MONOGRAFÍA DE INTERNET
INTERNET MONOGRAPH

La política de internet. Privacidad y libertad en el ciberespacio

The policy of internet. Privacy and freedom in the cyberspace

DEMANDADO 14-7-2021 **REVISADO** 29-7-2021 **ACEPTADO** 3-8-2021

Manuel Castells

Profesor senior de la Universitat Obertade Catalunya, exprofesor de la University of Berkeley, Estados Unidos

Palabras claves: Internet, política, ciberespacio, libertad

Key Words: Internet, politics, cyber-space, freedom

RESUMEN Creado como un medio para la libertad, en los primeros años de su existencia global, internet parecía presagiar una nueva era de liberación. Los gobiernos podían hacer muy poco para controlar unos flujos de comunicación capaces de trascender la geografía y, por tanto, las fronteras políticas. La libertad de expresión podía extenderse por todo el planeta sin depender de los medios de comunicación de masas, ya que internet permitía la comunicación de muchos a muchos sin trabas. La propiedad intelectual (de la música, las publicaciones, las ideas, la tecnología y el software) debía compartirse necesariamente ya que, en cuanto estas creaciones salían a la red, no había manera de limitarlas. La privacidad estaba protegida por el anonimato de la comunicación en internet, así como por la dificultad de rastrear las fuentes e identificar el contenido de los mensajes transmitidos por medio de los protocolos de internet.

ABSTRACT Created as a means for freedom, in the first years of its global existence, Internet seemed to presage a new era of liberation. Governments couldn't do much to control the communication

flows capable of transcending geography, and as a result, the political frontiers. The freedom of expression could be extended around the world, without depending of the mass mediums of communication, since internet allowed communicating from many places to others without any difficulty. The intellectual property (of music, publications, ideas, technology and software) had to be shared necessarily because, the moment the creations came out in the web, and there was no way to limit them. Privacy was protected from the anonymity of communication on the internet, and the difficulty to find the origins and identify the content of the messages transmitted through the protocols of Internet too.

Privacidad y libertad en el ciberespacio

Este paradigma de la libertad estaba basado en fundamentos tecnológicos e institucionales. Tecnológicamente, su arquitectura basada en la conexión informática en red sin restricciones, sobre protocolos que interpretan la censura como un fallo técnico y simplemente la sortean dentro de la red global, hacen que sea bastante difícil -por no decir imposible- controlarla. No es que esta sea la "naturaleza" de internet: es que internet es así, debido al diseño intencional de sus creadores originales.

Institucionalmente, el hecho de que internet se desarrollara inicialmente en Estados Unidos, implica que quedaba situada bajo el amparo de la protección constitucional de la libertad de expresión [?], amparada por los tribunales estadounidenses. Como el eje troncal de internet global estaba centrado principalmente en Estados Unidos, cualquier restricción impuesta a servidores de otros países podía en principio evitarse reenrutándose a través de un servidor estadounidense.

Sin duda, las autoridades de un determinado país podrían detectar a los recipientes de determinada clase de mensajes, poniendo en práctica su capacidad de vigilancia y allí castigar a los infractores de acuerdo con sus leyes, algo que 105 disidentes chinos han experimentado a menudo en sus propias vidas. Pero este proceso de vigilancia/castigo era demasiado costoso para poder imponerse a gran escala y, en cualquier caso, no servía para detener la comunicación por internet, sino únicamente para penalizarla. La única manera de controlar internet era permanecer al margen de la red aunque pronto se vio que, para todos los países del mundo, este era un precio demasiado alto, tanto en términos de oportunidades

de negocio como de acceso a la información global. En este sentido, internet contribuyó de manera decisiva a socavar la soberanía nacional y el control del estado. Pero eso sólo fue posible gracias a la protección judicial que recibía en el núcleo de su eje troncal global, o sea, Estados Unidos. En realidad, por mucho que hablaran de Internet y la libertad, la realidad es que el Congreso de Estados Unidos y la administración Clinton trataron de armarse de instrumentos legales de control sobre la red. Después de todo, el control de la información ha constituido siempre la base de poder del estado a lo largo de la historia, y Estados Unidos no es una excepción a esta regla. Esta es la razón por la que uno de los valore, ejemplares de la Constitución estadounidense es, precisamente, haber situado el derecho a la libre expresión como primera enmienda a la Constitución. En su intento de ejercer control sobre internet, el Congreso y el Departamento de Justicia de Estados Unidos utilizaron un argumento que nos conmueve a todos: proteger a los niños de los perversos sexuales que circulan por internet. Pero no sirvió de nada. El 12 de junio de 1996, un tribunal federal de Pensilvania declaró inconstitucional la "Ley de decencia en las comunicaciones" ("Communications decency act") declarando que: "Igual que podemos afirmar que la fuerza de Internet reside en el caos, el valor de nuestra libertad depende del caos y la diversidad de la expresión sin trabas defendida por la Primera Enmienda" (cfr. Lewis. 1996). El Tribunal supremo sostuvo este "derecho constitucional al caos" el 26 de junio de 1997. En junio de 2000, la Corte de apelación de Estados Unidos en Filadelfia derogo la "Ley para la protección del menor on line" ("Child on line protection act") de 1998. Así, dadas las dificultades para que en Estados Unidos se imponga la regulación gubernamental de la comunicación informática, debido a la naturaleza global de la red, parece que el intento directo por parte del estado de controlar internet mediante los medios tradicionales de censura y represión ha fracasado.

Sin embargo, estos dos pilares (tecnológico e institucional) de la libertad en internet podrían ser cuestionados, y de hecho lo están siendo, por nuevas tecnologías y nuevas regulaciones (Lessig. 1999: Samuelson, 2000). Aplicaciones de software pueden configurarse sobre internet, permitiendo la identificación de rutas de comunicación y contenidos. Mediante el uso de estas tecnologías, se puede transgredir la privacidad y, en cuanto se llega a relacionar a determinados individuos con procesos de comunicación específi-

cos en contextos institucionales concretos, es posible utilizar todas las formas tradicionales de control político y organizativo contra el individuo conectado en red. Este es el poderoso y convincente argumento esgrimido por Lawrence Lessig en su influyente obra sobre esta materia (Lessig, 1999). Aunque mis puntos de vista divergen un tanto de su interpretación (y aún más de su postura normativa), la tesis de Lessig debe tomarse como punto de partida de cualquier análisis en esta materia. La transformación de la libertad y la privacidad en internet es consecuencia directa de su comercialización. La necesidad de asegurar e identificar la comunicación en internet para poder ganar dinero gracias a la red y la necesidad de proteger los derechos de propiedad intelectual en la misma, han derivado en el desarrollo de nuevas arquitecturas de software (lo que Lessig denomina, el "código") que posibilitan el control de la comunicación informática. Los gobiernos de todo el mundo apoyan estas tecnologías de vigilancia y se afanan en adoptarlas, para conseguir recuperar parte del poder que corrían el riesgo de perder (Lyon, 2001a, 2001b). Sin embargo, hay una serie de nuevas tecnologías de la libertad que se oponen a dichas tecnologías de control. Así la sociedad civil se lanza a las barricadas de las nuevas batallas por la libertad y los tribunales de justicia ofrecen un cierto grado de protección contra los abusos más descarados, por lo menos en algunos contextos (aunque no en el lugar de trabajo). Internet ha dejado de ser un espacio libre, pero tampoco se ha cumplido la profecía orwelliana. Es un terreno controvertido en el que se está disputando la nueva y fundamental batalla a favor de la libertad en la era de la información.

Tecnologías de control

De los intereses compartidos por el comercio y los gobiernos ha surgido una variedad de tecnologías de control. Existen las tecnologías de control, las de vigilancia y las de investigación. Todas se basan en dos supuestos básicos: el conocimiento asimétrico de los códigos en la red y la capacidad para definir un espacio de comunicación específico, susceptible de ser controlado. Vamos a repasar sucintamente estas cuestiones como primer paso para analizar los procesos de restricción de la libertad que tienen lugar en internet.

Las tecnologías de la identificación incluyen el uso de contraseñas, cookies y procesos de autentificación. Las cookies son marcadores digitales que los sitios web colocan automáticamente en los discos duros de los ordenadores que se conectan a ellos. Una vez se ha

insertado la cookie en un ordenador, todos los movimientos on line realizados desde dicho ordenador son grabados automáticamente por el servidor del sitio web que la colocó. Los procesos de autentificación utilizan firmas digitales que permiten a otros ordenadores verificar el origen y las características de la persona que se conecta. A menudo se basan en la tecnología de encriptación. La autentificación generalmente funciona en niveles, ya que los usuarios individuales son identificados por servidores que a su vez están siendo identificados por redes. Uno de los primeros ejemplos de protocolos de seguridad en Internet fue la "Capa de conexión segura" (SSL: "Secure socket layer"), introducida por Netscape. Algunos consorcios de compañías emisoras de tarjetas de crédito y empresas de comercio electrónico han adoptado otros protocolos estándares de seguridad.

Las tecnologías de vigilancia son diferentes pero a menudo se basan en las tecnologías de identificación para poder localizar al usuario individual. Las tecnologías de vigilancia interceptan mensajes y colocan marcadores que permiten rastrear los títulos de comunicación desde un determinado ordenador y controlar la actividad de la máquina día y noche. Pueden identificar un servidor determinado en el origen de un mensaje. Entonces, mediante la persuasión o la coacción, los gobiernos, las empresas o los tribunales pueden obtener del proveedor de servicios internet la identidad del potencial sospechoso utilizando sus tecnologías de identificación o simplemente buscándola en sus listados cuando poseen dicha información (ya que a través de las direcciones electrónicas se suelen obtener las direcciones reales de los clientes de casi todos los proveedores de servicios Internet).

Las tecnologías de investigación atañen a la elaboración de bases de datos mediante los resultados de la vigilancia y la acumulación de información grabada asiduamente (Garfinkel, 2000). Una vez recogidos los datos en formato digital, todas las piezas de información contenidas en la base de datos pueden ser agregadas, desagregadas, combinadas e identificadas según el objetivo y la capacidad legal. A veces, se trata tan sólo de elaborar un perfil agregado, como en la investigación de mercado, tanto para el comercio como para la política. En otros casos se trata de un objetivo individualizado ya que en ocasiones se puede caracterizar a una persona determinada mediante un amplio corpus de información contenida

en sus archivos electrónicos, desde pagos con tarjeta de crédito hasta visitas a sitios web, correo electrónico y llamadas de teléfono. En el entorno tecnológico actual, cualquier información transmitida electrónicamente puede ser procesada, identificada y combinada, dentro de una unidad de análisis que puede ser colectiva o individual.

La encriptación es la tecnología fundamental que protege la privacidad del mensaje (aunque no la del mensajero, ya que el ordenador de origen puede ser identificado a través del punto de entrada en la red electrónica) (Levy, 2001). Esto es especialmente cierto en el caso de la "Encriptación de clave pública" ("Public key encryption" –PKI-), que contiene dos claves de descodificación, una de las cuales es privada. De todos modos, como indica Lessig, la encriptación es una tecnología ambigua, ya que por un lado respeta la confidencialidad, pero por otro, constituye la base de las tecnologías de identificación avanzadas. Permite el desarrollo de las firmas digitales certificadas que, una vez generalizada su demanda, acabarán con el anonimato en internet, ya que cada perro tendrá que registrarse como tal perro, para tener acceso al mundo canino o si no, acabará viviendo con los gatos de su ciberbarrio.

Estas tecnologías gestionan el control de acuerdo a dos condiciones básicas. Primero, los controladores conocen los códigos de la red mientras que los controlados los desconocen. El software es confidencial y propietario y únicamente puede ser modificado por su dueño. Una vez en la red, el usuario medio se encuentra prisionero en una arquitectura que le es ajena. Por otro lado, los controles se ejercen sobre la base de un espacio definido en la red. Por ejemplo, en la red construida en torno a un determinado proveedor de servicios internet o la intranet de una empresa, una universidad o una agencia gubernamental. En efecto, internet es una red global, pero los puntos de acceso a la misma no lo son. Si se ponen filtros en este acceso, el precio de la libertad global acabará siendo la sumisión local. Pasemos ahora a observar estas tecnologías de control en acción.

El fin de la privacidad

La libertad que comporta internet ha despertado tanto entusiasmo que a menudo hemos olvidado la persistencia de las prácticas autoritarias de vigilancia en un entorno que sigue siendo el más importante de nuestras vidas: el lugar de trabajo. Como los trabaja-

dores dependen cada vez más del trabajo informático en red en su actividad, la mayor parte de las empresas se han arrogado el derecho de controlar el uso de sus redes por parte de los empleados. En Estados Unidos, un estudio hecho público en abril de 2000, indicó que el 73,5 % de las empresas estadounidenses lleva a cabo regularmente alguna clase de vigilancia del uso de internet por parte de sus empleados. Ha habido incontables casos de trabajadores despedidos por un supuesto uso inapropiado de la red (Howe, 2000: 16). Programas tales como Gatekeeper, muestran al servidor toda la actividad internet que está teniendo lugar en cualquier organización suscrita a dicho servidor. El control del trabajador por parte de la dirección en el taller de la fábrica constituyó una fuente habitual de conflictos durante la era industrial. Pero parece que la era internet no hará más que exacerbar esta tensión. que se volverá cada vez más persistente, debido a su omnipresencia automatizada.

Más allá de las paredes de cristal del mundo empresarial, hay gente que proclama, como hace Scott McNealy (el carismático consejero delegado de Sun Microsystems) que: "Ya no le queda a usted ni un ápice de privacidad: vaya acostumbrándose" (cfr. Scheer, 2000: 100.) Aquí el cambio fundamental ha residido en las tecnologías de recolección de datos asociadas a la economía del comercio electrónico. En muchos casos, la fuente principal de ingresos de las empresas de comercio electrónico es la publicidad y el marketing. Por otro lado, estas obtienen ingresos de las pancartas (banners) publicitarias que cuelgan para sus usuarios. Además, venden los datos personales de sus usuarios a sus clientes con fines comerciales o los utilizan ellos mismos para definirlos mejor. En todos los casos, se consigue siempre una valiosísima información de cada clic efectuado dentro del sitio web. En Estados Unidos, el 92 %, de los sitios web recogen los datos personales de sus usuarios y los procesan de acuerdo a sus intereses comerciales (Lessig, 1999: 153). Las empresas juran que sólo utilizan los datos de forma agregada para elaborar perfiles de mercado. Después de todo, la mayoría de los consumidores no ejerce su derecho de opt-out, que les permitiría negarse a autorizar el uso de sus datos personales. De hecho, los defensores del consumidor han demostrado lo incómodo que es ejercer el derecho a la cláusula opt-out, por lo que proponen una opción opt-in, que constituye una decisión afirmativa

de aceptación[1]. En cualquier caso, el Congreso de Estados Unidos, bajo fuertes presiones por parte de los anunciadores y el sector del comercio electrónico, rechazó la obligatoriedad de incluir la opción opt-out en la actividad comercial. En la Unión Europea, la mayor presión gubernamental a favor de la protección del consumidor derivó en una ley de la privacidad, bajo la cual las empresas no están autorizadas a utilizar los datos personales de sus clientes sin su aprobación explícita. Entonces el problema estriba en el intercambio de datos a cambio del privilegio de acceder a los sitios web. La mayor parte de la gente renuncia a su derecho a la privacidad para poder navegar por los distintos sitios comerciales de Internet. Una vez se ha renunciado a este derecho de protección de la intimidad, los datos personales se convierten en propiedad legal de las empresas internet y de sus clientes.

Para ilustrar este proceso, veamos el caso de Double click, la mayor empresa de colocación de publicidad en internet. Su trabajo consiste en colocar archivos cookie por millones en todos los ordenadores que se conectan a los sitios web, equipados con tecnología Double click. En cuanto la cookie se introduce en un ordenador, este comenzará a recibir determinados anuncios en cualquier visita que efectúe a los miles de sitios web que emplean los servicios de Double click. Como tantas otras empresas internet, Double click a menudo prueba hasta dónde puede llegar en la reducción de la privacidad de las personas. Así, en noviembre que de 1999, Double click compró Abacus, una base de datos de nombres, direcciones e información sobre los hábitos de compra de 90 millones de hogares en Estados Unidos. Con la ayuda de esta base de datos, Double click creó perfiles que relacionaban los nombres y direcciones verdaderas de las personas con sus compras on line y off lineo Las protestas de los defensores de la privacidad obligaron a Double click a interrumpir dicha actividad hasta que se pudiera llegar a un acuerdo entre el gobierno y el sector sobre los estándares que debían tenerse en cuenta para abordar las cuestiones relacionadas con la privacidad (Rosen, 2000a).

Como indica Rosen (2000b), las tecnologías que hacen posible bajarse libros, revistas, música y películas en formato digital al disco

[1] El usuario emplea la opción opt-in para recibir únicamente la clase de comunicaciones cuya recepción haya sido previamente autorizada por él o ella misma.

duro de un ordenador, permiten a los editores y las empresas de ocio registrar y controlar los hábitos de navegación de las personas para poder enviar publicidad específica a cada uno de sus clientes. El mayor conglomerado empresarial de comunicación electrónica del mundo, AOL-Time warner es un ejemplo que ha de considerarse. La caja multimedia integrada del futuro (que con tanto empeño ansían Microsoft y ATT) probablemente tenga una capacidad de vigilancia considerable. Los Identificadores Globalmente únicos (GUID: Globally unique identifiers) permiten ligar cada documento, mensaje de correo electrónico o chat colgado en la red con la verdadera identidad de la persona que lo hizo. En noviembre de 1999, unos defensores de la privacidad se enfrentaron a Real jukebox cuando se percataron de que el reproductor de música podía enviar información a la casa madre, RealNetworks, sobre la música que se bajaba cada usuario, y que esa información podía relacionarse con un número de identificación único que apuntaba a la identidad del usuario. Por temor a la mala publicidad que este hecho podía generar en su contra. RealNetworks desmontó el GUID. Recuerden, no obstante, que la identificación digital constituye la norma más que la excepción en este sector: los productos de software de Microsoft, como el Word 97 y el Powerpoint 97 incluyen identificadores en cada uno de los documentos que producimos con ayuda de dichos programas. La identidad de estos programas puede rastrearse hasta el ordenador que los originó.

La privacidad en el ámbito del e-mail no es objeto de una adecuada protección legal. Según Rosen:

> En una decisión legal totalmente circular, el Tribunal supremo ha dictaminado que las protecciones constitucionales contra las búsquedas no justificadas dependen de si los ciudadanos tienen unas expectativas subjetivas de privacidad que la sociedad está preparada para aceptar como razonables... Más recientemente, los tribunales han dictaminado que, adoptando simplemente una norma escrita que advierte a los empleados de que su correo electrónico puede estar controlado, los empresarios conseguirán rebajar las expectativas de intimidad de sus empleados hasta el punto en que podrán controlar toda la información que quieran (Rosen, 2000a: 51).

Las oportunidades de negocio son ilimitadas en este nuevo sector dedicado a comerciar con el comportamiento privado. En las elecciones del año 2000 en Estados Unidos, una empresa creó una base de datos denominada Aristotle, que, mediante datos obtenidos de diversas fuentes, proporcionaba un perfil político de unos

150 millones de ciudadanos, para vender estos perfiles al mejor postor, que generalmente eran las oficinas electorales de los candidatos políticos.

Utilizando los avances tecnológicos de las empresas comerciales de internet los gobiernos han conseguido incrementar sus propios programas de vigilancia, combinando los rudos métodos tradicionales con la nueva sofisticación técnica. En el ámbito internacional, el programa Echelon, creado por Estados Unidos y el Reino Unido durante la guerra fría, parece haberse adaptado al espionaje industrial, según las agencias gubernamentales francesas, a base de combinar las tradicionales escuchas e interferencias en las telecomunicaciones con la interceptación de mensajes electrónicos. El programa Carnivore del FBI trabaja en colaboración (voluntaria o no) con proveedores de servicios internet, registrando todo el tráfico de e-mails, distribuyendo posteriormente la información deseada sobre la base de un muestreo y procesamiento de claves automatizado. En el año 2000, el FBI pidió 75 millones de dólares al Congreso para financiar programas de vigilancia como la "Tormenta digital" ("Digital storm"), una nueva versión de la grabación de conversaciones telefónicas, combinada con programas informatizados para buscar palabras claves en los mensajes.

Es posible vislumbrar la potencial aparición de un sistema de vigilancia electrónico en el horizonte histórico. La ironía reside en que fueron, en general, las empresas internet, vehementes libertarias en lo ideológico[2], quienes proporcionaron la tecnología necesaria para romper el anonimato y limitar la intimidad y que además fueron las primeras en utilizarla. Al hacerlo, permitieron que la vigilancia gubernamental penetrara el espacio de libertad que los pioneros de internet habían conseguido ganar, aprovechándose de la ignorante indiferencia de las burocracias tradicionales.

De todos modos, la historia es contradictoria y la contraofensiva de los amantes de la libertad está ya en marcha. Pero antes de tomar en consideración esta tendencia alternativa, debemos examinar las consecuencias del deterioro de la privacidad en las otras dimensiones que, unidas, constituyeron el ámbito de la libertad en internet.

[2] Grupos en los que se infiltran miembros o partidarios de la administración norteamericana y del poder global (N. del E).

Soberanía, libertad y propiedad cuando la privacidad desaparece

En el año 2000, los gobiernos de todo el mundo se tomaron en serio la amenaza de lo que ellos mismos denominaron "cibercrimen". Para entonces estaba claro que la infraestructura de comunicaciones informáticas de la que dependían la riqueza, la información y el poder en nuestro mundo era muy vulnerable a la intrusión, la interferencia y a los trastornos. Internet está surcada por implacables oleadas de virus y gusanos; los crackers atraviesan los cortafuegos y roban números de tarjetas de crédito, los activistas políticos ocupan los sitios web, los archivos de algunos ordenadores militares circulan por todo el mundo e incluso se ha conseguido extraer software confidencial de la propia red interna de Microsoft. A pesar de los miles de millones de dólares invertidos en seguridad electrónica, está claro que la seguridad global de una red es tan buena como la seguridad particular de su componente más débil. Si se consigue entrar en una red por cualquiera de sus puntos, resulta bastante factible circular por sus diversos nodos sin demasiada dificultad.

De hecho el daño real producido, tanto en las agresiones a la persona como a la propiedad, ha sido muy limitado y se ha exagerado bastante en general. En cualquier caso, no es nada comparable a la pérdida de vidas humanas, la degradación del medio ambiente y las pérdidas económicas infligidas por los desaguisados de la industria automovilística, por ejemplo (¿se acuerdan de los neumáticos de Firestone/Ford?) o de la industria química (por favor, no olviden Bhopal). Y sin embargo, la sola idea de que las redes informáticas puedan ser inseguras, resulta insoportable para los poderes fácticos de nuestro mundo: todo depende de estas redes y el control de dichas redes es un principio esencial para conseguir mantener la dominación [!].

Pero había algo más. El hacking y el cracking, dirigidos a cualquier punto de la red global y desde cualquier extremo de la misma, sirvieron para dejar constancia de la impotencia de las formas tradicionales de control policial, basadas en los poderes del estado dentro de sus fronteras nacionales. Estos hechos exacerbaron aún más la ansiedad de los gobiernos de todo el mundo por su incapacidad para detener los flujos de comunicación que habían prohibido dentro de sus fronteras, sean los mensajes de "Falun gong" en China, las memorias del médico de Mitterrand en Francia o la su-

basta en la red de papeletas válidas de votantes ausentes en Estados Unidos (posteriormente este sitio web se trasladó a Alemania). La soberanía del estado siempre había comenzado con el control de la información y dicho control se estaba comenzando a erosionar lenta pero irremisiblemente. Debido al carácter global de internet, fue necesario llevar a cabo un esfuerzo concertado de los gobiernos más importantes para actuar conjuntamente y crear un espacio nuevo y global de acción policial. De hecho, al hacer esto perdieron soberanía, ya que se vieron obligados a compartir el poder y ponerse de acuerdo en unos estándares comunes de reglamentación, de manera que ellos mismos se convirtieron en una red, una red de agencias de reglamentación y control policial. Pero la soberanía compartida fue el precio que hubo de pagarse para retener, de modo colectivo, algún grado de control político. Así, utilizando tanto medios legítimos como ilegítimos, el estado contraatacó. La reunión del G-8 en París en junio de 2000 fue la punta de lanza de dicha acción y el Consejo de Europa se hizo eco de esta preocupación organizando una "Convención contra el cibercrimen", cuyo borrador redactaron las agencias de seguridad de los países europeos, con el asesoramiento de las empresas globales de software, el intento más completo y de mayor alcance hasta ese momento, de control de las comunicaciones en la red. Muchos países del mundo, como Rusia. China. Malasia, Singapur y otros países, aplaudieron esta nueva y determinada actitud por parte de varios grandes gobiernos para controlar a internet. Actitud que interpretaron, con razón, como una confirmación de su anterior desconfianza. Las disposiciones de todas estas políticas concertadas son a la vez demasiado vagas y demasiado técnicas para que podamos entrar en ellas pormenorizadamente. Además, pronto quedarán técnicamente obsoletas, por lo que tendrán que ser actualizadas constantemente. Lo que de verdad cuenta es el empeño y la metodología de la intervención. En pocas palabras, lo que pretenden es neutralizar el poder de encriptación que está en manos de los ciudadanos a base de restringir o prohibir su tecnología. Prohíben, por ejemplo, las tecnologías de seguridad personal. Amplían de manera considerable el poder del gobierno para intervenir teléfonos e interceptar el tráfico de datos. Por otra parte, establecen la obligatoriedad para los proveedores de servicios internet de instalar técnicas de rastreo de los usuarios, así como la notificación obligatoria de la identidad de los usuarios a petición de las agencias gubernamentales, dentro de un espectro de situa-

ciones y circunstancias muy amplio y vagamente definido. Tengan en cuenta que, en general, todo esto se resume en una limitación del grado de privacidad en la comunicación por internet -con lo que internet pasaría de ser un espacio de libertad a convertirse en una casa de cristal--. La comunicación seguirá fluyendo sin trabas, porque la arquitectura de internet lo permite. Pero la redefinición del espacio de acceso, a través del control sobre los proveedores de servicios internet y el establecimiento de protocolos especiales de vigilancia ejecutables en internet para determinadas redes, permite que el control (y el castigo) pueda aplicarse a posteriori. Lessig tiene razón. La nueva arquitectura de internet el nuevo código, se convierte en el instrumento principal de control, permitiendo el ejercicio de la regulación y el control policial por parte de los medios tradicionales de aplicación del poder estatal.

La primera víctima de esta reconquista del ciberespacio es la propia soberanía. Para ejercer la regulación global, los estados tienen que fusionarse y compartir su poder. Pero no de acuerdo al viejo sueño del gobierno mundial absoluto, sino en forma de un estado red, la criatura política engendrada por la era de la información (Carnoy y Castells, 2002). La segunda víctima es la libertad, o sea, el derecho de ejercer nuestro libre albedrío. ¿Por qué? ¿Por qué se traduce la amenaza contra la privacidad en una potencial limitación de la libertad? En parte, por culpa del mecanismo utilizado para imponer la soberanía en un contexto global. Para que los estados puedan funcionar como aliados en esta red de control, deben ponerse de acuerdo en unos estándares, establecidos según el mínimo común denominador. Si un gobierno determinado tiene que cooperar para imponer el control sobre los sitios web de pornografía infantil situados en su territorio, lo hará únicamente a condición de tener acceso a los datos obtenidos interceptando el trafico entre su país y los países que están fuera de su alcance, si no ¿por qué iba a acceder a cooperar? El concepto mismo de la colaboración policial internacional está basado en compartir los esfuerzos asociados a la obtención de información. Otra cuestión es la capacidad de un estado concreto para actuar contra una determinada actuación que se esté produciendo en una jurisdicción ajena -en este caso las antiguas formas de poder basadas en la territorialidad, limitarían dicha injerencia- obstante, compartir el acceso global a las redes de información es un medio contundente de imponer el poder estatal colectivo a los ciudadanos en cual-

quier lugar, ya que las consecuencias derivadas de la información obtenida orientarán la represión en contextos específicos. Si bien el nivel de represión variará según el grado de libertad de cada país, la base informativa de la represión se ajustará a los estándares de sospecha razonable compartidos por todos los gobiernos que participen en la red de vigilancia policial. Por ejemplo, el consumo legal de metadona o marihuana practicado en Holanda por un ciudadano estadounidense puede ser expuesto o incluso castigado (mediante leyes o normas) en Estados Unidos, como consecuencia de la vigilancia conjunta de la distribución de drogas. En este sentido, como el hecho de ser gay o lesbiana constituye un delito punible por ley en algunos países, como Malasia y Arabia Saudí por ejemplo, la vigilancia conjunta de chat rooms sobre preferencias sexuales (con el pretexto en la búsqueda de pornografía infantil), si se revelase la identidad real de los ciudadanos de estos países, puede derivar en graves consecuencias para estas personas, a pesar de la tolerancia legal respecto a su orientación sexual en otros países.

Es más, la vigilancia global limita la libertad de expresión, quizá en un grado menor en países como Estados Unidos, que cuentan con una sólida protección legal de este derecho fundamental. Pero si el tráfico es interceptado conjuntamente por agencias de varios países, la utilización de los datos obtenidos en dicha investigación no quedará confinada a la jurisdicción de los tribunales estadounidenses.

No obstante, en el nuevo entorno de acción policial global existe una amenaza más importante contra la libertad: la estructuración del comportamiento cotidiano de acuerdo a las normas dominantes de la sociedad. La libertad de expresión constituía la esencia del derecho a una comunicación sin trabas en un momento en que la mayor parte de las actividades cotidianas no estaban relacionadas con la expresión personal en el ámbito público. Pero en nuestra era, una porción significativa de nuestra vida cotidiana, como el trabajo, el ocio y la interacción personal, si tiene lugar en la red. Como he analizado en los capítulos precedentes, una parte sustancial de la actividad económica, social y política es en realidad un híbrido de interacción on line e interacción física (on-flesh). En muchos casos, la una no puede existir sin la otra. Así, la vida en un sistema electrónico sin privacidad implica que la mitad de nuestras vidas esté permanentemente expuesta a la vigilancia. Como vivi-

mos existencias compuestas, esta exposición puede derivar en una existencia esquizofrénica de acuerdo a la cual seríamos nosotros mismos off line y una imagen de nosotros mismos on lineo con lo que internalizaríamos la censura. El problema no es el miedo al "Gran hermano" porque en general esta vigilancia no tendrá consecuencias negativas para la mayoría de nosotros -lo más seguro es que no acarree consecuencias de ninguna clase-. En realidad la cuestión más preocupante es la ausencia de reglas explícitas de conducta, y la dificultad de predecir las consecuencias de nuestro comportamiento expuesto, que dependen de los contextos de interpretación y de los criterios utilizados para juzgar nuestro comportamiento, por una diversidad de actores situados tras las paredes de nuestra casa de cristal. No es el "Gran hermano" quien nos vigila, sino más bien una multitud de pequeñas hermanas, agencias de vigilancia y procesamiento de información, que registrarán nuestro comportamiento siempre, ya que estaremos rodeados de bases de datos a lo largo de toda nuestra vida, empezando, dentro de poco, con nuestro ADN y nuestros rasgos personales (nuestra retina o la marca digital de nuestro pulgar). Esta clase de vigilancia sólo afectará directamente a nuestras vidas bajo los regímenes autoritarios (situación en la que de hecho vive la mayor parte de la humanidad). Pero incluso en las sociedades democráticas donde se respetan los derechos civiles, la transparencia de nuestras vidas condicionará nuestras actitudes de manera decisiva. Nadie ha podido vivir jamás en una sociedad transparente. No obstante si este sistema de vigilancia y control de internet se desarrolla plenamente, no podremos hacer lo que queramos. No tendremos libertad, ni un lugar donde escondernos.

La gran ironía histórica al respecto es que una de las instituciones clave en la defensa de la libertad, la libre empresa, es la pieza clave para la construcción de este sistema de vigilancia, a pesar de la buena fe y la ideología libertaria de la mayor parte de las empresas internet. Sin su ayuda, los gobiernos carecerían del know-how y. sobre todo, de la posibilidad de intervenir en internet: todo depende de su capacidad para influir en los proveedores de servicios internet y en las redes específicas, en todos los contextos. Por ejemplo, la compañía IGC ("Intemet crimes group Inc.") está especializada en revelar la identidad de cualquier emisor anónimo de contenidos, con la cooperación de los proveedores de servicios internet. EWATCH, un servicio de PR Newswire, puede revelarle la

identidad de cualquier nombre que encuentre en la pantalla por un importe de 5.000 dólares: tiene cientos de clientes corporativos. Además, la vigilancia puede ejercerse con carácter retroactivo: Deja.com ha reunido una base de datos sobre grupos de noticias de Usenet que se puede explorar en todos sus listados en la red desde 1995 (Anónimo, 2000).

¿Por qué coopera con tanto afán el sector de la tecnología de la información en la reconstrucción del viejo mundo del control y la represión'? Hay dos razones fundamentales, aparte de actitudes oportunistas ocasionales. La primera, que concierne principalmente a las empresas puntocom, es la necesidad de quebrantar la privacidad de sus clientes para lograr vender su información. La segunda es que necesitan el apoyo del gobierno para conservar sus derechos de propiedad en la economía basada en internet. El caso Napster, en 2000-2001 constituyó un punto de inflexión. Ante la existencia de una tecnología (MP3) que permite a la gente (especialmente a los jóvenes) compartir e intercambiar su música a escala global, sin necesidad de pagar nada, las compañías discográficas movilizaron tanto a los tribunales como a la legislación gubernamental para conseguir recuperar los derechos de propiedad. Finalmente, Bertelsmann llegó a un acuerdo con Napster, que permitía el uso de esta tecnología en el contexto de una nueva estrategia comercial -bajo el control de las casas editoras-. Las editoriales y los medios de comunicación en general deben hacer frente a una amenaza similar. Los derechos de propiedad intelectual constituyen una fuente fundamental de beneficios en la economía de la información. De hecho, su protección resulta crucial para mantener la diferencia de valor entre la economía del conocimiento, basada en las redes globales dominantes y las economías industriales y de consumo, que predominan en los países en vías de desarrollo. Como señala Lessig, el “uso razonable” público de la información privada protegida por las leyes de copyright se está viendo considerablemente reducido en un contexto de protección obligatoria de esta información utilizada como un incentivo para que los productores de esta información puedan seguir generándola. Y. sin embargo, se está perdiendo el equilibrio entre estimular la producción y permitir el uso público de la misma, ya que la información se está convirtiendo en un artículo de consumo y está siendo dirigida cada vez más hacia mercados con alto nivel adquisitivo. Para imponer dicha protección, las empresas productoras de

información deben ser capaces de controlar el acceso y la identidad en internet, donde se distribuye la mayor parte de la información. Por ello, tienen mucho interés en apoyar los esfuerzos del gobierno por restablecer el control, construyendo un sistema basado en la arquitectura del software controlado, un código, por utilizar la terminología de Lessig.

El ataque global contra la privacidad para recuperar el control en un modelo de soberanía compartida, asegura los derechos de propiedad sobre la información a cambio de la utilización pública de dicha información. Con el objeto de afianzar sus intereses, las empresas y los gobiernos amenazan conjuntamente la libertad, violando la privacidad en nombre de la seguridad. Pero esta es tan sólo una cara de la moneda.

Las barricadas de la libertad en internet

Códigos contra códigos. Las tecnologías del control pueden contrarrestarse con las tecnologías de la libertad. Las hay en abundancia. a menudo producidas y comercializadas por empresas que han encontrado un nuevo nicho de mercado o inventadas, en otros casos, por resueltos luchadores por la libertad, decididos a asumir el reto. A continuación citaré algunos ejemplos, que probablemente estén anticuados en un año, pero que son ilustrativos de la batalla tecnológica actualmente en curso.

Algunas empresas como Disappearing Inc. y ZipLip han creado un tipo de correo electrónico autodestructible que utiliza tecnología de encriptación. La empresa canadiense Zero-knowledge systems descompone las identidades con un paquete de software denominado Freedom que proporciona cinco seudónimos digitales atribuibles a diversas actividades. Con el sistema Freedom es imposible rastrear los sinónimos para descubrir la verdadera identidad. Freedom dificulta el rastreamiento encriptando el correo electrónico y los requerimientos de navegación por la web y enviándolos a través de, al menos, tres enrutadores intermediarios hasta su destino final. Cada enrutador sólo puede aceptar un nivel de la encriptación. Zero-knowledge utiliza la misma tecnología, por lo que la propia empresa no es capaz de relacionar los seudónimos con los suscriptores individuales. La empresa cuenta únicamente con una lista de nombres y clientes, sin conexión con sus seudónimos. Anonymizer.com ofrece anonintizadores a cambio de su publicidad. Estos son servidores extra que aíslan el navegador del

cliente de su destino final. Idzap.corn ofrece servicios similares (Anónimo. 2000, Rosen. 2000a).

El rápido desarrollo de las tecnologías de protección de la privacidad, es precisamente lo que preocupa a los gobiernos y les lleva a intentar prohibir los usos privados de la tecnología de encriptación e ilegalizar el uso y la venta de tecnologías como las que hemos presentado anteriormente (Levy, 2001).

La lucha por el código se desarrolla también en otro campo: el desarrollo de los códigos de fuente abierta. Si los códigos de software son abiertos, entonces podrán ser alterados, bien por un usuario con los conocimientos suficientes, por una organización sin ánimo de lucro, o por una red de hackers, que trabaje en pro del bien común en la era de la información. El control propietario de los códigos de software abre el camino hacia la restricción de los usos de la información y el final de la privacidad en internet. Puede que usted piense que así es como debe ser. Pero para los que no estén de acuerdo, es muy importante poder tener la capacidad de conocer y modificar el código fuente, y en general, todo el software. En un mundo en el que el software fuera de fuente abierta, la capacidad del gobierno y las empresas para controlar la arquitectura fundacional de internet quedaría sustancialmente reducida. El camino que elijan las sociedades a este respecto no depende del código propiamente dicho sino de la habilidad de estas y sus instituciones para imponer el código, modificarlo o resistirse a él. En los albores del siglo XXI se da una inquietante combinación en el mundo de internet: una ideología libertaria muy extendida, junto a un grado de control cada vez mayor. Los movimientos sociales en defensa de la libertad en internet, tales como la coalición formada en torno al Centro de Información sobre la Privacidad Electrónica (Electronic Privacy lnformation Center) en Estados Unidos, constituyen fuentes fundamentales para la conservación del internet original como espacio de libertad. Pero la resistencia no será suficiente. Las leyes, los tribunales, la opinión pública, los medios de comunicación, la responsabilidad corporativa y las agencias políticas serán instancias fundamentales que contribuirán a decidir el futuro de internet. Es imposible controlar las redes globales, pero se puede controlar a la gente que las utiliza y, de hecho, en el futuro estará controlada, a no ser que las sociedades opten por la defensa de la libertad en internet, actuando desde las barricadas de

sus nostálgicos libertarios pero yendo más allá de ellas en su confrontación con los mecanismos del poder político.

Internet y libertad: ¿Prescindir de los gobiernos?

En buena parte de este análisis, así como en la ideología de los primeros usuarios de internet, está implícito el supuesto de que los gobiernos no son los aliados de la libertad. Y sin embargo, la historia nos enseña que el principal bastión contra la tiranía ha sido la democracia institucional y no la ideología libertaria. Entonces, ¿por qué no encomendar a los gobiernos. a los democráticos por lo menos, la regulación de los usos apropiados de Internet? Por ejemplo, la reglamentación de la Unión Europea respecto a los datos de usuarios obtenidos por parte de las empresas puntocom, protege la privacidad en un grado muy superior al permisivo ambiente laissez-faire imperante en Estados Unidos. No obstante, los gobiernos europeos están empeñados al mismo tiempo en retener todo el poder que puedan sobre la información y la comunicación, liderando el movimiento, por ejemplo, contra la difusión de la tecnología de encriptación, el sistema más efectivo para que la gente pueda controlar sus comunicaciones. En definitiva, y aunque se escuden con diversos pretextos, los gobiernos no se fían realmente de sus ciudadanos -porque creen que tienen la razón-. Los ciudadanos, por su parte, desconfían de sus gobiernos -porque ya han visto bastante-. En Estados Unidos, en 1998, un 60 % de los ciudadanos opinaba que “a los gobernantes no les importa nada lo que la gente como yo piensa” y el 63 % pensaba que “el gobierno está dirigido por unos pocos grandes intereses”. En California, los porcentajes respectivos en respuesta a esta misma pregunta fueron del 54 y el 70 % (Baldassare. 2000: 43). Podemos encontrar datos muy similares en muchos países del mundo, con la notable excepción de las democracias escandinavas. Por tanto, si la gente no se fía de su gobierno y los gobiernos no confían en sus ciudadanos (después de todo, los partidos políticos utilizan toda clase de estratagemas para ganar las elecciones), no es de extrañar que en el surgimiento de internet como un espacio de libertad se manifestara esta misma división, con los defensores de la libertad tratando de conservar esta nueva tierra de promisión y los gobiernos movilizando sus considerables recursos para cerrar este escape en sus sistemas de control.

Pero la historia podría ser diferente. Podríamos pensar en una estrategia de desarme mutuo garantizado o de recuperación de la confianza mutua. Pero como los gobiernos siguen dominando las instituciones de la sociedad, son ellos los que deberían dar el primer paso: la responsabilidad social descansa sobre sus hombros. En realidad, internet bien podría servir para que los ciudadanos vigilasen a su gobierno y no para que el gobierno vigile a sus ciudadanos. Podría transformarse en un instrumento de control, información, participación e incluso de toma de decisiones estructurado de abajo arriba. Los ciudadanos podrían tener acceso a los archivos del gobierno, lo cual constituye en realidad un derecho ciudadano. Tendrían que ser los gobiernos y no las vidas privadas de la gente los que deberían transformarse en casas de cristal, a excepción de algunas cuestiones fundamentales de seguridad nacional. Únicamente en unas condiciones de transparencia de las instituciones políticas podrían los gobiernos pretender legítimamente establecer unos mínimos controles sobre internet para detectar los pocos casos en que se manifestase el lado perverso que habita en todos nosotros. A no ser que los gobiernos dejen de temer a los ciudadanos y, por ende, a internet, el llamamiento de los ciudadanos a las barricadas de la libertad, como último recurso, mostrará una sorprendente continuidad histórica.

Bibliografía

Anonimo (2000) “The invisible Man”, *Yahoo! internet life*, octubre, 108-100.

Baldassare, Mark (2000) *California in the new millennium. The changing social and political landscape,* Berkeley, University of California Press.

Carnoy, Martin, Castells, Manuel (2001) “Globalization, The knowledge society and the network state: Poulantzas at the millennium*”, Global networks*, 1(1), 1-18.

Garfinkel, Simson (2000) *Dutabase nation,* Sebastopol, CA, O'Reilly and Associates.

Howe, Jeff (2000) “Big boss is watching”, *Yahoo! internet Life*, No. 168, 105- 107.

Lessig, Lawrence (1999) *Code and other laws of cyberspace,* New York, Basic Books.

Levy, Stephen (2001) *Crypto. How the code rebels beat the government,* New York,Viking.

Lewis, Peter H. (1996) "Judge temporarily blocks law that bars indecency on the Internet", *New York Times*, 16 de febrero, C 1.

Lyon, David (2001a) *Surveillance society: Monitoring everyday life,* Buckingham, Open University Press.

- (2001b) "Everyday surveillance: personal data and social classification". *Information, communication and society.* No. 2, 242-257.

Rosen, Jeffrey (2000a) "The erodel self", *New York Times sunday magazine*, http://www.nytimes.com/2000/04/30/magazine/-the-eroded-self.html.

- (2000b) *The unwanted gaze: The destruction of privacy in America*, New York, Random House.

Samuelson, Pamela, (2000) "Five challenges for regulating the global information society", *Regulating the global information society*, Chris Marsden (edición), Londres, Routledge.