 24-25, 34, 36-37
 - revolución bolchevique, 34-35
- Viajes, información sobre, 126-127
- Vigilancia multidireccional, 187-194
- Vigilancia relacionada con el ámbito de la salud, 59-60
- Vigilancia videográfica
 - amenazas a la intimidad y sus implicaciones, 109-110, 174-175
 - ciberinsectos, 113
 - Nueva York y otras ciudades, 103-105
 - tecnología de Búsqueda Infrarroja (FLIR), 108
 - tecnología de fotocopia estroboscópica, 108
 - tecnología de reconocimiento facial, 106-107
 - tecnología de visión nocturna, 108-109
 - tecnología de visualización por satélite, *véase* Satélites
 - tecnología para detectar objetos «escondidos», 107-108
 - tecnioniéra (*nannycam*), 101-102
 - vigilancia urbana en las calles, 104-106

Vuelos internacionales, 126-127

Warhol, Andy, 193

Weber, Max, 58, 59

«Winter Market, The» (Gibson),
85-86

Woodward, Louise, 101-115

World Trade Center, explosión de
una bomba en el, 224

Zamiatin, Eugene, 42-43, 177

Zapatistas, 203-204

Reg Whitaker

El fin de la privacidad

La revolución de la información y el auge de la sociedad informatizada están reconstruyendo actualmente las estructuras del poder a escala global. A veces, por ejemplo, el correo electrónico no es tan privado como parece. Los empresarios pueden controlar cada uno de los movimientos de sus trabajadores a lo largo de toda la jornada. Los ministerios de Hacienda conocen todos los detalles de la economía personal y profesional de los ciudadanos. Códigos de barras y tarjetas de crédito, domiciliaciones y otros datos bancarios, incluso «tarjetas inteligentes» que transmiten el historial médico y criminal y métodos de seguridad capaces de leer el ADN, son sólo una pequeña muestra de esa gran cantidad de información privada que ya se mueve en los ámbitos corporativos. Datos que, a su vez, pueden ser combinados y utilizados para confeccionar perfiles individuales o de grupo potencialmente mucho más detallados que los informes que pudieran elaborarse en el pasado las policías estatales y las agencias de seguridad. Los penalistas del siglo XIX teorizaron una cárcel ideal denominada Panóptico, un sistema de vigilancia completo y total. Pues bien, el libro que el lector tiene entre sus manos es el análisis más minucioso realizado hasta el momento sobre hasta qué punto vivimos cada vez más en un Panóptico virtual.

Reg Whitaker es profesor de Ciencias Políticas en la York University de Toronto. Es autor, junto a Gary Marcuse, de *Cold War Canada: The Making of National Insecurity* y ha publicado numerosos artículos sobre política, seguridad, servicios de inteligencia y el poder de la información en el mundo contemporáneo.

ISBN 84-493-0772-4



9 788449 307720



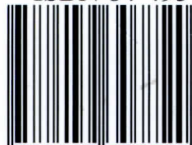
Reg Whitaker

El fin de la privacidad

La revolución de la información y el auge de la sociedad informatizada están reconstruyendo actualmente las estructuras del poder a escala global. A veces, por ejemplo, el correo electrónico no es tan privado como parece. Los empresarios pueden controlar cada uno de los movimientos de sus trabajadores a lo largo de toda la jornada. Los ministerios de Hacienda conocen todos los detalles de la economía personal y profesional de los ciudadanos. Códigos de barras y tarjetas de crédito, domiciliaciones y otros datos bancarios, incluso «tarjetas inteligentes» que transmiten el historial médico y criminal y métodos de seguridad capaces de leer el ADN, son sólo una pequeña muestra de esa gran cantidad de información privada que ya se mueve en los ámbitos corporativos. Datos que, a su vez, pueden ser combinados y utilizados para confeccionar perfiles individuales o de grupo potencialmente mucho más detallados que los informes que pudieran elaborar en el pasado las policías estatales y las agencias de seguridad. Los penalistas del siglo XIX teorizaron una cárcel ideal denominada Panóptico, un sistema de vigilancia completo y total. Pues bien, el libro que el lector tiene entre sus manos es el análisis más minucioso realizado hasta el momento sobre hasta qué punto vivimos cada vez más en un Panóptico virtual.

Reg Whitaker es profesor de Ciencias Políticas en la York University de Toronto. Es autor, junto a Gary Marcuse, de *Cold War Canada: The Making of National Insecurity* y ha publicado numerosos artículos sobre política, seguridad, servicios de inteligencia y el poder de la información en el mundo contemporáneo.

ISBN 84-493-0772-4



9 788449 307720

