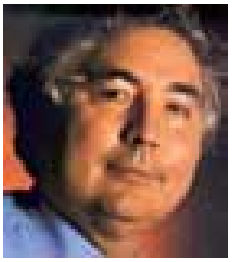
Lección inaugural del curso académico 2001-2002 de la UOC

Internet, libertad y sociedad: una perspectiva analítica



Manuel Castells

Profesor sénior del Internet Interdisciplinary Institute (IN3) de la UOC

Como toda tecnología, Internet es una creación cultural: refleja los principios y valores de sus inventores, que también fueron sus primeros usuarios y experimentadores. Es más, al ser una tecnología de comunicación interactiva con fuerte capacidad de retroacción, los usos de Internet se plasman en su desarrollo como red y en el tipo de aplicaciones tecnológicas que van surgiendo. Los valores libertarios de quienes crearon y desarrollaron Internet, a saber, los investigadores académicos informáticos, los *hackers*, las redes comunitarias contraculturales y los emprendedores de la nueva economía, determinaron una arquitectura abierta y de difícil control. Al mismo tiempo, cuando la sociedad se dio cuenta de la extraordinaria capacidad que representa Internet, los valores encarnados en la red se difundieron en el conjunto de la vida social, particularmente entre las jóvenes generaciones. Internet y libertad se hicieron para mucha gente sinónimos en todo el mundo.

Frente a tal transformación tecnológica y cultural, los detentores del poder de controlar la información a lo largo de la historia, es decir, los estados y las iglesias, reaccionaron con preocupación y, en los estados no democráticos, con hostilidad, tratando de restablecer el control administrativo de la expresión y la comunicación. Pero la ejecución del proyecto estatista sobre Internet se encuentra con obstáculos considerables. En los países democráticos, Internet se consolida como

instrumento esencial de expresión, información y comunicación horizontal entre los ciudadanos y recibe la protección constitucional y judicial de las libertades. En todos los países, menos en las teocracias, la importancia económica y tecnológica de Internet excluye que se pueda ignorar o relegar su amplio uso en la sociedad. Más aún, la ideología del progreso mediante la tecnología hace de la promoción de Internet un valor legitimador para gobiernos que fundan su estrategia en el desarrollo económico dentro del marco de la globalización. De ahí el complicado encaje de bolillos político entre la libertad y el control por parte de los Estados.

Por su parte, los internautas suelen afirmar sus derechos individuales fuera de contexto, situándose como vanguardia tecnológicamente liberada de una sociedad informáticamente iletrada. Más aún, los emprendedores llegan a empresarios mediante la comercialización acelerada de Internet, un proceso en el que frecuentemente traicionan sus principios libertarios, por ejemplo, mediante el sacrificio de la privacidad de sus clientes o la colaboración técnica e informativa con los dispositivos de control y vigilancia de la Administración.

Los ciudadanos, en general, tienden a hacer un uso instrumental y poco ideológico de Internet: lo utilizan para lo que les sirve y consideran la libertad en Internet como un tema fundamental cuando hace tiempo que se han acostumbrado al control político y comercial de su principal fuente de información: la televisión. Pero dicha actitud puede cambiar conforme vaya asentándose en la sociedad la primera generación que está creciendo con Internet. Conforme el uso de Internet vaya generalizando la información y el conocimiento sobre la importancia social decisiva del control sobre Internet, puede ser que la batalla por la libertad en la red, incluida la libertad económica de acceso a la red, desborde los confines de la actual elite ilustrada.

Internet: ¿una arquitectura de libertad? Libre comunicación y control del poder

¿Es controlable Internet? Éste es un debate sempiterno en el que se mezclan los sueños personales, los grados de (des)conocimiento tecnológico, la rutina del poder y la rapidez del cambio de los parámetros de referencia. Tratemos de clarificarlo.

En principio, el diseño de la red, a partir de una estructura en estratos (*layers*), con capacidad distribuida de comunicación para cada nodo y transmisión por *packet switching*, operada por protocolos TCP/IP, según múltiples canales de comunicación alternativos, proporciona una gran libertad a los flujos de información que circulan por Internet (www.isoc.org).

En sentido técnico, es cierta la célebre afirmación de John Gilmore de que los flujos en Internet interpretan la censura (o interceptación) como un fallo técnico y encuentran automáticamente una ruta distinta de transmisión del mensaje. Al ser una red global con poder de procesamiento de información y comunicación multinodal, Internet no distingue fronteras y establece comunicación irrestricta entre todos sus nodos. La única censura directa posible de Internet es no estar en la red. Y esto es cada vez más costoso para los gobiernos, las sociedades, las empresas y los individuos. No se puede estar "un poquito" en Internet. Existe, sí, la posibilidad de emitir mensajes unidireccionales propagados en Internet, sin reciprocidad de comunicación, en la medida en que los servidores de un país (por ejemplo, Afganistán) permanezcan desconectados de la red interna. Pero cualquier conexión en red de ordenadores con protocolos Internet permite la comunicación global con cualquier punto de la red.

Sin embargo, si la red es global, el acceso es local, a través de un servidor. Y es en este punto de contacto entre cada ordenador y la red global en donde se produce el control más directo. Se puede, y se hace en todos los países, negar acceso al servidor, cerrar el servidor o controlar quién comunica qué y a quién mediante una vigilancia

electrónica de los mensajes que circulan por el servidor. Pero los censores no lo tienen tan fácil como parece. Primero, porque en algunos países hay una protección legal considerable de la libertad de expresión y comunicación en Internet. Tal es el caso, en particular, de Estados Unidos, en donde, en 1996 y en 2000, los tribunales estadounidenses, con sentencias corroboradas por el Supremo, declararon inconstitucionales dos intentos legislativos de la Administración Clinton para establecer la censura de Internet, con el pretexto de controlar la pornografía infantil. En una sentencia célebre, de 1996, el Tribunal Federal del Distrito Este de Pensilvania reconoció que Internet es un caos, pero afirmó, textualmente: "La ausencia de regulación gubernativa de los contenidos de Internet ha producido, incuestionablemente, una especie de caos, pero lo que ha hecho de Internet un éxito es el caos que representa. La fuerza de Internet es ese caos. De la misma forma que la fuerza de Internet es el caos, la fuerza de nuestra libertad depende del caos y de la cacofonía de la expresión sin trabas que protege la Primera Enmienda. Por estas razones, sin dudarlo, considero que la Ley de Decencia en las Comunicaciones es *prima facie* inconstitucional." Así se protegió una libertad amenazada por una Administración que, pese a sus declaraciones en favor de Internet, siempre desconfió, como la mayoría de los gobiernos, de la libre expresión y autoorganización de los ciudadanos (www.eff.org).

Así pues, en la medida en que la censura de Internet es difícil en Estados Unidos y que, en 2001, la mayoría de flujos globales de Internet utilizan un *backbone* norteamericano (y muchos otros podrían utilizarlo en caso de necesidad), la protección que Estados Unidos hace de Internet crea un espacio institucional de libertad para la gran mayoría de circuitos de transmisión por Internet.

Quiero señalar, incidentalmente, que esto no admite la interpretación de un canto a Estados Unidos como tierra de libertad: lo es en algunos aspectos y en otros, no. Pero, en lo que concierne a la libre expresión en Internet, sí representa, por su tradición de liberalismo constitucional, un elemento decisivo en la capacidad de comunicación autónoma mediante Internet. Si no se pueden censurar las

comunicaciones en Estados Unidos, siempre hay formas de conectar a cualquier nodo en la red, pasando por Estados Unidos, una vez que el mensaje ha salido del servidor. Los censores tienen, sin embargo, el recurso de desconectar el servidor, de penalizar a sus administradores o de identificar el origen o al receptor de un mensaje no permitido y reprimirlo individualmente. Eso es lo que hacen los chinos, los malasios, los singapureanos y tantos otros, asiduamente, y eso es lo que pretende la legislación que se propone en algunos países europeos, España entre otros.

Ahora bien, la represión no es lo mismo que la censura. El mensaje se comunica, las consecuencias llegan luego. De modo que, más que bloquear Internet, lo que se puede hacer y se hace es reprimir a quienes hacen un uso indebido según los criterios de los poderes al uso. Por eso tienen razón tanto los que declaran Internet incontrolable como aquellos que lo consideran el más sofisticado instrumento de control, en último caso bajo la égida de los poderes constituidos. Técnicamente, Internet es una arquitectura de libertad. Socialmente, sus usuarios pueden ser reprimidos y vigilados mediante Internet. Pero, para ello, los censores tienen que identificar a los transgresores, lo cual implica la definición de la transgresión y la existencia de técnicas de vigilancia eficaces.

La definición de la transgresión depende, naturalmente, de los sistemas legales y políticos de cada jurisdicción. Y aquí empiezan los problemas. Lo que es subversivo en Singapur no necesariamente lo es en España. Y cuando, en el año 2000, en Estados Unidos, un *web site* organizó la venta legal de votos de personas ausentes que vendían su voto al mejor postor de los candidatos políticos, motivando una persecución legal, el *web site* se trasladó a Alemania, donde un delito electoral americano no caía bajo la represión policial. De modo que la geometría política variable de Internet permite operar desde distintos servidores hacia distintas redes. Como no hay una legislación global, pero sí hay una red global de comunicación, la capacidad de control sistemática y preventiva se diluye en la práctica.

Sí, en cambio, se puede proceder, desde cada centro de poder, a la

identificación y subsiguiente represión de quienes sean los transgresores de las normas dictadas por dicho poder. Para ello, se dispone ahora de tecnologías de control que, en su mayor parte, fueron creadas por los empresarios informáticos que hacen negocio de cualquier cosa sin importarles demasiado los principios libertarios que afirman en su vida personal. Dichas tecnologías son fundamentalmente de tres tipos: de identificación, de vigilancia y de investigación (www.epic.org).

Las principales tecnologías de identificación son las contraseñas, los *cookies* y los procedimientos de autenticidad. Las contraseñas son los símbolos convenidos que usted utilizó para entrar en esta red. Los *cookies* son marcadores digitales que los *web sites* así equipados insertan automáticamente en los discos duros de los ordenadores que los conectan. Una vez que un *cookie* entra en un ordenador, todas las comunicaciones de dicho ordenador en la red son automáticamente registradas en el *web site* originario del *cookie*. Los procedimientos de autenticidad son firmas digitales que permiten a los ordenadores verificar el origen y características de las comunicaciones recibidas.

Generalmente, utilizan tecnología de encriptación. Trabajan por niveles, de modo que los servidores identifican a usuarios individuales y las redes de conexión identifican a los servidores.

Las tecnologías de vigilancia permiten interceptar mensajes, insertar marcadores gracias a los cuales se puede seguir la comunicación de un ordenador o un mensaje marcado a través de la red; también consisten en la escucha continua de la actividad de comunicación de un ordenador o de la información almacenada en dicho ordenador. El famoso programa Carnivore del FBI permite analizar mediante palabras clave enormes masas de información de las comunicaciones telefónicas o Internet, buscando y reconstruyendo en su totalidad aquellos mensajes que parezcan sospechosos (aunque algunas detenciones sobre esas bases resultaron bastante chuscas, arrestando a buenas madres de familia que comentaban electrónicamente el peligro del consumo de drogas en la escuela de sus hijos). Las tecnologías de vigilancia permiten identificar el servidor originario de un determinado

mensaje. A partir de ahí, por colaboración o coacción, los mantenedores de los servidores pueden comunicar al detentor del poder la dirección electrónica de donde provino cualquier mensaje.

Las tecnologías de investigación se organizan sobre bases de datos obtenidos del almacenamiento de la información resultante de las tecnologías de vigilancia. A partir de esas bases de datos se pueden construir perfiles agregados de usuarios o conjuntos de características personalizadas de un usuario determinado. Por ejemplo, mediante el número de tarjeta de crédito, asociado a un número de carné de identidad y a la utilización de un determinado ordenador, se puede reconstruir fácilmente el conjunto de todos los movimientos que realiza una persona que dejen registro electrónico. Como eso es algo que hacemos todos los días (teléfono, correo electrónico, tarjetas de crédito), parece evidente que ya no hay privacidad desde el punto de vista de la comunicación electrónica.

O sea, la combinación de las tecnologías de identificación, de vigilancia y de investigación configuran un sistema en que quien tenga el poder legal o fáctico de acceso a esa base de datos puede conocer lo esencial de lo que cada persona hace en la red y fuera de ella. Desde ese punto de vista, la red no se controla, pero sus usuarios están expuestos a un control potencial de todos sus actos más que nunca en la historia. Así pues, un poder político, judicial, policial o comercial (defensores de derechos de propiedad) que quiera actuar contra un internauta determinado puede interceptar sus mensajes, detectar sus movimientos y, si están en contradicción con sus normas, proceder a la represión del internauta, del prestador de servicios, o de los dos.

Obviamente, el control no proviene tan sólo del gobierno o de la policía.

Las empresas vigilan rutinariamente el correo electrónico de sus empleados y las universidades, el de sus estudiantes, porque la protección de la privacidad no se extiende al mundo del trabajo, bajo el control de la organización corporativa.

Pero ni Internet es una red de libertad, en un mundo en que la tecnología puede servir para el control de nuestras vidas mediante su registro electrónico, ni la tendencia al control ubicuo es irreversible. En sociedad, todo proceso está hecho de tendencias y contratendencias, y la oposición entre libertad y control continúa sin fin, a través de nuevos medios tecnológicos y nuevas formas institucionales.

A las tecnologías de control y vigilancia se contraponen tecnologías de libertad. Por un lado, el movimiento para el software de fuente abierta permite la difusión de los códigos sobre los que se basa el procesamiento informático en las redes. Por consiguiente, a partir de un cierto nivel de conocimiento técnico, frecuente entre los centros de apoyo a quienes defienden la libertad en la red, se puede intervenir en los sistemas de vigilancia, se pueden transformar los códigos y se pueden proteger los propios programas. Naturalmente, si se acepta sin rechistar el mundo de Microsoft, se acabó cualquier posibilidad de privacidad y, por tanto, de libertad en la red. Entre otras cosas, porque cada programa Windows contiene un identificador individual que acompaña a través de la red cualquier documento generado desde ese programa. Pero la creciente capacidad de los usuarios para modificar sus propios programas crea una situación más compleja en la que el controlado puede pasar a ser controlador de los sistemas que lo vigilan.

La otra tecnología fundamental en la reconstrucción de la libertad en la red es la encriptación (www.kriptopolis.com).

Bien es cierto que, como toda tecnología, su relación con la libertad es ambigua, como señala Lessig (1999; 2000 en castellano), porque, por un lado, protege la privacidad del mensaje pero, por otro, permite los procedimientos de autentificación que verifican la identidad del mensajero.

Sin embargo, en lo esencial, las tecnologías de encriptación permiten, cuando funcionan, mantener el anonimato del mensaje y borrar las huellas del camino seguido en la red, haciendo difícil, pues, la interceptación del mensaje y la identificación del mensajero. Por eso, la batalla sobre la encriptación es, desde el punto de vista técnico, una

batalla fundamental por la libertad en Internet.

Pero no todo es tecnología en la defensa de la libertad. En realidad, lo más importante no es la tecnología sino la capacidad de los ciudadanos para afirmar su derecho a la libre expresión y a la privacidad de la comunicación. Si las leyes de control y vigilancia sobre Internet y mediante Internet son aprobadas por una clase política que sabe que el control de la información ha sido siempre, en la historia, la base del poder, las barricadas de la libertad se construirán tecnológicamente. Pero es aún más importante que las instituciones de la sociedad reconozcan y protejan dicha libertad. Por eso, movilizaciones de opinión como la de Electronic Frontier Foundation, en Estados Unidos, y tantas otras redes en Europa y en el mundo han sido elementos influyentes a la hora de frenar las tendencias represivas que se albergan en las burocracias gubernamentales y en los sectores ideológicamente conservadores, asustados del potencial liberador de Internet. En último término, es en la conciencia de los ciudadanos y en su capacidad de influencia sobre las instituciones de la sociedad, a través de los medios de comunicación y del propio Internet, en donde reside el fiel de la balanza entre la red en libertad y la libertad en la red.

La cultura de libertad como constitutiva de Internet

Las tecnologías son producidas por su historia y por el uso que se hace de ellas. Internet fue diseñada como una tecnología abierta, de libre uso, con la intención deliberada de favorecer la libre comunicación global. Y cuando los individuos y comunidades que buscan valores alternativos en la sociedad se apropiaron de esa tecnología, ésta amplificó aún más su carácter libertario, de sistema de comunicación interactivo, abierto, global y en tiempo escogido (www.isoc.org/internet-history/brief.html).

En principio, esta afirmación podría sorprender, puesto que el

antepasado más directo de Internet, Arpanet, fue creado en 1969 (y presentado al mundo en 1972) en ARPA, la oficina de proyectos avanzados de investigación del Departamento de Defensa del gobierno de Estados Unidos. Y, sin embargo, no sólo el diseño de sus creadores se inspiró en principios de apertura de la red, sino que los principales nodos de Arpanet se localizaron en universidades, con acceso posible a ellos por parte de profesores y estudiantes de doctorado, eliminando toda posibilidad de control militar estricto. Ni siquiera es cierta la historia, a menudo contada, de que Arpanet se creó para salvaguardar las comunicaciones norteamericanas de un ataque nuclear sobre sus centros de mando y coordinación. Es cierto que hubo un proyecto de Paul Baran, en la Rand Corporation, propuesto a la Fuerza Aérea, para construir un sistema de comunicación flexible y descentralizado basado en una nueva tecnología de transmisión, *packet switching*. Pero, si bien dicha tecnología fue esencial en el desarrollo de Internet, el proyecto de Baran fue rechazado por el Departamento de Defensa e Internet no encontró aplicaciones militares hasta treinta años más tarde, cuando las tropas de elite estadounidenses empezaron a organizarse en red aprovechando la facilidad de comunicación interactiva ubicua.

La razón oficial para el desarrollo de Arpanet fue facilitar la comunicación entre los distintos grupos universitarios de informática financiados por el Departamento de Defensa y, en especial, permitir que compartieran tiempo de ordenador en las potentes máquinas que existían tan sólo en algunos centros. Pero, de hecho, muy rápidamente el aumento de capacidad y velocidad de los ordenadores hizo que sobrara tiempo de computación, con lo que la utilidad directa de Arpanet no era evidente. Lo que de verdad ocurrió fue que un grupo de investigadores informáticos, generosamente financiados por el Departamento de Defensa, encontraron un instrumento perfecto para llevar a cabo su investigación en red, y, pronto, se entusiasmaron con la perspectiva de desarrollar un sistema de comunicación entre ordenadores, que se concretó en los protocolos TCP/IP desarrollados por Cerf y Kahn en 1973, y luego por Cerf, Kahn y Postel en 1978.

Desde el principio, los diseñadores de Internet, todos ellos procedentes del mundo académico, aunque algunos de ellos trabajaron en el

entorno del Departamento de Defensa y consultoras asocidadas, buscaron deliberadamente la construcción de una red informática abierta y sin cortapisas, con protocolos comunicables y una estructura que permitiera añadir nodos sin cambiar la configuración básica del sistema. Fue una cultura de libertad inspirada en los principios de la investigación académica y en la práctica de compartir los resultados de la investigación con los colegas, de forma que el juicio de la comunidad informática académica sobre la contribución de cada uno era la recompensa más importante al trabajo obtenido.

¿Por qué el Departamento de Defensa les dejó tal libertad? En realidad, porque quien supervisó el desarrollo de Internet fue una agencia de promoción de investigación, ARPA, formada en buena parte por científicos e ingenieros y que siguió la estrategia innovadora y atrevida de buscar la supremacía tecnológica de Estados Unidos (tras el susto recibido por el Sputnik soviético) a partir de la excelencia de sus universidades. Pero cualquier académico que se precie no acepta limitaciones a su libertad de investigación y comunicación de resultados. Por tanto, para obtener la mejor investigación en informática y telecomunicaciones (que ARPA vio en seguida como tecnologías decisivas), los fondos fueron a parar a los mejores grupos (MIT, Stanford, Berkeley, Carnegie Mellon, UCLA, USC, SRI, BBN, UC Santa Barbara, Utah, etc.) sin restricciones burocráticas. De hecho, la estrategia resultó, porque no solamente se desarrolló Internet, sino que, merced al salto gigantesco de la investigación universitaria en tecnologías de información y comunicación, Estados Unidos obtuvo una supremacía tecnológica que también llegó al terreno militar, que puso a la defensiva en los años ochenta a la Unión Soviética y, en último término, llevó a su malograda perestroika y posterior desintegración, como hemos demostrado en nuestro libro (Castells y Kiselyova, 1995).

Una vez que las tecnologías de Internet se desarrollaron de forma abierta a través de las universidades, fueron conectando con otros medios sociales y otras actitudes culturales a lo largo de los años setenta y ochenta. Por un lado, los *hackers* vieron en Internet un medio privilegiado de comunicación e innovación y aplicaron su enorme

potencial de creatividad y capacidad tecnológica a perfeccionar el software de Internet, utilizando el poder de la colaboración abierta en red para incrementar su capacidad tecnológica. Por otro lado, los movimientos contraculturales y alternativos tomaron Internet como forma de organización de comunidades virtuales y proyectos culturales autónomos, a partir del desarrollo de los PC, que puso en manos de la gente el poder de procesamiento informático y de comunicación en red (Rheingold, 1993; 2000). Con cada nueva oleada de usuarios, llegó una plétora de nuevas aplicaciones que los programadores autónomos inventaron a partir de su práctica; por ejemplo, el *World Wide Web*, que programó Tim Berners-Lee, en el CERN, en 1990.

Cada nueva aplicación se publicaba en la red, con lo que el conocimiento colectivo se fue profundizando y la capacidad tecnológica de la red ampliando y haciéndose más fácil de usar. Así, se generalizó el uso de Internet por círculos concéntricos a partir de los *hackers* y los estudiantes de las universidades más avanzadas, hasta llegar a los más de 400 millones de usuarios en la actualidad (había 16 millones en 1995, primer año del *World Wide Web*).

Una vez que Internet tuvo pleno desarrollo tecnológico y una base de usuarios suficientemente amplia, una nueva generación de empresarios lo utilizó como negocio y como nueva forma de hacer negocio, llevando su uso a todos los ámbitos de la economía y, por tanto, de la sociedad. Si la investigación académica inventó Internet, la empresa fue la que lo difundió en la sociedad, tres décadas más tarde. Pero, entre los dos procesos tuvo lugar la apropiación, transformación y desarrollo de Internet por dos culturas de libertad que fueron decisivas en su tecnología y en sus aplicaciones: la cultura *hacker* y las comunidades contraculturales, que plasmaron su autonomía en la tecnología, estructura y usos de la red.

Hackers, crackers, libertad y seguridad

Los *hackers* y su cultura son una de las fuentes esenciales de la invención y continuo desarrollo de Internet. Los *hackers* no son lo que los medios de comunicación o los gobiernos dicen que son. Son, simplemente, personas con conocimientos técnicos informáticos cuya pasión es inventar programas y desarrollar formas nuevas de procesamiento de información y comunicación electrónica (Levy, 1984; Raymond, 1999). Para ellos, el valor supremo es la innovación tecnológica informática. Y, por tanto, necesitan también libertad. Libertad de acceso a los códigos fuente, libertad de acceso a la red, libertad de comunicación con otros *hackers*, espíritu de colaboración y de generosidad (poner a disposición de la comunidad de *hackers* todo lo que se sabe, y, en reciprocidad, recibir el mismo tratamiento de cualquier colega). Algunos *hackers* son políticos y luchan contra el control de los gobiernos y de las corporaciones sobre la red, pero la mayoría no lo son, lo importante para ellos es la creación tecnológica. Se movilizan, fundamentalmente, para que no haya cortapisas a dicha creación. Los *hackers* no son comerciales, pero no tienen nada contra la comercialización de sus conocimientos, con tal de que las redes de colaboración de la creación tecnológica sigan siendo abiertas, cooperativas y basadas en la reciprocidad.

La cultura *hacker* se organiza en redes de colaboración en Internet, aunque de vez en cuando hay algunos encuentros presenciales. Distintas líneas tecnológicas se agrupan en torno a grupos cooperativos, en los cuales se establece una jerarquía tecnológica según quiénes son los creadores de cada programa original, sus mantenedores y sus contribuidores. La comunidad suele reconocer la autoridad de los primeros innovadores, como es el caso de Linus Torvalds en la comunidad Linux. Pero sólo se reconoce la autoridad de quien la ejerce con prudencia y no la utiliza para su beneficio personal.

El movimiento *hacker* más político (en términos de política de libertad tecnológica) es el creado por Richard Stallman, un programador de

MIT, que constituyó en los años ochenta la Free Software Foundation para defender la libertad de acceso a los códigos de UNIX cuando ATT trató de imponer sus derechos de propiedad sobre UNIX, el sistema operativo más avanzado y más compatible de su tiempo, y sobre el que se ha fundado en buena parte la comunicación de los ordenadores en la red. Stallman, que aprendió el valor de la libertad en el movimiento de libre expresión en sus tiempos de estudiante en Berkeley, sustituyó el *copy right* por el *copy left*. Es decir, que cualquier programa publicado en la red por su Fundación podía ser utilizado y modificado bajo licencia de la Fundación bajo una condición: difundir en código abierto las modificaciones que se fueran efectuando. Sobre esa base, desarrolló un nuevo sistema operativo, GNU, que sin ser Unix, podía utilizarse como UNIX. En 1991, un estudiante de 21 años de la Universidad de Helsinki, Linus Torvalds, diseñó su propio UNIX kernel para su PC 386 sobre la base de Fundación. Y, siguiendo las reglas del juego, publicó la fuente de su código en la red, solicitando ayuda para perfeccionarlo. Cientos de programadores espontáneos se pusieron a la tarea, desarrollando así el sistema operativo Linux (que recibió ese nombre del administrador del sistema en la Universidad de Helsinki, puesto que el nombre que Torvalds le había dado era el de Freix), considerado hoy en día el más avanzado del mundo, sobre todo para ordenadores en Internet, y la única alternativa actual a los programas de Microsoft. Linux cuenta en la actualidad con más de 30 millones de usuarios y está siendo promocionado por los gobiernos de Francia, de Brasil, de la India, de Chile, de China, entre otros, así como por grandes empresas como IBM. Siempre en código abierto y sin derechos de propiedad sobre él.

El filósofo finlandés Pekka Himanen (www.hackerethic.org) argumenta convincentemente que la cultura *hacker* es la matriz cultural de la era de la información, tal y como la ética protestante fue el sistema de valores que coadyuvó decisivamente al desarrollo del capitalismo, según el análisis clásico de Max Weber. Naturalmente, la mayoría de los capitalistas no era protestante ni la mayoría de los actores de la sociedad de la informacion es *hacker*. Pero lo que esto significa es lo siguiente: una gran transformación tecnoeconómica necesita un caldo

de cultivo en un sistema de valores nuevo que motive a la gente para hacer lo que hace. En el caso del capitalismo, fue la ética del trabajo y de la acumulación de capital en la empresa como forma de salvación personal (lo cual, desde luego, no impidió, sino que justificó, la explotación de los trabajadores).

En la era de la información, la matriz de todo desarrollo (tecnológico, económico, social) está en la innovación, en el valor supremo de la innovación que, potenciada por la revolución tecnológica informacional, incrementa exponencialmente la capacidad de generación de riqueza y de acumulación de poder. Pero innovar no es un valor obvio. Debe estar asociado a una satisfacción personal, del tipo que sea, ligado al acto de la innovación. Eso es la cultura *hacker*, según Himanen. El placer de crear por crear. Y eso mueve el mundo, sobre todo el mundo en que la creación cultural, tecnológica, científica y también empresarial, en su aspecto no crematístico, se convierte en fuerza productiva directa por la nueva relación tecnológica entre conocimiento y producción de bienes y servicios. Se podría argumentar que, así definido, hay *hackers* en todas partes y no sólo en la informática. Y ése es, en realidad, el argumento de Himanen: que todo el mundo pueder ser *hacker* en lo que hace y que cualquiera que esté movido por la pasión de crear en su actividad propia está motivado por una fuerza superior a la de la ganancia económica o la satisfacción de sus instintos. Lo que ocurre es que la innovación tecnológica informática tiene el piñón directo sobre la rueda del cambio en la era de la información, de ahí que la cultura *hacker* se manifieste de forma particularmente espectacular en las tecnologías de información y en Internet.

En realidad, los *hackers* han sido fundamentales en el desarrollo de Internet. Fueron *hackers* académicos quienes diseñaron los protocolos de Internet. Un *hacker*, Ralph Tomlinson, trabajador de la empresa BBN, inventó el correo electrónico en 1970, para uso de los primeros internautas, sin comercialización alguna. *Hackers* de los Bell Laboratories y de la Universidad de Berkeley desarrollaron UNIX. *Hackers* estudiantes inventaron el módem. Las redes de comunicación electrónica inventaron los tablones de anuncio, los chats, las listas

electrónicas y todas las aplicaciones que hoy estructuran Internet. Y Tim Berners-Lee y Roger Cailliau diseñaron el *browser/editor World Wide Web*, por la pasión de programar, a escondidas de sus jefes en el CERN de Ginebra, en 1990, y lo difundieron en la red sin derechos de propiedad a partir de 1991. También el *browser* que popularizó el uso del *World Wide Web*, el Mosaic, fue diseñado en la Universidad de Illinois por otros dos *hackers* (Marc Andreesen y Eric Bina) en 1992. Y la tradición continúa: en estos momentos, dos tercios de los servidores de web utilizan Apache, un programa servidor diseñado y mantenido en software abierto y sin derechos de propiedad por una red cooperativa.

En una palabra, los *hackers* informáticos han creado la base tecnológica de Internet, el medio de comunicación que constituye la infraestructura de la sociedad de la información. Y lo han hecho para su propio placer, o, si se quiere, por el puro goce de crear y compartir la creación y la competición de la creación. Ciertamente, unos pocos de entre ellos también se hicieron ricos como empresarios, pero mediante aplicaciones de sus innovaciones, no mediante la apropiación de la innovación cooperativa en su propio beneficio (aunque el caso de Andreesen es menos claro, en este sentido). Otros obtuvieron buenos puestos de trabajo, pero sin ceder en sus principios como *hackers*. También hubo quien se hizo famoso, como Linus Torvalds, pero su fama vino de su reconocimiento de la comunidad de *hackers*, que implica el respeto a sus reglas de libertad y cooperación. Los más permanecieron anónimos para el mundo y llevan y llevaron una vida modesta. Pero obtuvieron, mediante su práctica de innovación cooperativa, la más alta recompensa a la que aspira un *hacker*, el reconocimiento como tal por parte de la única autoridad que puede otorgar dicha distinción: la comunidad global de *hackers*, fuente esencial de innovación en la era de la información.

En los márgenes de la comunidad *hacker* se sitúan los *crackers*. Los *crackers*, temidos y criticados por la mayoría de *hackers*, por el desprestigio que les supone ante la opinión pública y las empresas, son aquellos que utilizan sus conocimientos técnicos para perturbar procesos informáticos (Haffner y Markoff, 1995).

Hay muy distintos tipos de *crackers*, pero no considero entre ellos a aquellos que penetran en ordenadores o redes de forma ilegal para robar: éstos son ladrones de guante blanco, una vieja tradición criminal. Muchos *crackers* pertenecen a la categoría de *script kiddies*, es decir, bromistas de mal gusto, muchos de ellos adolescentes, que penetran sin autorización en sistemas o crean y difunden virus informáticos para sentir su poder, para medirse con los otros, para desafiar al mundo de los adultos y para chulear con sus amigos o con sus referentes en la red. La mayoría de ellos tiene conocimientos técnicos limitados y no crea ninguna innovación, por lo que son, en realidad, marginales al mundo *hacker*. Otros *crackers*, más sofisticados, penetran en sistemas informáticos para desafiar personalmente a los poderes establecidos, por ejemplo, a Microsoft o las grandes empresas. Y algunos utilizan su capacidad tecnológica como forma de protesta social o política, como expresión de su crítica al orden establecido. Ellos son quienes se introducen en sistemas militares, administraciones públicas, bancos o empresas para reprocharles alguna fechoría. Entre los ataques de *crackers* con motivación política hay que situar los practicados por movimientos políticos o por servicios de inteligencia de los gobiernos, como la guerra informática desarrollada entre los *crackers* islámicos e israelíes o entre los pro-chechenos y los servicios rusos.

En suma, en la medida en que los sistemas informáticos y las comunicaciones por Internet se han convertido en el sistema nervioso de nuestras sociedades, la interferencia con su operación a partir de una capacidad técnica de actuación en la red es un arma cada vez más poderosa, que puede ser utilizada por distintos actores y con distintos fines. Éstas son las acciones de los *crackers*, que deben ser absolutamente deslindados de los *hackers*, a cuya constelación pertenecen, pero con quienes no se confunden.

La vulnerabilidad de los sistemas informáticos plantea una contradicción creciente entre seguridad y libertad en la red. Por un lado, es obvio que el funcionamiento de la sociedad y sus instituciones y la privacidad de las personas no puede dejarse al albur de cualquier

acción individual o de la intromisión de quienes tienen el poder burocrático o económico de llevarla a cabo. Por otro lado, como ocurre en la sociedad en general, con el pretexto de proteger la información en la red se renueva el viejo reflejo de control sobre la libre comunicación.

El debate sobre seguridad y libertad se estructura en torno a dos polos: por un lado, la regulación político-jurídica de la red; por otro, la autoprotección tecnológica de los sistemas individuales. Naturalmente, hay fórmulas intermedias, pero, en general, dichas fórmulas mixtas tienden a gravitar hacia la regulación institucional de la comunicación electrónica. Quienes defienden la capacidad de autorregulación de la red argumentan que existen tecnologías de protección que son poco vulnerables, sobre todo cuando se combinan los *fire walls* (o filtros de acceso) de los sistemas informáticos con las tecnologías de encriptación, que hacen muy difíciles de interceptar los códigos de acceso y el contenido de la comunicación. Es así como están protegidos los ordenadores del Pentágono, de los bancos suizos o de Scotland Yard. La mayor parte de las instituciones de poder y de las grandes empresas tiene sistemas de seguridad a prueba de cualquier intento de penetración que no cuente con capacidad tecnológica e informática similar. Cierto que hay una carrera incesante entre sistemas de ataque informático y de protección de éstos, pero por esto mismo, el corazón de dichos sistemas es poco vulnerable para el común de los *crackers*.

Ahora bien, al estar los sistemas informáticos conectados en red, la seguridad de una red depende en último término de la seguridad de su eslabón más débil, de forma que la capacidad de penetración por un nodo secundario puede permitir un ataque a sus centros más protegidos. Esto fue lo que ocurrió en el año 2000 cuando los *crackers* se introdujeron en el sistema de Microsoft y obtuvieron códigos confidenciales, a partir de la penetración en el sistema personal de un colaborador de Microsoft que tenía acceso a la red central de la empresa. Es manifiestamente imposible proteger el conjunto de la red con sistemas de *fire walls* y encriptación automática. Por ello, sólo la difusión de la capacidad de encriptación y de autoprotección en los sistemas individuales podría aumentar la seguridad del sistema en su

conjunto. En otras palabras, un sistema informático con capacidad de computación distribuida en toda la red necesita una protección igualmente distribuida y adaptada por cada usuario a su propio sistema. Pero eso equivale a poner en manos de los usuarios el poder de encriptación y autoprotección informática. Algo que rechazan los poderes políticos con el pretexto de la posible utilización de esta capacidad por los criminales (en realidad, las grandes organizaciones criminales tienen la misma capacidad tecnológica y de encriptación que los grandes bancos). En último término, la negativa de las administraciones a permitir la capacidad de encriptación y de difusión de tecnología de seguridad entre los ciudadanos conlleva la creciente vulnerabilidad de la red en su conjunto, salvo algunos sistemas absolutamente aislados y, en última instancia, desconectados de la red.

De ahí que gobiernos y empresas busquen la seguridad mediante la regulación y la capacidad represiva de las instituciones más que a través de la autoprotección tecnológica de los ciudadanos. Es así como se reproduce en el mundo de Internet la vieja tensión entre seguridad y libertad.

La experiencia española de regulación de Internet

Los gobiernos de la mayoría de los países han acogido Internet con una actitud esquizofrénica. Por un lado, como icono de modernidad e instrumento de desarrollo económico. Por otro, con una profunda desconfianza hacia el uso que pueden hacer los ciudadanos de esa potencialidad de libre comunicación horizontal. De ahí los continuos intentos de regulación, legislación e instauración de mecanismos de control, siempre al amparo de la protección necesaria de los niños, los principios democráticos y los consumidores.

En Estados Unidos, la Administración Clinton intentó dos veces, en 1996 y en 2000, establecer la censura de Internet por vía legislativa, perdiendo la batalla, en ambas ocasiones, tanto ante la opinión pública como ante los tribunales. En Europa, varios gobiernos y la Comisión

Europea han tomado diversas iniciativas reguladoras. Fiel a su trayectoria histórica, el gobierno francés ha sido particularmente celoso de la soberanía nacional en materia de control de la información. La alarma sonó en Francia, en 1995, cuando las memorias del médico de Mitterrand, cuya publicación había sido prohibida por la autoridad judicial, se difundieron en la red. El ministro de Información declaró que dicho gesto era un atentado intolerable contra la autoridad del Estado e inició un esfuerzo de largo alcance para crear mecanismos de control de la información en Internet, toda vez que el sueño francés de un Minitel republicano y tricolor, controlado desde el centro, se desvaneció ante la realidad de las redes globales autoevolutivas.

La Comisión Europea dictó varias directivas reguladoras que debían ser incorporadas en las legislaciones nacionales. Una de ellas, la directiva 2000/31/CE, estableció criterios para regular el comercio electrónico buscando "la integración jurídica comunitaria con objeto de establecer un auténtico espacio sin fronteras interiores en el ámbito de los servicios de la sociedad de la información". La vaguedad del concepto de "servicios de la sociedad de la informacion" dejó abierta la puerta a toda clase de interpretaciones, plasmadas en textos legislativos y ordenanzas administrativas.

Con la intención de traducir la directiva europea en una ley española, el Ministerio de Ciencia y Tecnología del gobierno español elaboro un Anteproyecto de Ley de Servicios de la Sociedad de la Información, cuya primera publicación tuvo lugar el 16 de marzo de 2000. El proyecto fue difundido en Internet para su discusión. Dio lugar a tal polémica entre la comunidad internauta, tanto española, como mundial, que sigue en discusión en estos momentos. La tercera redacción del Anteproyecto, elaborada el 30 de abril de 2001, está en trámite parlamentario en octubre del 2001, habiendo ya suscitado un vivo debate durante su discusión en el Senado en septiembre de este mismo año (www.internautas.org/propuestalssi.htm). El proyecto ha sido fuertemente criticado por sectores influyentes de los internautas españoles, agrupados en este caso en torno a la campaña contra el LSSI lanzada por la revista digital Kriptópolis, especializada en temas

de seguridad y libertad en la red, con una postura militante en la defensa de los derechos civiles de los usuarios de Internet. Kriptópolis ha llevado su oposición hasta el punto de decidir el traslado provisional de su *web site* a un servidor en New Jersey, en previsión de los efectos de censura que podría suponer la aprobación en España de este proyecto de ley. La Asociación de Internautas ha sido menos radical en su postura, pero también solicita una modificación del articulado que, manteniendo la regulación de servicios comerciales en la red para proteger a los usuarios, impida la arbitrariedad administrativa en la decisión sobre lo que se puede y no se puede hacer en la red. Sin poder entrar en el detalle del debate jurídico, teniendo en cuenta el objetivo analítico general de esta lección, resaltaré que las críticas, apoyadas por los partidos políticos de oposición (http://www.psc.es/ambit/ntic/documents/default.asp?apt=665, www.ic-v.org/lssi/index.htm), se centran en dos puntos esenciales:

Por un lado, la falta de protección judicial en la decisión de sancionar a un prestador de servicios por algún acto relativo a la difusión de información en la red. El artículo 11 del Anteproyecto establece que: "Todos los prestadores de servicios de la sociedad de la información establecidos en España deberán cumplir las siguientes obligaciones en relación con los contenidos: [...] c). Suspender la transmisión, el alojamiento de datos, el acceso a las redes de telecomunicaciones o la prestación de cualquier otro servicio de la sociedad de la información, en ejecución de resoluciones dictadas por una autoridad judicial o administrativa". La palabra esencial, naturalmente, es *administrativa*, porque ello abre la vía a que un funcionario, sin iniciativa judicial, pueda intervenir en la libre expresión en Internet, en contradicción directa con el artículo 20 de la Constitución Española.

El segundo punto controvertido en el Anteproyecto de LSSI es la definición de un ente inventado por la Comisión Europea, "los servicios de la sociedad de la información". En principio, en el Anteproyecto se establece que, a los efectos de la ley, los servicios regulados son aquellos que "representen una actividad económica y comercial" y no son regulados, en cambio, aquellas "páginas web, servicios de FTP, intercambio de ficheros, servidores de correo, noticias, boletines

informativos, o cualquier otro servicio considerado como personales, aun cuando éstas tengan asignado dominio propio, sean realizadas de forma personal o entre varias personas, y que no tienen como fin último ser una actividad económica y comercial". Esta delimitación es lo que permite al Ministerio argumentar que se está respetando plenamente la libertad de expresión y que lo único que se regula es la actividad comercial en la red. Sin embargo, es difícil hacer una distinción clara entre lo que tiene y no tiene implicaciones de actividad económica en la red, porque ofrecer información en línea, o instrumentos de búsqueda o acceso y recopilación de datos que ofrezcan publicidad directa o indirecta puede ser considerada como actividad comercial. Por ejemplo, el tener *banners* publicitarios en un portal implica una actividad económica por parte del prestador de servicios. Y aquellas páginas personales que, para financiarse, ofrecen enlaces a portales con contenido comercial o publicitario también podrían caer bajo una cierta interpretación de lo que es y no es comercial.

Así, esta misma lección inaugural, al ofrecer enlaces electrónicos con sitios y portales que pueden estar asociados a *banners* publicitarios (que difícilmente se pueden evitar cuando se está haciendo referencia a una amplia gama de fuentes de información en la red), podría caer bajo la guillotina del censor administrativo a quien no le gustaran ciertas afirmaciones o que, simplemente, no las entendiera y decidiera prohibir por si acaso, como solía ocurrir en la España franquista. Más aún, teniendo en cuenta la importancia de las sanciones previstas en la normativa, con multas de hasta 600.000 euros para los prestadores de servicios, la actitud lógica de la mayoría de ellos podría ser la autocensura en caso de duda, de modo que la capacidad de expresión en Internet, a partir de los servidores basados en España, se vería fuertemente limitada (pero no así, como el mismo caso de Kriptópolis indica, la de aquellas empresas u organizaciones con capacidad para alojarse en un servidor extranjero y más concretamente estadounidense, puesto que es en Estados Unidos donde Internet goza de mayor protección judicial).

En estos momentos, el debate social y parlamentario continúa en la sociedad, en las instituciones y en la red, y es probable que haya nuevas modificaciones y aclaraciones en la ley definitiva. Pero la experiencia es rica en enseñanzas, de las que quiero resaltar tres.

La primera es el considerable nerviosismo de las administraciones, alentado desde las burocráticas instituciones europeas, sobre su posible pérdida de control de las actividades en la red, nerviosismo favorecido por el desconocimiento y la falta de familiaridad con el medio Internet. Como señala el abogado de Kriptópolis, Sánchez Almeida, ya existen suficientes normativas para proteger los derechos de los ciudadanos y penalizar las conductas delictivas, dentro y fuera de la red. Basta con aplicarlas. El problema puede ser técnico, la dificultad de aplicar esas sanciones en la red, lo cual requiere una modernización de las instituciones judiciales y policiales. Pero ante la dificultad de esa modernización se intenta resolver el problema descentralizando la censura previa a la estructura de prestadores de servicios y haciéndolos responsables de las excepcionales infracciones que puedan representar algunos contenidos. Es como hacer responsables a los propietarios de las imprentas por las consecuencias que pudieran resultar de la publicación de ciertos artículos en la prensa. O a los operadores de telecomunicaciones por las conversaciones telefónicas entre mafiosos que planean un robo.

Mi segunda observación se refiere a la postura ideológica defensiva de los reguladores de Internet. Se multiplican las fórmulas precautorias para afirmar la importancia de Internet y de su libre expresión, en línea con la ideología liberal que predomina en la mayoría de los gobiernos europeos, cualquiera que sea su tendencia política. Pero los viejos reflejos estatistas se combinan con esa ideología, llevando a formulaciones ambiguas y políticas titubeantes, cuya plasmación legislativa contribuye a la confusión.

En tercer lugar, es notable la capacidad de reacción de la comunidad internauta a cualquier intento de coartar su libertad. No tendrán la vida fácil quienes aún piensen que las instituciones del Estado pueden continuar operando como antes del desarrollo de Internet.

Ahora bien, la defensa de la libertad en Internet tiende a ser selectiva. Se reacciona contra el Estado, pero se descuida la defensa de la libertad de los usuarios, de los ciudadanos y de los trabajadores, en un mundo en que los abusos de poder y la desigualdad no han desaparecido ante la magia de la red. Por un lado, muchos prestadores de servicios imponen condiciones económicas leoninas para acceder a la red, invaden la privacidad de sus usuarios y organizan enlaces en la red según sus intereses comerciales, por ejemplo, jerarquizando los *web sites* en los buscadores. Por otro lado, los derechos sindicales de expresión en la red están siendo ignorados en muchas empresas, como denuncia, entre otras, la campaña sobre este tema llevada a cabo en el 2001 por Comisiones Obreras de Cataluña. En suma, la libertad en Internet, como en la sociedad, es indivisible. La defensa de la libre expresión y comunicación en la red debería alcanzar a todo el mundo, a los consumidores, a los trabajadores, a las organizaciones cívicas. Y en esa libertad parece normal incluir las condiciones materiales de dicha libertad, empezando por las tarifas de conexión y la difusión de los medios informáticos de comunicación en el conjunto de la población. La libertad sin igualdad se convierte en privilegio y debilita los fundamentos de su defensa por parte de la sociedad en su conjunto.

Encriptación

Las organizaciones de poder, a lo largo de la historia, han hecho del secreto de sus comunicaciones un principio fundamental de su actividad. Dicho secreto se intentó proteger mediante la encriptación, es decir, la codificación del lenguaje mediante una clave secreta sólo conocida por la organización emisora del mensaje y el destinatario del mensaje determinado por dicha organización. El anecdotario histórico abunda con ejemplos de batallas e, incluso, guerras supuestamente perdidas o ganadas mediante la interceptación y desencriptación de mensajes decisivos entre los centros de poder. El origen de la informática contemporánea durante la Segunda Guerra Mundial parece estar relacionado con los esfuerzos de matemáticos extraordinarios,

como el inglés Turing, para desarrollar algoritmos capaces de descifrar los códigos del enemigo.

Por tanto, en cierto modo, no es de extrañar en la era de la información, basada en la comunicación de todo tipo de mensajes, que el poder (y, por tanto, la libertad) tenga una relación cada vez más estrecha con la capacidad de encriptar y descifrar. Hete aquí que lo que era una arcana tecnología matemática relegada a los dispositivos secretos de los servicios de inteligencia de los Estados se haya convertido, en el espacio de dos décadas, en la tecnología clave para el desarrollo del comercio electrónico, para la protección de la privacidad, para el ejercicio de la libertad en la red y, también, paradójicamente, para nuevas formas de control en la red. La encriptación es el principal campo de batalla tecnológico-social para la preservación de la libertad en Internet.

Trataré de explicar el sentido de esta afirmación. Y lo haré utilizando una somera referencia histórica al desarrollo de la encriptación en la sociedad en las dos últimas décadas, con especial referencia a Estados Unidos. Como documenta Steven Levy (2001) en su apasionante libro sobre el tema, la tecnología de encriptación estaba monopolizada en todos los países por los servicios de inteligencia, que tenían a su disposición una legión de matemáticos de primer orden, y, en cuanto aparecieron los ordenadores, las mejores y más potentes máquinas a su servicio. Con la ayuda de dichas máquinas, los matemáticos construían claves difíciles de penetrar y, al tiempo, procesaban a gran velocidad una enorme combinatoria para encontrar los puntos débiles (patrones repetitivos que pudieran desvelar la clave secreta) en los mensajes cifrados de otras organizaciones.

En Estados Unidos, la supersecreta National Security Agency (con poderes mucho más extensos que los del FBI o la CIA) fue y es la que dispone de la mayor capacidad tecnológica de encriptación/desciframiento del planeta. Tal importancia se le atribuyó a esta tecnología que se clasificó en el rubro de armamento que no se podía exportar fuera de Estados Unidos sin un permiso especial del Departamento de Defensa. De modo que enviar una fórmula

matemática a un colega fuera de Estados Unidos se convirtió en un delito penado por la ley. Más aún, la NSA tuvo buen cuidado de cooptar, contratar o amenazar a aquellos matemáticos que se adentraron en ese complejo campo de investigación. Pero hubo quienes resistieron a la presión y se atrevieron a desarrollar fórmulas autónomas de encriptación. Tal fue el caso del legendario Whitfield Diffie, un matemático sin carrera académica, obsesionado por la encriptación desde joven, que, en colaboración con un profesor de Stanford, Marty Hellman, y con la ayuda de un estudiante de Berkeley, Ralph Merkel, descubrió, a mediados de los setenta, nuevas formas de encriptación y, pese a las presiones del gobierno, las publicó. Su genialidad consistió en el llamado principio de la doble clave o clave pública. Hasta entonces, toda clave se basaba en un algoritmo que permitía cifrar un mensaje de forma difícil de reconocer y, al mismo tiempo, reconstruirlo en su sentido original basándose en el conocimiento de dicho algoritmo. Este método tradicional requería una centralización total del sistema de claves únicas y, por tanto, era vulnerable a quien penetrara en esa base de datos. Lo que se adaptaba al secreto militar de una organización separada de la sociedad no era practicable en una sociedad en que todo se basaba en comunicación electrónica y en que los individuos, las empresas y las propias instituciones necesitaban una protección cotidiana de sus mensajes para garantizar su privacidad y su autonomía. Esto requería una descentralización e individualización del sistema de encriptación. Mediante el principio de la doble clave, cada persona u organización tiene dos claves de encriptación (o sea, códigos informáticos que permiten transformar el texto de un mensaje en un sistema digital que altera el sentido lingüístico y lo puede volver a reconstruir).

Una de las claves es *pública* en el sentido de que es asignada al originario/destinatario de un mensaje y que se conoce, mediante un listado, qué clave corresponde a quién. Pero, sin el conocimiento de la clave privada, es muy difícil, si no imposible, descifrar el mensaje. Esa otra clave es específica a cada individuo u organización, sólo quien la detenta la puede utilizar, pero sólo sirve con relación a su clave pública en la que recibe el mensaje. Mediante este ingenioso sistema

matemático, se garantiza a la vez la generalidad del cifrado y la individualidad de su desciframiento.

Como en otros temas de la historia de Internet, el poder de encriptación descentralizado recibió dos usos. Por un lado, fue comercializado. Por otro, sirvió como instrumento de construcción de autonomía de redes de comunicación. La comercialización, en su origen, corrió a cargo de tres matemáticos de MIT o asociados a MIT, Rivest, Shamir y Adleman, que perfeccionaron el sistema de encriptación Diffie-Hellman y, con ayuda de hombres de negocios más avezados que ellos, patentaron y desarrollaron la tecnología de encriptación RSA, que sirvió de base para buena parte de las tecnologías de protección de las comunicaciones electrónicas que se utilizan hoy en día.

En efecto, a partir del sistema de doble clave, no sólo se puede preservar el secreto del mensaje sino establecer la autenticidad de su originario. De modo que la encriptación es la base de las firmas digitales que permiten el desarrollo del comercio electrónico en condiciones de relativa seguridad. En efecto, si la gente pudiera encriptar sus mensajes en lugar de enviar un mensaje por correo electrónico con su número de tarjeta de crédito abierto a todo el mundo, no tendrían por qué temer su interceptación y mal uso. Esto es, en realidad, lo que hacen las grandes empresas con capacidad de encriptación para transferir fondos y comunicarse mensajes confidenciales. Pero la tecnología de autentificación y firma digital se está difundiendo bajo el control de las empresas e instituciones, sin transmitir la capacidad autónoma de encriptación a los usuarios. Ello es así, por un lado, porque la comercialización de la tecnología creó un sistema de patentes que la hacen costosa en su uso comercial.

Pero, más importante todavía, las administraciones de casi todos los países han puesto enormes cortapisas a la difusión de la tecnología de encriptación por lo que ello representa de posible autonomía para los individuos y organizaciones contestatarias con respecto a los gobiernos y a las grandes empresas. De ahí que se desarrollara una segunda tendencia, de matriz libertaria, para proporcionar a los ciudadanos la

tecnología de encriptación. Un personaje fundamental en este sentido fue Phil Zimmerman, otro matemático rebelde que, en 1991, en respuesta a los intentos del Senado estadounidense de prohibir la encriptación en el marco de la legislación antiterrorista, difundió en Internet su sistema PGP (*Pretty Good Privacy*). PGP está también basado en principios similares a los inventados por Diffie y Hellman, pero en lugar de crear un directorio de claves públicas se basa en una red autónoma de autentificación en la que cada persona autentifica con su firma digital a una persona que conoce y así sucesivamente, de modo que, con conocer bien a una persona de la cadena, dicho conocimiento es suficiente para saber que la identidad del detentor de una determinada clave pública es fidedigna. Zimmerman sufrió persecución judicial por su gesto, pues, naturalmente, la publicación en Internet supuso que mucha gente en todo el mundo registrara las fórmulas en su ordenador, lo que, desde el punto de vista jurídico, equivalía a exportar armamento sin licencia, aunque Zimmerman no se beneficiara de la operación. También la empresa comercializadora de RSA lo amenazó judicialmente por utilizar conocimientos que habían patentado los investigadores de MIT (pero no Diffie y Hellman, los primeros innovadores de la tecnología). Zimmerman pertenecía a una red informal de criptógrafos que se reunían anualmente en un movimiento contracultural (autodenominados *cypherpunks*) y que aumentaron su número e influencia con el advenimiento de Internet. Uno de los participantes más respetados en este movimiento tecnolibertario es John Gilmore, uno de los pioneros de Sun Microsystems, que, en 1990, creó, junto con Mitch Kapor y John Perry Barlow, la Electronic Frontier Foundation, una de las principales organizaciones de defensa de las libertades en el mundo digital. Es significativo el discurso que sobre la encriptación pronunció John Gilmore en 1991 en una reunión sobre "ordenadores, libertad y privacidad":

"¿Qué tal si creáramos una sociedad en la que la información nunca pudiera ser registrada? ¿En la que se pudiera pagar o alquilar un vídeo sin dejar un número de tarjeta de crédito o de cuenta bancaria? ¿En la que pudiera certificar que tiene permiso de conducir sin dar su

nombre? ¿En la que se pudiera enviar o recibir un mensaje sin revelar la localización física, como una casilla postal electrónica? Éste es el tipo de sociedad que quiero construir. Quiero garantizar, con física y matemáticas, no con leyes, cosas como la verdadera privacidad de las comunicaciones personales [...] la verdadera privacidad de los expedientes personales [...], la verdadera libertad de comercio [...], la verdadera privacidad financiera [...] y el verdadero control de la identificación" (citado por Levy, 2001; pág. 208).

Esta utopía de la libertad sin instituciones, mediante el poder de la tecnología en manos de los individuos, es la raíz de los proyectos libertarios en la sociedad de la información. Es una poderosa visión que informó proyectos empresariales y sociales a lo largo de la siguiente década. Por ejemplo, uno de los personajes más innovadores del mundo de la criptografía, David Chaum, desarrolló el dinero digital sin huella personal y fundó en Holanda una empresa, Digicash, para comercializar su invento. La empresa fracasó por falta de apoyos en el mundo empresarial, que siempre desconfió de su carácter visionario.

Pero, del mundo de los cypherpunks, como se autodenominaron los anarcocriptógrafos, salieron tecnologías de protección de la privacidad a través de los diseños de anonimato en la red mediante los *remailers*, es decir, programas que retransmiten automáticamente los mensajes a través de un circuito de *servers* hasta borrar los orígenes de procedencia de los mensajes (www.anonymizer.com). El más avanzado diseñador de estos *remailers* en los años noventa fue, en 1993, el informático finlandés Julf Helsingius, que desarrolló sistemas de *remail* desde su casa de Helsinki para permitir la libre comunicación de alcohólicos en rehabilitación sin riesgo a ser identificados. Creó Penet, un sistema que opera en una máquina UNIX con un 386, y sin ningún tipo de publicidad empezó a recibir miles de mensajes de todo el mundo que, transitando por su sistema, borraban todo rastro. La ingenuidad de *hacker* de Helsingius acabó obligándolo a cerrar su servidor cuando una querella criminal contra él, efectuada desde Los Ángeles, llevó a la policía finlandesa hasta su casa. Negándose a ejercer la censura y a denunciar los orígenes de las rutas que llegaban

a su servidor, prefirió cerrar Penet. Sin embargo, la idea de anonimizadores continuó desarrollándose y, en estos momentos, hay numerosas empresas (de las cuales la más conocida es la canadiense Zero Knowledge) que permiten a cualquiera utilizar Internet sin dejar huella (www.silentsurf.com).

Si tal posibilidad se generalizara, la libertad de las personas para comunicarse, expresarse y organizarse sería total. De ahí las diversas iniciativas en los gobiernos de todo el mundo para controlar la capacidad de encriptación y para limitar su uso.

Sin embargo, los términos del debate no son tan claros, porque la tecnología de encriptación sirve a la vez para proteger la privacidad (garantizando, por tanto, la libertad de comunicación) y para autentificar lo originario de un mensaje, permitiendo, por consiguiente, individualizar los mensajes (www.qsilver.queensu.ca/sociology). Más aún, en los movimientos contestatarios en torno a Internet, tales como la red Freenet, se produjo, en el año 2000, una evolución desde la defensa del derecho a encriptar (para proteger la privacidad del ciudadano) hacia el derecho a descifrar (para permitir el acceso de los ciudadanos a la información detentada por gobiernos y empresas). Ahora bien, en cualquier caso, la práctica de ambos derechos pasa por la capacidad autónoma de la gente para utilizar las tecnologías de encriptación. Esto significa, por un lado, el libre desarrollo de tecnologías de encriptación en comunicación horizontal del tipo PGP, a saber, con doble clave y autentificación mediante redes de confianza interpersonal. Por otro, requiere la capacidad de libre difusión de la información de tecnologías de encriptación en la red. Tanto la administración estadounidense como el G8 y el Consejo de Europa (además de los sospechosos habituales de la censura, a saber, China, Singapur, Malasia, los países islámico-fundamentalistas, etc.) se han pronunciado a favor del control burocrático de la tecnología de encriptación y están desarrollando legislación y medidas administrativas para conseguirlo.

En realidad, a pesar de lo que piensen los tecnolibertarios, ninguna tecnología asegura la libertad. Pero de igual manera que el control de

los medios de impresión fue en la historia el fundamento de la restricción o expansión de la libertad de prensa, en nuestra época la difusión o control de la tecnología de encriptación se ha convertido en un criterio definidor para saber en qué medida los gobiernos confían en sus ciudadanos y respetan sus derechos.

* * *

¿Cuál es, entonces, la relación entre Internet y libertad? La historia y la cultura de Internet lo constituyeron como tecnología de libertad. Pero la libertad no es una página blanca sobre la que se proyectan nuestros sueños. Es el tejido áspero en el que se manifiestan los poderes que estructuran la sociedad. Al efecto Gilmore se contrapone el efecto Microsoft. Según el primero, Internet interpreta cualquier censura como un obstáculo técnico y tiende a rodearlo. Según el segundo, Microsoft interpreta cualquier proceso de comunicación como oportunidad de negocio y tiende a monopolizarlo. A las aspiraciones de libertad se contraponen los instintos básicos de las burocracias políticas, cualesquiera que sean sus ideologías. Y a liberación de la humanidad por la tecnología de la información se contrapone la realidad presente de una humanidad mayoritariamente desinformada y marginada de la tecnología.

Internet, en nuestro tiempo, necesita libertad para desplegar su extraordinario potencial de comunicación y de creatividad. Y la libertad de expresión y de comunicación ha encontrado en Internet su soporte material adecuado. Pero tanto Internet, como la libertad, sólo pueden vivir en las mentes y en los corazones de una sociedad libre, libre para todos, que modele sus instituciones políticas a imagen y semejanza de su práctica de libertad.

Referencias bibliográficas

CASTELLS, M.; KISELYOVA, E. (1995). *The collapse of the Soviet Union: the View from the Information Society*. Berkeley: University of California, International & Area Studies Book Series.

HAFFNER, K.; MARKOFF, J. (1995). *Cyberpunks: outlaws and hackers in the computer frontier*. New York: Touchstone Books.

HIMANEN, P. (2001). *The hacker ethic and the spirit of the Information Age*. Prólogo de Linus Torvalds. New York: Random House (en castellano, Destino, 2002).

LESSIG, L. (1999). *Code and other laws of cyberspace*. New York: Basic Books (en castellano, Taurus, 2001).

LEVY, S. (1984). *Hackers. Heroes of the computer revolution*. New York: Penguin.

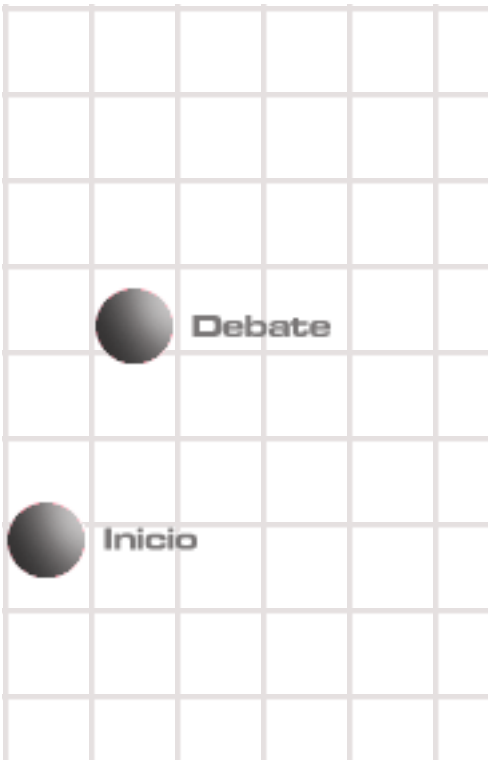
LEVY, S. (2001). *Crypto. How the code rebels beat the government - saving privacy in the digital age*. New York: Viking.

RAYMOND, E. (1999). *The cathedral and the bazaar. Musings on Linux and Open Source by an accidental revolutionary*. Sebastopol, California: O' Reilly (en castellano, Alianza Editorial, 2002).

RHEINGOLD, H. (1993/2000). *The virtual community. Homesteading in the electronic frontier*. Cambridge, Massachussets: MIT Press.

[Fecha de publicación: octubre 2001]

Imprimir
Recomendar
El autor
Referencias bibliográficas


Debate
Inicio