

Assange, J. y Appelbaum, J. (2012). Cypherpunk. Digital: OR Books.

Autor: Jesse Tangen-Mills¹

El caso contra la policía del pensamiento digital

“Internet, nuestra mejor herramienta de emancipación, ha sido transformado en el facilitador más peligroso de totalitarismo que se haya visto jamás. Internet es una amenaza a la civilización humana”. Así comienza Julian Assange el libro que coescribió, *Cypherpunks*. Si *Cypherpunks* –o ciferpunqueros– le suena a ciencia ficción, tiene toda la razón. Pero en la mitología que invoca Assange vale la pena por lo menos considerarlo, dado que hoy en día es la figura pública más buscada y perseguida, por un lado (un senador estadounidense pidió su asesinato con *drone*), y venerada y alabada, por el otro (el filósofo Cornel West lo llamó un *freedom fighter*).

El prefijo ‘cifer’ en el título se deriva de la palabra griega para una escritura secreta. En este caso, manipula el cifer con criptografía en transmisiones por Internet que permite, por momentos, anonimía total. Los *cypherpunks* se definen por su activismo a favor de la libertad digital. Según ellos “criptografía es la última forma directa de acción no violenta” (p. 11). Tales mitologías no pueden ser hechas sin una metanarrativa, y Assange no nos desilusiona. Escribe en el prefacio: “Vimos que la unión entre estructuras estatales existentes y el internet creyó una apertura para cambiar la naturaleza de los estados” (p. 8). Queda implícito que los colaboradores ciferpunqueros de Wikileaks son de otros países –Estados Unidos, Alemania– es decir, que forman parte de la ‘apertura’ de la que habla Assange. Entre sus colegas cuenta con: Jacob Applebaum, de San Francisco, quien ha abogado el sistema de anonimía *online* Tor; Andry Muller-Maguhm, miembro de Chaos Computer Club de Alemania e inventor de Cryptophone –un teléfono digital que presta comunicaciones encriptadas–; Jeremy Zimmerman, del grupo La Quadrature du Net, proponente de los

¹ Pontificia Universidad Javeriana, Colombia. jesse.tangenmills@gmail.com

derechos de anonimia *online* y líder de la campaña europea contra la adopción del ACTA (Acuerdo Antipirata y Comercio, por sus siglas en inglés).

Cypherpunk es el resultado de una conversación dentro de la embajada ecuatoriana en Londres entre Assange y otros *cypherpunks*. Desde hace un año el creador de Wikileaks vive exiliado ahí para evitar una extradición que siente inminente. Pesan sobre él acusaciones de acoso sexual en Suecia, por lo cual puede ser extraditado a los Estados Unidos. Su red de conexiones con la prensa en todos los países del mundo le ha otorgado el poder de revelar los datos ocultos de embajadas, tanto de los Estados Unidos como de Europa y el tercer mundo. Quizá su publicación más vergonzosa para los Estados Unidos fue el “Afghan War Diary”, que documenta docenas de encubrimientos. Por ejemplo, un video muestra a miembros de las fuerzas armadas matando libremente a civiles desarmados, entre ellos, dos periodistas de la agencia Reuters. Encarcelaron al soldado ahora informante Bradley Manning, y le pusieron en aislamiento por un año, bajo posible pena de la muerte.

La relación entre Assange y Colombia es distinta. Después de una reunión clandestina con el editor de *El Espectador*, Fidel Cano, Assange pasó los miles de cables diplomáticos interceptados al periódico, que resultaron en varios artículos sobre la parapolítica, publicados durante 2011.

La conversión de Internet abierto en un sistema de vigilancia es la preocupación principal de los *cypherpunks*. La salvación del ciberespacio es la criptografía. El índice de la importancia de la criptografía según ellos son dos guerras cifer. A diferencia de la noción de Virilio de una ciberguerra, ésta toma lugar solamente en Internet y las cortes. La primera fue en los años 90 cuando varios gobiernos intentaron prohibir el software cifer que hacían proliferar los hacktivistas. Y ahora estamos en la segunda lucha por la criptografía. En el nombre de lo que los *cypherpunks* llaman “los cuatro jinetes de info-apocalipsis” –la pornografía infantil, el terrorismo, el lavado de dinero y “la guerra contra algunas drogas” (p.43)–, los gobiernos polemizan la autonomía total que proveen algunas tecnologías. Es precisamen-

te la visión de un Internet no seguro, carente de vigilancia, lo que permite a los estados avanzar en sus ‘ciberguerras’ contra la criptografía.

Vale la pena recordar que Internet fue ya imaginado antes de su creación, como un espacio de posibilidad visto desde dos campos: los utopistas y los milenarios. El ciber mundo utópicamente libre y abierto ha existido desde que el novelista William Gibson acuñó la palabra. No obstante, sus detractores abundan, quizá más memorablemente en la interpretación apocalíptica de Paul Virilio, en la cual subraya la implicación de la ubicuidad de Internet (y presintiendo en los 90 la era del *drone*). Assange comparte algo de los dos campos, aunque su tono alarmista delata una tendencia al pesimismo (en una entrevista reciente citó una preocupación por el aumento constante de la velocidad en Internet).

No obstante, la pregunta más relevante es: ¿hasta qué punto podemos considerar a Internet un ‘mundo’, más que cualquier otra tecnología? ¿No sería aún más radical entender Internet como la extensión del ser humano? Para los *cypherpunks* alguna vez fue un rango digital libre y abierto, que ahora es monitoreado y controlado dentro de espacios nacionales. Desde el modelo chino, con un sistema monolito, hasta el estadounidense, mucho más bifurcado pero con más agentes de control, o, como en el caso libio, donde es una tecnología simplemente comprada en el mercado internacional para uso nacional, todos los estados ya manejan sus propias formas de vigilancia y control para Internet. Sin embargo, como propone Assange, el debate entre los Estados-naciones y sus poblaciones está ya quedando en las manos de agencias de inteligencia, muchas de ellas privadas. La tecnología es cada día menos costosa, y así la vigilancia digital es un mercado en aumento. Assange pregunta si ahora ese estado de conexión y vigilancia define lo que es el Estado. Cita el caso de una red de fibra óptica en el sur del Líbano, controlada y financiada por Hizbulá, que permite una cierta autonomía y dentro de esa autonomía otras normas de control.

Es precisamente la gran cantidad y variedad de los datos publicados por Wikileaks lo que evita un claro sello político. La mantra quiasmática de Assange es: “transparencia para los poderosos, clandestinidad por los no pode-

rosos”. No obstante, si el lector espera, como diría Gilles Deleuze, algún tipo de línea de fuga, no la encontrará, pero verá en cambio un discurso jurídico sobre la igualdad frente a la transmisión de datos. De hecho, impresiona que con todo lo liberal que es Assange –con énfasis en el bien común y la importancia del derecho, “las libertades básicas” (p. 87)–, tantos lo hayan pintado cómo un extremista. La lógica clave del supuesto insurgente digital está en el fondo basada en la teoría de Emile Durkheim (la noción por ejemplo de que el Estado define la violencia).

Quizá el problema que los gobiernos tienen con Assange es su apoyo flagrante a chivatos. En una época donde las huellas digitales parecen ser el mecanismo más avanzado de identificación humana, básicamente cualquier persona puede ser expuesta por aquellos que dominan el manejo de los códigos de programación. Mientras tanto, algunos gobiernos pueden ver todo lo que hacen sus ciudadanos si les interesa. Por el momento, el conocimiento y las conexiones de Assange le han otorgado un poder quizás único. Pero ¿qué afectos pueden tener unos clips filtrados?

Wikileaks mantiene que la publicación de cables, gracias a alianzas con Nawaat.org de Túnez (Tunileaks), catalizó la primavera árabe en 2010. Puede que en parte sea cierto, pero su mantra no era el mismo de Assange, sino una derivación de un poema de Abou Al-kasem Ecebbi (1909-1934): “La gente quería derribar el régimen” (Omri, 2013). Así que el alfabetismo tradicional –como proponía Benedict Anderson– parece seguir jugando un rol clave en los imaginarios nacionales y por extensión en los movimientos sociales. El Estado es más que sólo “determinar dónde y cómo se aplica la fuerza coercitiva contundentemente” (p.12). La derrota del régimen de Ben Ali más bien muestra cómo Wikileaks, o la transparencia, funcionan en tándem con las tecnologías tradicionales del Estado.

Es por sus intervenciones que Assange mantiene aún algún grado de fe en el ciber mundo: “Si miramos el desarrollo que produce en masa nuevos productos culturales y lenguajes a la deriva, y las subculturas que forman sus propios mecanismos de interacción potenciadas por Internet” (p.158). No es casualidad que esa definición se pueda aplicar a los *cypher-*

punks. Lo que los *cypherpunks* aún no reconocen es la tendencia humana, como argumenta Sloterdijk, a encerrarse en sus propias normas establecidas por el lenguaje o, si queremos, por poemas, en el caso de Túnez. Esas rejas son más fuertes que la opresión abierta del Estado. La visión *ciferpunkiana* suena orwelliana, pero en su raíz es un argumento jurídico; todos debemos tener *derecho* a saber cómo funciona un computador y *derecho* a no ser espiados. Pero ¿qué haríamos en la Internet libre? Intercambiar productos intelectuales. Diagnosticarnos libremente. La Internet es tan libre como nosotros mismos. Sin embargo Assange expresa otro punto que merece mención, sobre la posibilidad de un poder “extremadamente agobiante, homogenizado, de una estructura totalitaria transnacional posmoderna con una complejidad increíble” (p. 159) o “una compleja interacción multipartidaria que ha surgido como resultado de varias élites en sus propios Estados-naciones elevándose juntos, desde sus respectivas bases poblacionales” (p. 160). Esto parece posible con el tiempo, aunque otros dirían que esos Estados son nada más vectores por el capital dentro de los cuales han creado practicas discursivas fuertemente agenciadas.

Es sorprendente que los rebeldes más rebeldes, que en muchas maneras han pagado un gran precio por sus creencias, al final del día no ofrezcan realmente nuevas posibilidades. Claro, está que la propuesta de Assange dé más transparencia digital a los poderosos y más clandestinidad a los no poderosos. Quizás la idea implícita más poderosa del libro es un alfabetismo en el que podamos entender cómo funcionan los soportes que usamos. Bajo ese modelo podríamos decidir qué queremos develar y comprender cómo funcionan fuerzas más grandes que nosotros dentro de nuestros aparatos. Assange ha dicho en varias ocasiones que el celular –y sobre todo el *smartphone*– manda millones de datos todos los días, a velocidades cada vez más rápidas, a bases donde nuestros comunicados son archivados. De esta manera es imaginable un mundo ciber, no en el sentido de que viajamos en el mundo digital, sino en el sentido de que todo lo que hacemos y escribimos, desde SMS a *e-mails*, estará disponible para los ‘poderosos’. Como suele decir Assange, “sólo falta que alguien tenga la llave para prender la máquina”. Lo que él no ve es que nosotros estamos cada vez más cerca de meter la llave por miedo.

Referencias

- Anderson, B. (1983, 2006). *Imagined Communities: Reflections on the Origin and Spread of Nationalism*. Nueva York: Verso.
- Assange, J. y Appelbaum, J. (2012). *Cypherpunk*. Digital: OR Books.
- Omri, M. (2013). "A Revolution of Dignity and Poetry". En: *Boundary 2: A Journal of Literature and Culture*, 40 (1), pp. 137-165.
- Sloterdijk, P. (2001). *Normas para el parque humano*. Madrid: Siruela.
- Virilio, P. (1996). *El ciber mundo, la política de lo peor*. Madrid: Cátedra.