



**Assange, J., Appelbaum, J., Müller-Maguhn, A. & Zimmermann, J. (2013). *Cypherpunks*. Barcelona: Deusto.**

«La buena criptografía puede resistir la aplicación ilimitada de la violencia. No existe fuerza coercitiva alguna que pueda resolver un problema matemático».

Julian Assange, *Cypherpunks*.

Un *cypherpunk* es un activista que utiliza la criptografía como forma de acción directa no violenta para alcanzar un cambio político y social. Surge en el marco de unas sociedades altamente tecnologizadas donde nuestros movimientos pueden ser monitorizados y aplica el cifrado como forma de resistencia a ese control. *Cypherpunks* es el libro en el que Julian Assange, Jacob Appelbaum, Andy Müller-Maguhn y Jérémie Zimmermann, cuatro activistas de este movimiento, debaten sobre el futuro de Internet y las implicaciones de la vigilancia masiva de la que hoy todos tenemos conocimiento gracias a las revelaciones de Edward Snowden.

Internet ha servido como herramienta de emancipación en muchos sentidos y, debido a que sigue desarrollándose, tiene numerosas posibilidades que están todavía por explorar. Sin embargo, del mismo modo que puede servir para este fin, puede utilizarse para su contrario. Según las palabras del propio Julian Assange, “se ha transformado en la [herramienta] facilitadora más peligrosa del totalitarismo jamás vista” (p. 13). Internet puede ayudar a dotarnos de una mayor autonomía, como cuando la utilizamos para organizar determinadas reivindicaciones al margen de los marcos institucionales establecidos, pero también puede destinarse a controlar cada uno de nuestros movimientos, como de hecho ocurre.

---

Como los autores comentan en este debate que llevan a cabo, el control viene ya integrado en los dispositivos que son cada vez más herméticos, impidiendo de este modo que podamos comprenderlos. Cada día es más complicado abrir un teléfono y entender su arquitectura, del mismo modo que cada día es más difícil cambiar los faros del coche sin pasar por el mecánico debido a su propia estructura. Si no conocemos las herramientas que estamos manejando no podemos gobernarlas y somos nosotros los que pasamos a ser gobernados por ellas. Además, hay que añadir el hecho de que hoy estos dispositivos están conectados a la red, lo que permite la monitorización antes mencionada. La falta de acceso al conocimiento se convierte de este modo en un medio de dominación, algo que está relacionado con el trabajo que Assange lleva a cabo – con la colaboración de los demás integrantes de este debate – en WikiLeaks. El secreto, lo que está oculto, aquello a lo que no podemos acceder, tiene un control sobre nosotros en la medida en que escapa a nuestro conocimiento, de forma que nos mantiene al margen de sus procesos sin ninguna posibilidad de intervenir en ellos. Sólo aquellos ante quienes lo oculto es desvelado pueden jugar un papel en su desarrollo. Precisamente por este motivo, la criptografía aplicada a nuestras prácticas comunicativas nos dota de autonomía al frenar el dominio que sobre ellas puedan ejercer fuerzas externas dejándolas margen e impidiendo que penetren en nuestras comunicaciones privadas. De aquí radica el sentido de la famosa expresión de Julian Assange: “privacidad para el débil, transparencia para el poderoso”. La criptografía sirve para brindar privacidad a las personas, impidiendo de este modo que ningún gobierno pueda inmiscuirse en sus asuntos privados y dotándolas así de independencia y libertad sobre sus acciones. La transparencia, en cambio, aplicada a gobiernos e instituciones, impide que en ellos se concentre y limite su poder evitando que nada quede oculto y, de este modo, fuera del control ciudadano.

Los cuatro *cypherpunks* que en esta obra se dan cita consideran que el ciberespacio ha sido militarizado y que en él se lleva a cabo un control exhaustivo de nuestros movimientos a través de la industria que diariamente consumimos. Se trata de un enfoque que Andy Müller-Maguhn, uno de los primeros miembros del *Chaos Computer Club*, encuentra “estratégico”: no se limitan a vigilar un tráfico determinado en un espacio concreto de tiempo y lugar, como correspondería a un enfoque “táctico”, sino que lo hacen por defecto, almacenando la información de todas las acciones que llevamos a cabo para poder, posteriormente, procesarla con sistemas analíticos “porque nunca sabes cuando alguien se convierte en sospechoso” (p. 53). Por su parte, Jérémie Zimmermann, co-fundador y portavoz del grupo *La Quadrature du Net*, apunta:

---

La vigilancia financiada por los Estados es un asunto capital que desafía a la estructura intrínseca de todas las democracias y al modo en que éstas funcionan, pero también existe la vigilancia privada que potencialmente puede derivar en la recopilación masiva de datos. Sólo hay que fijarse en Google. Si eres un usuario estándar de Google, el buscador sabe con quién te comunicas, a quién conoces, a quién buscas, tu posible orientación sexual y tus creencias religiosas y filosóficas (p. 65).

Jacob Appelbaum, uno de los principales defensores e investigadores del Proyecto *Tor3*, denuncia que, mediante lo que él denomina “los cuatro jinetes del info-apocalipsis” –pornografía infantil, terrorismo, drogas y blanqueo de dinero–, se está llevando a cabo una invasión de la privacidad sin precedentes y, junto al resto de autores, reflexiona sobre si estos problemas son una razón suficiente para ello, concluyendo que no. Todos ellos recuerdan que las agencias de espionaje estadounidenses tienen acceso a toda la información que es almacenada por Google y Facebook, donde pasa el mayor tráfico de Internet, por lo que prácticamente cualquier dato que emitamos está a su alcance: “¿Acaso sabes lo que buscaste hace dos años, tres días y cuatro horas? No lo sabes; Google sí” (p. 65). Para Jacob, las empresas no están exentas de culpa si construyen unos sistemas donde todo queda registrado aún sabiendo que hay leyes que permiten a los gobiernos acceder a todos esos datos con total impunidad, cuando pueden realizar otros diseños donde, por el mismo código fuente, no habría forma de llevar a cabo dicha incursión. Y es que, sostienen, que es la propia arquitectura la que define las posibilidades del sistema beneficiando un tipo de política u otro.

Como Lawrence Lessig escribió ya en su obra *El código* (2009), dicho código tiene una función reguladora que permite o impide (según sea) realizar determinado tipo de acciones. Se ve muy bien la idea en el ejemplo que utiliza sobre la regulación de volar sobre una propiedad privada en *Second Life* frente al espacio físico:

Fijémonos, no obstante, en la importante diferencia existente entre una y otra regulación. En el espacio real la ley establece penas por violar la regla de “alto/bajo”; en *Second Life*, simplemente no se puede violar la regla de los 15 metros. La regla forma parte del código y éste controla cómo somos en *Second Life*. No tenemos la opción de desobedecer la regla, al igual que no la tenemos de desobedecer la ley de la gravedad

(Lessig, 2009, p. 186).

---

En este caso, el código se convierte en ley impidiendo una determinada acción. De este mismo modo, el diseño de un *software* determina los usos que de ella se pueden hacer. Langdon Winner (1986) también coincide en este punto, considerando que la tecnología comienza en su diseño. Es precisamente en este sentido en el que la criptografía puede servir como herramienta contra cualquier fuerza coercitiva que nos quieran aplicar. Y si se utilizase para crear las leyes de Internet, todavía en construcción, podría garantizar su independencia y con ella las que Assange considera que son nuestras cuatro libertades básicas: la libertad de movimiento, de pensamiento, de comunicación y de interacción económica, hoy todas ellas vulneradas. Para los *cyberpunks*, ninguna amenaza a nuestra seguridad debe pasar por encima de nuestras libertades, y en cualquier caso nos corresponde a nosotros, como ciudadanos libres y autónomos, decidir lo que queremos sin que otro ajeno a nosotros nos lo imponga. Como ellos mismos apuntan, los problemas relacionados con la pornografía infantil, las drogas, el blanqueo de dinero o el terrorismo no van a desaparecer porque sean censurados, excusa por la que todos nuestros datos son almacenados. Y además, para Assange, “el hecho de establecer un régimen de censura capaz de eliminar grandes trozos de historia significa que nunca afrontaremos el problema, porque no podemos identificar el problema en sí” (p. 145). Desde el punto de vista de todos ellos, nosotros tenemos capacidad suficiente para gestionar lo que vemos, leemos, etc. y, por tanto, somos nosotros quienes tenemos que poder decidir.

Con el desarrollo de las nuevas tecnologías y el fuerte aumento de control sobre lo que hacemos, son muchas las preguntas que debemos hacernos si queremos estudiar sus implicaciones. Este libro nos invita a reflexionar sobre algunas de ellas, y nos ofrece una clave que puede resolver el problema: la criptografía. Hoy sabemos que estamos sometidos a una vigilancia masiva por parte de los servicios de espionaje de los Estados Unidos y, aunque son muchas las personas que argumentan no interesarse por el tema porque desde su punto de vista no tienen nada que esconder, el hecho es que el derecho a la privacidad está siendo vulnerado y esto es algo que debemos analizar. Como usuarios tenemos una responsabilidad y como seres humanos no deberíamos relegarla. Cuando sabemos que estamos siendo observados nos autocensuramos inconscientemente, independientemente de que estemos haciendo algo malo o no, coartando de este modo nuestra libertad. No se dicen ni se hacen las mismas cosas en público que en privado y esto es algo que hay que considerar.

Los *cyberpunks* tienen muy claro que los próximos pasos que se tomen en relación al ciberespacio acabarán por determinarlo y que del mismo modo que puede servir como espacio

de emancipación, puede servir como espacio de control. Para ellos el problema es urgente y la solución radica en nosotros: “sólo una élite rebelde y altamente tecnificada podrá ser libre, estas ratas listas que corretean por el teatro de la ópera” (p. 168). La criptografía puede ser una herramienta clave para este fin, pero si continuamos sin conocer la tecnología que manejamos toda seguridad se basará en un acto de fe. Hace falta con urgencia una cultura tecnológica.

Estela Mateo Regueiro  
Universidad de Salamanca  
estelamr@usal.es

## Referencias

ASSANGE, J., APPELBAUM, J., MÜLLER-MAGUHN, A., ZIMMERMANN, J. (2013). *Cypherpunks*. Barcelona: Deusto. (Edición original 2012).

LESSIG, L. (2009). *El Código 2.0*. Madrid: Traficantes de Sueños. (Edición original 2006)

WINNER, L. (1986). *The whale and the reactor: a search for limits in age of high technology*. Chicago: University of Chicago Press.