Encriptación

Autor: Manuel Castells

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

Fecha de Publicación: Octubre de 2001

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.

Referencias bibliográficas

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