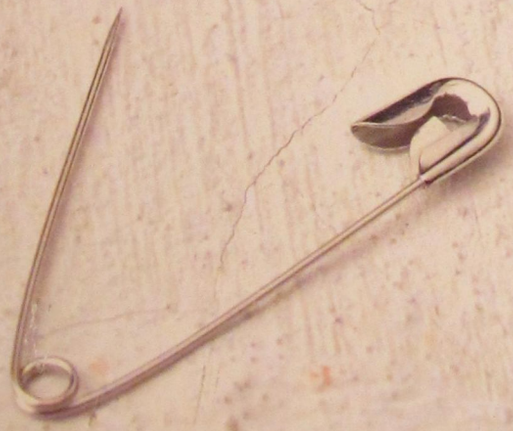
CRIPTOPUNKS

LA LIBERTAD Y EL FUTURO DE INTERNET

JULIAN ASSANGE

CON JACOB APPELBAUM
ANDY MÜLLER-MAGUHN
Y JÉRÉMIE ZIMMERMANN



TRILCE

CRIPTOPUNKS

LA LIBERTAD Y EL FUTURO DE INTERNET

CRIPTOPUNKS

LA LIBERTAD Y EL FUTURO DE INTERNET

JULIAN ASSANGE

con Jacob Appelbaum

Andy Müller-Maguhn

y Jérémie Zimmermann

traducción Nicolás Lerner

TRILCE

Esta obra ha sido coeditada por Ediciones Trilce (Montevideo),
Marea Editorial (Buenos Aires) y Lom ediciones (Santiago de Chile).

Título original: *Cypherpunks. Freedom and the Future of the Internet*
Primera edición 2012, publicada en los Estados Unidos por OR Books LLC, Nueva York

Durazno 1888
11200 Montevideo, Uruguay
tel. y fax: (598) 2412 77 22 y 2412 76 62
trilce@trilce.com.uy
www.trilce.com.uy

ISBN 978-9974-32-611-8
Primera edición: mayo 2013

CONTENIDO

¿QUÉ ES UN CRIPTOPUNK?

Los criptopunks abogan por el uso de la criptografía[1] y otros métodos similares como medios para lograr el cambio social y político. El movimiento, fundado a comienzos de la década de los noventa, fue especialmente activo durante las «guerras criptográficas»[2] de la década de los noventa y en la «primavera de internet»[3] de 2011. El término *cypherpunk*,[4] criptopunk en castellano, proviene de la unión de las palabras *cypher* (clave, cifra, código criptográfico) y *punk*, y se incorporó al Oxford English Dictionary en el año 2006.[5]

1 Término griego que significa «escritura secreta», o uso de la comunicación en clave.
2 Enfrentamientos entre los activistas criptopunks y otros que bregaban por el libre uso de la criptografía como *sofware* libre y la administración estadounidense que clasificó la criptografía como munición de guerra e intentó restringir su uso sin lograrlo. Actualmente hay una «segunda guerra criptográfica» en curso. (Véase nota 51).
3 Se refiere al vastísimo movimiento contra las ley SOPA y PIPA en los Estados Unidos. Dichas leyes provocaron la ira de considerables porciones de la comunidad en línea internacional y generaron una fuerte reacción de actores de la industria cuyos intereses están en una red libre y abierta. Véase la nota 77.
4 *Cypherpunk* en el original. Hemos optado por la traducción «criptopunk» debido a que ya está en uso. A pesar de no ser una traducción exacta expresa el sentido de la palabra inglesa.
5 Véase: <http://web.resorceshelf.com/go/resourceblog/ 43743>.

MÁS ALLÁ DEL LIBERTARISMO: PREFACIO PARA AMÉRICA LATINA

La lucha de WikiLeaks es una gesta compleja. En mi trabajo como periodista he luchado contra guerras y para que los grupos poderosos rindieran cuentas ante el pueblo.

Mediante esta labor, he llegado a comprender la dinámica del orden internacional y la lógica del imperio. He visto a países pequeños ser amedrentados y dominados por países más grandes o plagados de empresas extranjeras que los hacen tomar decisiones en detrimento propio. He visto el amordazamiento del deseo popular, elecciones compradas y vendidas, y las riquezas de países como Kenia robadas y rematadas entre plutócratas en Londres y Nueva York.

Estas experiencias me han formado como criptopunk. Me han aportado una sensibilidad respecto de los temas que se discuten en este libro, que es de especial interés para los lectores de América Latina. El libro no los examina en su totalidad, eso es para otro libro — para muchos otros libros—. Pero quisiera detenerme en estos temas y pedirles a los lectores que los tengan en mente durante la lectura del presente texto.

En los últimos años se ha visto el debilitamiento de las viejas hegemonías. Las poblaciones desde el Maghreb hasta el golfo Pérsico se han levantado ante tiranías para conseguir la libertad y la autodeterminación. Movimientos populares en Pakistán y Malasia prometen constituir un nuevo foco de fuerza en el escenario mundial. Mientras que América Latina ha comenzado a transitar un período muy esperado de soberanía e independencia tras siglos de dominio imperial. Cuando el sol se pone sobre las democracias occidentales, estos avances constituyen la esperanza de nuestro mundo. Viví en carne propia la nueva independencia y vitalidad de América Latina cuando Ecuador, la Alianza Bolivariana para los Pueblos de Nuestra América (ALBA), la Unión de Naciones Suramericanas (UNASUR) e incluso la Organización de los Estados Americanos (OEA) salieron en defensa de mis derechos luego de haber recibido asilo político.

La duradera lucha latinoamericana por la autodeterminación es importante porque marca el camino para que el resto del mundo avance hacia la libertad y la dignidad. Pero la independencia de América Latina

está aún en pañales. Los intentos desestabilizadores de Estados Unidos todavía son moneda corriente en la región, como ocurrió, no hace mucho, en Honduras, Haití, Ecuador y Venezuela.

Este es el motivo por el cual el mensaje criptopunk es de especial importancia para el público de América Latina. El mundo debe ser consciente del riesgo que la vigilancia[6] significa para América Latina y para el antiguo Tercer Mundo. La vigilancia estatal no solo es un problema para la democracia o para la gobernabilidad, sino que es un problema geopolítico. El control de toda una población por parte de poderes internacionales naturalmente amenaza la soberanía. Las sucesivas intervenciones en los asuntos de las democracias latinoamericanas nos han enseñado a ser realistas. Sabemos que los antiguos poderes coloniales usarán cualquier ventaja para impedir la consagración de la independencia de todo el continente.

Este libro debate sobre lo que ocurre cuando corporaciones estadounidenses como Facebook disponen de una penetración casi total en la población de un país entero, pero no se detiene en las cuestiones geopolíticas de fondo.

Haciendo una simple consideración geográfica se nos presenta un aspecto importante. Todo el mundo sabe que la geopolítica global está determinada por los recursos petroleros. El flujo del crudo determina quién domina, quién es invadido y quién es marginado de la comunidad global. El control físico de solo un segmento de un oleoducto ofrece un enorme poder geopolítico. Los gobiernos en esta posición pueden obtener enormes concesiones.

Entonces ocurre que, de un golpe, el Kremlin puede sentenciar a Europa del Este y Alemania a un invierno sin calefacción. Y la sola posibilidad de que Teherán construya un oleoducto que llege a India y a China alcanza como pretexto para la lógica belicosa de Washington.

Con el control de los cables de fibra óptica, por donde pasan los gigantes flujos de datos que conectan a la civilización mundial, ocurre lo mismo que con los oleoductos. Este es el nuevo juego: controlar la comunicación de miles de millones de personas y organizaciones.

No es secreto que, en lo referente a internet y a las comunicaciones telefónicas, todos los caminos desde y hacia América Latina pasan por Estados Unidos. La infraestructura de internet dirige gran parte del trá-

---

6 *Surveillance* en el original. A diferencia de «vigilancia» («Cuidado y atención exacta en las cosas que están a cargo de cada uno», DRAE) el término inglés implica la vigilancia de sospechosos para evitar o detectar crímenes. Tiene connotaciones de control social y represión. Es usado frecuentemente cuando esa vigilancia se realiza por medios tecnológicos. El *surveillance state* refiere a un Estado que desarrolla una vigilancia (control, espionaje) masiva de sus habitantes arriesgando su privacidad y los derechos humanos. A lo largo de toda la obra el término vigilancia debe ser comprendido con esa connotación de la palabra inglesa.

fico desde y hacia América Latina a través de cables de fibra óptica que físicamente atraviesan las fronteras de Estados Unidos. El Gobierno de Estados Unidos no ha mostrado muchos escrúpulos en transgredir su propia ley al interceptar estas líneas para espiar a sus propios ciudadanos. Y no existen las leyes que impidan espiar a ciudadanos extranjeros. Cada día, cientos de millones de mensajes de toda América Latina son devorados por las agencias de espionaje de Estados Unidos y almacenados para siempre en depósitos del tamaño de ciudades. Los aspectos geográficos relativos a la infraestructura de internet por lo tanto tienen consecuencias para la independencia y soberanía de América Latina.

El problema también trasciende la geografía. Muchos gobiernos y ejércitos latinoamericanos resguardan sus secretos con *hardware* criptográfico. Se trata de aparatos y programas que codifican y descodifican mensajes. Los Gobiernos adquieren estos equipos para mantener sus secretos a salvo, a menudo con un alto costo para el pueblo, porque le temen, con razón, a la interceptación estadounidense de sus comunicaciones.

Pero las compañías que venden estos costosos dispositivos gozan de lazos estrechos con la comunidad de inteligencia de Estados Unidos *(Intelligence Community)*.[7] Sus directores ejecutivos y funcionarios de alto rango son matemáticos e ingenieros de la NSA (sigla de *National Security Agency*, la Agencia de Seguridad Nacional de los Estados Unidos),[8] quienes capitalizan las invenciones que crearon para el estado de vigilancia. Estos dispositivos están con frecuencia deliberadamente violados con un propósito: no importa quién vaya a usarlos o cómo lo hará —las agencias estadounidenses pueden desencriptar la señal y leer los mensajes—.

Estos dispositivos son vendidos a América Latina y a otros países como una forma de proteger sus secretos, pero en realidad son una forma de robar esos secretos. Los gobiernos estarían más a salvo usando *software* criptográfico abierto desarrollado por criptopunks, cuyo código es abierto para que todo el mundo vea que no se trata de una herramienta de espionaje, y que está disponible al precio de una conexión a internet.

---

7 Coalición de 17 agencias gubernamentales del Poder Ejecutivo de los Estados Unidos que trabajan de manera independiente y que colaboran para recabar la información de inteligencia necesaria para conducir las relaciones internacionales y las actividades de seguridad nacional. Está dirigida por el director de la Inteligencia Nacional.

8 Agencia de inteligencia criptológica del Gobierno de los Estados Unidos. Ella forma parte del Departamento de Defensa. Es responsable de obtener y analizar información transmitida por cualquier medio de comunicación, y de garantizar la seguridad de las comunicaciones del Gobierno contra agencias similares de otros países, y conlleva la utilización del criptoanálisis. La agencia está dirigida por un oficial de tres estrellas (un teniente general o bien un vicealmirante). La NSA es un componente clave de la «Comunidad de Inteligencia» de Estados Unidos.

Mientras tanto, Estados Unidos está acelerando la próxima gran carrera armamentista. Los descubrimientos de los virus Stuxnet, Duqu y Frame, anuncian una nueva era de programas altamente complejos con finalidad destructiva concebidos por Estados poderosos para atacar a Estados más débiles. Su uso agresivo en un primer golpe contra Irán está dirigido para socavar los esfuerzos persas para conseguir la soberanía nacional, finalidad que va en contra de los intereses estadounidenses e israelíes en la región.

Había una época en la que el uso de los virus informáticos en tanto armas ofensivas era un mecanismo argumental en novelas de ciencia ficción. Ahora es una realidad global, estimulada por la conducta irresponsable de la administración Obama, en contraposición a la ley internacional. Otros Estados ahora harán lo propio, mejorando su capacidad ofensiva para alcanzar a Estados Unidos.

Estados Unidos no es el único culpable. En los últimos años, la infraestructura de internet en países como Uganda se ha visto enriquecida por la inversión directa china. Se reparten abultados préstamos a cambio de contratos africanos para que compañías chinas construyan la infraestructura de la red troncal que conecte escuelas, ministerios gubernamentales y comunidades al sistema de fibra óptica global.

El continente africano se está conectando también, pero con *hardware* suministrado por un país que aspira a ser una súper potencia internacional. ¿Será internet el camino para que África siga estando dominado en el siglo XXI? ¿Está convirtiéndose África una vez más en un espacio para la confrontación de los poderes mundiales?

Estos son solo algunos de los caminos por los que este libro trasciende la lucha por la libertad individual.

Los criptopunks originales, mis camaradas, eran mayormente libertarios. Nosotros buscábamos proteger la libertad individual de la tiranía estatal y la criptografía era nuestra arma secreta. Esto fue algo subversivo porque la criptografía entonces era propiedad exclusiva de los Estados, usada como armas en sus varias guerras. Al desarrollar nuestro propio *software* contra las superpotencias, y al divulgarlo a lo largo y ancho del mundo, conseguimos liberar y democratizar la criptografía. Esta fue una lucha verdaderamente revolucionaria, librada en las fronteras de la nueva internet. La ofensiva fue rápida y onerosa pero, aunque es una ofensiva aún en curso, el camino está allanado.

La criptografía no solo puede proteger las libertades de los individuos, sino la soberanía y la independencia de países enteros, la solidaridad entre grupos con una causa común, y el proyecto de una emancipación global. Puede ser usada no solo para luchar contra la

tiranía del Estado sobre el individuo, sino contra la tiranía del imperio sobre la colonia.

Este es un mensaje en el que creo con firmeza, y se encuentra escrito entre líneas a lo largo del presente texto aunque no esté debatido en gran detalle. Merece su propio libro, y lo tendrá cuando sea el momento adecuado y mi situación lo permita. Por ahora, espero que esto baste para llamar la atención de los lectores al respecto y para que lo tengan presente durante la lectura.

Julian Assange
enero de 2013

INTRODUCCIÓN: UN LLAMAMIENTO A LAS ARMAS CRIPTOGRÁFICAS

Este libro no es un manifiesto. No hay tiempo para eso. Este libro es una advertencia.

El mundo no está descendiendo sino que está cayendo hacia una nueva distopía transnacional. Este cambio de ritmo no ha sido debidamente reconocido por fuera del ámbito de la seguridad nacional, sino que ha estado oculto a raíz de su confidencialidad, complejidad y envergadura. Internet, nuestro mayor instrumento de emancipación, ha sido transformado en la más peligrosa herramienta del totalitarismo que hayamos visto. Internet es una amenaza para la civilización humana.

Estas transformaciones se han dado en silencio porque los que saben lo que está ocurriendo trabajan en la industria de la vigilancia mundial y no se sienten incentivados a alzar la voz. De seguir su propio curso, en pocos años, la civilización global pasará a ser una distopía posmoderna de vigilancia, de la cual solo los más dotados individuos podrán escapar. De hecho, es posible que ese momento haya llegado.

Si bien muchos escritores han ponderado el significado de internet para la civilización global, están equivocados. Están equivocados porque no tienen el sentido de la perspectiva que ofrece la experiencia directa. Están equivocados porque no han conocido al enemigo.

No hay descripción del mundo que sobreviva al primer contacto con el enemigo.

Nosotros hemos conocido al enemigo.

En los últimos seis años, WikiLeaks ha tenido conflictos con casi todos los Estados poderosos. Conocemos por adentro al nuevo estado de vigilancia porque hemos sondeado sus secretos. Lo conocemos desde el lugar de un combatiente porque hemos tenido que proteger a nuestra gente, nuestras finanzas y nuestras fuentes de información de él. Lo conocemos desde una perspectiva global porque tenemos personas, recursos e información en casi todos los países del mundo. Lo conocemos desde el punto de vista del tiempo porque hemos estado combatiendo este fenómeno durante años y lo hemos visto duplicarse y diseminarse, una y otra vez. Es un parásito invasivo, que engorda a costa de las sociedades que entran en contacto con internet. Está extendiéndose por todo el planeta, infectando a todos los Estados y pueblos a su paso.

¿Qué hay que hacer?

Hubo un tiempo, en un lugar que no era este ni aquel, en el que nosotros —los arquitectos y ciudadanos de la joven internet— hablábamos sobre el futuro de nuestro nuevo mundo.

Veíamos que las relaciones entre todas las personas estarían mediadas por nuestro nuevo mundo, y que la naturaleza de los Estados, definida por la forma en que la gente intercambia información, valores y fuerzas, cambiaría también.

Vimos que la fusión entre las estructuras estatales existentes e internet creaba la posibilidad de cambiar la naturaleza de los Estados.

Primero, recordemos que los Estados son sistemas a través de los cuales fluyen fuerzas coercitivas. Es posible que dentro de un Estado haya facciones que compitan por el apoyo ciudadano, lo que conduce al fenómeno de la superficie democrática, pero los fundamentos del Estado son aplicar y evitar, de modo sistemático, la violencia. La propiedad de la tierra, los bienes, la renta, los dividendos, los impuestos, las multas, la censura, los derechos de autor y las marcas registradas se hacen respetar todas so pena de la aplicación de violencia estatal.

La mayor parte del tiempo no somos conscientes siquiera de lo cerca que estamos de la violencia, porque todos hacemos concesiones para evitarla. Tal como marinero huele la brisa, nosotros rara vez nos detenemos a contemplar las tinieblas que apuntalan la superficie de nuestro mundo.

¿Cuál sería el mediador de la fuerza coercitiva en el nuevo espacio que genera internet?

¿Tiene sentido acaso formular esta pregunta? En este espacio etéreo, este espacio aparentemente platónico de flujo de ideas e informacion, ¿podría existir la noción de fuerza coercitiva? ¿Una fuerza capaz de modificar registros históricos, intervenir teléfonos, separar pueblos, convertir la complejidad en escombros y levantar murallas cual ejército de ocupación?

La naturaleza platónica de internet, los flujos de ideas e información, está envilecida por sus orígenes físicos. Sus pilares son cables de fibra óptica que se extienden a lo largo del suelo oceánico, satélites que giran sobre nuestras cabezas, servidores informáticos alojados en edificios en ciudades de Nueva York a Nairobi. Así como el soldado que dio muerte a Arquímedes con una mera espada, un grupo armado también podría tomar el control del máximo desarrollo de la civilización occidental, nuestro espacio platónico.

Abstraído del viejo mundo de átomos en bruto, el nuevo universo de internet anhelaba independizarse, pero los Estados y sus secuaces pasaron a dominar nuestro nuevo mundo —mediante el control de sus fundamentos físicos—. El Estado, cual ejército en torno a un pozo petrolero, o un agente aduanero exigiendo sobornos en la frontera, pronto aprendería a apuntalar su dominio del espacio físico para conseguir el control de nuestro espacio platónico. Este impediría la independencia que habíamos soñado, y luego, ocupando líneas

de fibra óptica y los alrededores de estaciones satelitales en tierra pasaría a interceptar en masa el flujo de información de nuestro nuevo mundo —su esencia misma— incluso cuando toda relación humana, económica y política se sumaba a él. El Estado como sanguijuela en las venas y arterias de nuestras nuevas sociedades devoraría toda relación expresada o comunicada, cada sitio Web visitado, cada mensaje enviado y cada idea *googleada*, para luego almacenar este conocimiento, miles de millones de interceptaciones al día —un poder inimaginable— en amplios depósitos ultrasecretos, para siempre. Luego pasaría a socavar una y otra vez este tesoro, el producto intelectual colectivo y privado de la humanidad, con algoritmos de búsqueda y detección de patrones cada vez más sofisticados, abultando el tesoro y maximizando el desequilibrio de poder entre los que interceptan y los interceptados. Y luego, el Estado plasmaría lo aprendido en el mundo físico, cómo comenzar guerras, perpetrar ataques con *drones*, manipular comités de la ONU y acuerdos de comercio y hacer favores a su vasta red de industrias, infiltrados y cómplices.

Pero descubrimos algo. Nuestra única esperanza contra la dominación total. Una esperanza que —con coraje, perspicacia y solidaridad— podríamos usar para resistir. Una propiedad extraña del universo físico en el que vivimos.

La codificación es parte del universo.

Es más fácil encriptar información que desencriptarla.

Vimos que podíamos usar esta extraña propiedad para diseñar las leyes de un nuevo mundo: abstraer nuestro espacio platónico de sus fundamentos básicos de satélites, cables submarinos y quienes los controlan. Fortalecer nuestro espacio detrás de un velo criptográfico. Crear nuevos territorios a los que no puedan acceder aquellos que controlan la realidad física, porque seguirnos en dichos espacios requeriría de recursos infinitos.

Y de esta manera, declarar nuestra independencia.

Los científicos del Proyecto Manhattan descubrieron que el universo posibilitaba la construcción de una bomba nuclear. Esta no era una conclusión obvia. Quizá las armas nucleares no estuviesen dentro de las leyes de la física. No obstante, las bombas atómicas y los reactores nucleares son parte del universo. Son fenómenos que el universo bendice, como la sal, el mar o las estrellas.

De manera similar, el universo, nuestro universo físico, cuenta con la propiedad que le permite a un individuo, o un grupo de individuos, de manera confiable, automática e incluso sin saberlo, cifrar algo de modo tal que ni todos los recursos ni toda la voluntad política de la mayor superpotencia sobre la Tierra puedan descifrarlo. Y los senderos de la codificación entre las personas pueden entramarse para crear regiones libres de la fuerza coercitiva del Estado exterior, libres de la interceptación en masa, libres del control estatal.

De esta manera, las personas pueden enfrentar su voluntad a la de una superpotencia totalmente movilizada y ganar. La criptografía es la materialización de las leyes de la física, y no sabe de las bravuconerías de los Estados, ni de las distopías de la vigilancia transnacional.

No es obvio que el mundo tuviera que transitar este camino. Pero el universo de algún modo consagra la codificación.

La criptografía es la forma más acabada de acción directa no violenta.

Si bien los Estados con armas de destrucción masiva pueden ejercer una violencia ilimitada sobre millones de individuos, una sólida criptografía hace que ningún Estado, por más que ejerza una violencia ilimitada, pueda violar el propósito de mantener secretos a resguardo.

Una criptografía sólida puede resistir la aplicación de violencia ilimitada. No hay cantidad de fuerza coercitiva que pueda resolver un problema matemático.

Pero, ¿podríamos tomar este extraño dato sobre el mundo y desarrollarlo para que constituya un pilar emancipador básico de la humanidad en el espacio platónico de internet? Y a medida que las sociedades se fusionan con internet, ¿se podría proyectar esa libertad en la realidad física para promover una redefinición del Estado?

Recordemos que los Estados son los sistemas que determinan dónde y cómo se aplica consistentemente la fuerza coercitiva.

La pregunta de cuánta fuerza coercitiva puede filtrarse al espacio platónico de internet desde el mundo físico queda respondida por los ideales de la criptografía y los criptopunks.

A medida que los Estados se fusionan con internet y el futuro de nuestra civilización deviene en el futuro de internet, estamos obligados a redefinir las relaciones de fuerza.

Si no lo hacemos, la universalidad de internet convertirá a la humanidad en una enorme red de vigilancia y control en masa.

Debemos dar la voz de alarma. Este libro es como un grito del centinela en la noche.

El 20 de marzo de 2012, estando bajo arresto domiciliario en el Reino Unido a la espera de ser extraditado, me reuní con tres amigos y compañeros de equipo con la idea de que quizás nuestras voces al unísono pudieran despertar la aldea. Debemos comunicar lo que hemos aprendido mientras todavía haya una posibilidad para que usted, el lector, entienda y actúe a partir de lo que está ocurriendo.

Es hora de tomar las armas de nuestro nuevo mundo, de luchar por nosotros y por nuestros seres queridos.

Nuestro deber es resguardar la autodeterminación donde podamos, contener la inminente distopía donde no podemos, y, si todo el resto fracasa, acelerar su autodestrucción.

Julian Assange
Londres, octubre de 2012

PARTICIPANTES DE LA DISCUSIÓN

JULIAN ASSANGE es el editor en jefe de WikiLeaks[9] y ha tenido un rol de visionario. Uno de los colaboradores originales de la lista de correos criptopunk,[10] ahora es uno de los más destacados exponentes de la filosofía criptopunk. Su trabajo en WikiLeaks le ha dado vigencia política al tradicional lema criptopunk: «privacidad para los pobres, transparencia para los poderosos». Su trabajo más visible pasa por un enérgico ejercicio de la libertad de expresión para forzar la transparencia y la responsabilidad a instituciones poderosas. Julian es además un incisivo crítico de la intrusión del Estado y las corporaciones en la vida privada de las personas. Además, es autor de numerosos proyectos de *software* acordes con la filosofía criptopunk, como strobe.c el primer *port-scanner*, el sistema de archivos Rubberhose de cifrado negable, y del código original para WikiLeaks.[11] De adolescente, fue uno de los primeros investigadores en materia de seguridad informática y de redes, previo a que la ley definiera algunos tipos de piratería como actividades criminales. Tiempo más tarde, en los noventa, fue activista y proveedor de servicios de internet en Australia. Además, Julian fue coautor de la historia del movimiento hacker internacional junto a Sulette Dreyfus, titulada *Underground*, sobre la cual se basó libremente la película *Underground: The Julian Assange Story*.[12]

---

9 WikiLeaks: <http://wikileaks.org>.

10 El movimiento de los *cypherpunks* tuvo su origen en un grupo informal de gente interesada en criptografía y en preservar la privacidad. Se relacionaron a través de una lista de correo electrónico con discusiones sobre criptografía y sus efectos en la sociedad, matemáticas, computación, política, filosofía, etcétera. La lista se inició en 1992 y tuvo su mayor actividad hacia 1997 (más de mil de participantes).

11 Para más información véase: «The Idiot Savants' Guide to Rubberhose», Suelette Dreyfus: <http://marutukku.org/current/src/doc/maruguide/t1.html> (consultado el 14 de octubre de 2012).

12 Para más información sobre el libro *Underground*, véase: <http://www.underground.book.net>. Para más información sobre la película *Underground: The Julian Assange Story* véase: <http://www.imdb.com/title/tt2357453/> (consultado el 21 de octubre de 2012).

JACOB APPELBAUM es programador de computación, fundador de Noisebridge en San Francisco y miembro del Chaos Computer Club de Berlín.[13] Es un investigador y promotor del Proyecto Tor, un sistema de libre acceso en línea para mantener el anonimato para que todas las personas resistan la vigilancia y eludan la censura en internet.[14] En la última década, se ha abocado a colaborar con activistas por el medio ambiente y los derechos humanos. Con este fin, ha publicado novedosas investigaciones sobre seguridad, privacidad y anonimato en una serie de campos que van desde la informática forense a la marihuana medicinal. Jacob cree que todo el mundo tiene el derecho a leer, sin restricción, y el derecho a expresarse libremente, sin excepción. En 2010, cuando Julian Assange no pudo dar una conferencia en Nueva York, Jacob dio la charla en su lugar. Desde entonces, él, sus amigos y su familia han sido hostigados por el Gobierno estadounidense, interrogados en aeropuertos, sometidos a cacheos abusivos mientras se los amenazaba de modo implícito con la inminencia de abusos por parte del personal penitenciario. Asimismo, sus equipos fueron confiscados y la Justicia estadounidense ordenó, de modo secreto, a Twitter, la entrega de toda la información relacionada a la cuenta de Jacob.

A Jacob no lo amedrentan estas medidas, él continúa librando batallas legales y sigue siendo un abierto defensor de la libertad de expresión y un manifiesto partidario de WikiLeaks.

ANDY MÜLLER-MAGUHN pertenece hace mucho al Chaos Computer Club en Alemania; fue miembro de su comité y vocero de dicha asociación.[15] Es uno de los cofundadores de European Digital Rights (Derechos Digitales Europeos) (EDRI), una ONG que vela por el cumplimiento de los derechos humanos en la era digital.[16] De 2000 a 2003 fue elegido por los usuarios de internet como el director europeo de la Corporación de Internet para la Asignación de Nombres y Números (ICANN, por sus iniciales en inglés), que es responsable de las políticas mundiales de cómo deben funcionar los «nombres y los números» en internet.[17] Es especialista en telecomunicaciones y vigilancia, trabajó

---

13 Noisebridge es un *hacker space* con sede en San Francisco, una organización proveedora de infraestructura para proyectos técnico-creativos, dirigido en colaboración por sus miembros: <https://www.noisebridge.net/wiki/Noisebridge>.
El Chaos Computer Club Berlin es la filial berlinesa del Chaos Computer Club, véase: <https://berlin.ccc.de/wiki/Chaos_Computer_Club_Berlin>.

14 Proyecto Tor: <https://www.torproject.org>.

15 El Chaos Computer Club es la mayor asociación de *hackers* de Europa. Sus actividades van desde estudios e investigaciones técnicas a campañas, eventos, publicaciones y asesoramiento político/normativo: <http://www.ccc.de>.

16 EDRI: <http://www.edri.org>.

17 ICANN: <http://www.icann.org>

como periodista en su proyecto buggedplanet.info[18] sobre la industria de la vigilancia. Andy trabaja en comunicaciones criptográficas y creó junto a otros una compañía llamada Cryptophone, que vende dispositivos de comunicaciones seguras a clientes privados y ofrece consultoría estratégica en el contexto de la arquitectura de redes.[19]

JÉRÉMIE ZIMMERMANN es cofundador y vocero del grupo de defensa ciudadana La Quadrature du Net, la más importante organización europea defensora de los derechos al anonimato en línea y generadora de conciencia sobre los ataques contra las libertades en línea a través de regulaciones legales.[20] Jérémie trabaja desarrollando herramientas para que el público participe de un debate abierto sobre cómo generar el cambio. Está más que nada involucrado en las batallas relativas a los derechos de propiedad intelectual,[21] el debate en torno a la neutralidad de la red y otros asuntos regulatorios que son cruciales para el futuro de una internet libre. Recientemente, su grupo La Quadrature du Net obtuvo una victoria histórica en la política europea, con una exitosa campaña contra el Acuerdo comercial anti-falsificación (ACTA, por sus iniciales en inglés) en el Parlamento Europeo. Poco después de participar en la discusión que forma la base de este libro, Jérémie fue detenido por dos agentes del FBI cuando estaba por salir de Estados Unidos, y fue interrogado sobre WikiLeaks.

NOTA DEL EDITOR

Para facilitar la comprensión de la temática de *Criptopunks*, cada participante en el diálogo original tuvo la oportunidad de elaborar, aclarar y poner notas a sus intervenciones. El orden del manuscrito editado respeta en general la dinámica de la discusión original.

Pueden verse en internet dos videos —doblados al castellano— grabados durante el intercambio de ideas entre Assange, Appelbaum, Müller-Maguhn y Zimmermann que refiere esta obra: "Assange y los criptopunks" parte I y II (<http://assange.rt.com/es/episodio-9--assange-y-los-criptopunks>).

---

18 buggedplanet: <http://buggedplanet.info>.
19 Cryptophone: <http://www.cryptophone.de>.
20 La Quadrature du Net: <http://www.laquadrature.net>.
21 Véase nota 77 más adelante.

NOTA SOBRE LOS VARIOS INTENTOS POR REPRIMIR A WIKILEAKS Y A LAS PERSONAS VINCULADAS AL PROYECTO

En varios puntos a lo largo de la siguiente discusión se hace referencia a los recientes episodios en la historia de WikiLeaks y sus esfuerzos de divulgación. Estos pueden resultar poco conocidos para los lectores que no estén familiarizados con la historia de WikiLeaks, de modos que se los resume al comienzo.

La misión de WikiLeaks es recibir datos de parte de informantes,[22] hacerlos públicos y luego defenderse contra los inevitables ataques legales y políticos. Es ya un hecho rutinario que Estados y organizaciones poderosas intenten eliminar las publicaciones de WikiLeaks, y en tanto último recurso de divulgación, WikiLeaks ha debido fortalecerse para resistir esta adversidad.

En 2010, WikiLeaks realizó su más famosa publicación hasta la fecha, revelando el sistemático abuso del secreto oficial por parte de los militares y el Gobierno estadounidense. Estas publicaciones son conocidas como *Asesinato colateral*, *Los diarios de la guerra de Afganistán* y *Cablegate*.[23] La respuesta ha sido una compaña conjunta y permanente por parte del Gobierno estadounidense y sus aliados para destruir WikiLeaks.

EL GRAN JURADO DE WIKILEAKS

Como consecuencia directa de lo publicado por WikiLeaks, el Gobierno de Estados Unidos lanzó una investigación criminal —que involucró a múltiples organismos— sobre Julian Assange, el personal, simpatizantes y presuntos socios de WikiLeaks. Se convocó a un Gran Jurado en Alexandria, Virginia, con el apoyo del Departamento de Justicia y el FBI, para investigar la posibilidad de presentar cargos, incluyendo conspiración bajo la Ley de Espionaje de 1917, contra Julian Assange y otros. Funcionarios de Estados Unidos han dicho que se trata de una investigación de una «escala y naturaleza sin prece-

22 En el original *whistleblower*: persona que revela fechorías desde dentro de una organización con el objetivo de detenerlas.

23 *Collateral Murder* (*Asesinato colateral*): <http://www.collateralmurder.com>. The Iraq War Logs (*Los registros de la guerra de Irak*): <http://wikileaks.org/irqThe Afghan>. War Diary (*Los diarios de la guerra en Afganistán*): <http://wikileaks.org/afgCablegate> (el *Cablegate*): <http://wikileaks.org/cablegate.html>.

dentes». En los procesos judiciales del Gran Jurado no hay juez o abogados de la defensa presentes. Desde entonces, en las audiencias del comité parlamentario se ha escuchado a miembros del Congreso de Estados Unidos sugerir que la Ley de Espionaje pueda ser usada como herramienta para perseguir a periodistas que «publicaran deliberadamente información filtrada» lo que sugiere que este enfoque está siendo adoptado en el sistema judicial estadounidense.[24]

Al momento de la publicación de este libro, la investigación sobre WikiLeaks seguía en curso.[25]

Varias personas fueron legalmente intimadas a aportar su testimonio. En autos del juicio a Bradley Manning, el soldado acusado de suministrarle información a WikiLeaks, aparece un archivo del FBI sobre la investigación a WikiLeaks que tiene más de 41.000 páginas, 8000 de las cuales refieren a Manning. Bradley Manning ha estado detenido sin un proceso judicial en su contra por más de 880 días. El Relator Especial sobre la Tortura de Naciones Unidas, Juan Méndez, formalmente halló que Bradley Manning había sido tratado de forma cruel e inhumana, lo que posiblemente calificara como tortura.[26]

LLAMADOS A ASESINAR A JULIAN ASSANGE Y CONSTITUCIÓN PÚBLICA DE GRUPOS OPERATIVOS CONTRA WIKILEAKS

La investigación del Gran Jurado no es la única fuente de ataques contra WikiLeaks. En diciembre de 2010, a raíz del Cablegate, varios políticos estadounidenses en actividad reclamaron el asesinato extrajudicial de Julian Assange, incluso mediante aviones no tripulados. Senadores de Estados Unidos calificaron a WikiLeaks como una «organización terrorista» y tildaron a Assange de «terrorista de alta tecnología» y de «combatiente enemigo» involucrado en una «guerra cibernética».[27]

---

24 «Congressional committee holds hearing on national security leak prevention and punishment», Reporters Committee for Freedom of the Press, 11 de julio de 2012: <http://www.rcfp.org/browse-media-law-resources/news/congressional-committee-holds-hearing-national-security-leak-prevent> (consultado el 21 de octubre de 2012).

25 Para más información sobre el Gran Jurado convocado en torno a WikiLeaks consultar la línea de tiempo de la periodista *freelance* Alexa O'Brien's: <http://www.alexaobrien.com/timeline_us_versus_manning_assange_wikileaks_2012.html> (consultado el 22 de octubre de 2012).

26 «El trato que Bradley Manning recibió fue cruel e inhumano, afirma el supervisor de casos de tortura de la ONU», *The Guardian*, 12 de marzo de 2012: <http://www.guardian.co.uk/world/2012/mar/12/bradley-manning-cruel-inhuman-treatment-un> (consultado el 24 de octubre de 2012).

27 «WikiLeaks: guilty parties "should face death penalty"», *Telegraph*, 1 de diciembre de 2010: <http://www.telegraph.co.uk/news/worldnews/wikileaks/8172916/WikiLeaks-guilty-parties-should-face-death-penalty.html> (consultado el 22 de octubre de 2012).

Previo a la publicación de *Los registros de la guerra de Irak* y el *Cablegate*, el Pentágono creó un equipo de 120 miembros llamado Grupo Operativo sobre WikiLeaks (WTF, por sus iniciales en inglés), dedicado a «tomar medidas» contra WikiLeaks. También hay en funcionamiento grupos operativos constituidos públicamente en el FBI, la CIA y el Departamento de Estado de los Estados Unidos.[28]

CENSURA DIRECTA

En un hecho de censura sin precedentes para una publicación periodística, el Gobierno estadounidense presionó a proveedores de servicios de internet para que suspendieran el servicio que le brindaban a WikiLeaks.org. El 1 de diciembre de 2010, Amazon retiró a WikiLeaks de sus servidores de almacenamiento, y el 2 de diciembre se interrumpió el servicio DNS que apuntaba al dominio WikiLeaks.org. Durante este período, WikiLeaks se mantuvo en línea gracias a una campaña de «espejado masivo», en la cual miles de partidarios de WikiLeaks copiaron el sitio Web, y alojaron su propia versión, distribuyendo las direcciones IP a través de las redes sociales.[29]

La administración Obama advirtió a los empleados federales que los materiales divulgados por WikiLeaks seguían siendo confidenciales —aunque estos estaban siendo publicados por algunas de las principales organizaciones de noticias del mundo incluyendo *The New York Times* y *The Guardian*—. Se informó a los empleados que acceder al material, ya sea en WikiLeaks.org o en el *The New York Times*, calificaría como una violación a la seguridad.[30] Agencias gubernamentales como la Biblioteca del Congreso, el Departamento de Comercio y el Ejército estadounidense bloquearon el acceso a los contenidos de WikiLeaks desde sus redes. La inhabilitación no se limitó al sector público. Empleados del Gobierno estadounidense advirtieron a instituciones académicas que aquellos estudiantes que aspirasen a tener una carrera en la función pública debían evitar el material divulgado por WikiLeaks en sus investigaciones y en sus actividades en línea.

---

28 CIA launches task force to assess impact of U.S. cables' exposure by WikiLeaks», *Washington Post*, 22 de diciembre de 2012: <http://www.washingtonpost.com/ wp-dyn/content/article/2010/12/21/AR2010122104599.html?hpid=topnews&sid=ST2010122105304> (consultado el 22 de octubre de 2012).

29 «WikiLeaks fights to stay online after US company withdraws domain name», *The Guardian*, 3 de diciembre de 2012: <http://www.guardian.co.uk/media/blog/2010/dec/03/wikileaks-knocked-off-net-dns-everydns> (consultado el 23 de octubre de 2012).

30 «Don't Look, Don't Read: Government Warns Its Workers Away From WikiLeaks Documents», *The New York Times*, 4 de diciembre de 2010: <http://www.nytimes.com/2010/12/05/world/05restrict.html?hp&_r=2&> (consultado el 23 de octubre de 2012).

CENSURA FINANCIERA: EL BLOQUEO BANCARIO

WikiLeaks se financia con donaciones de sus partidarios. En diciembre de 2010, importantes instituciones bancarias y financieras, incluyendo a VISA, MasterCard, PayPal y Bank of America, cedieron a la presión extraoficial de Estados Unidos para dejar de brindarle servicios financieros a WikiLeaks. Estas instituciones bloquearon las transferencias bancarias y toda donación realizada mediante las principales tarjetas de crédito. Si bien son instituciones estadounidenses, su omnipresencia en las finanzas mundiales impidió que donantes tanto en Estados Unidos como en el resto del mundo pudieran enviar dinero a WikiLeaks para apoyar sus actividades de divulgación.

El «bloqueo bancario», tal como se lo conoció, fue llevado a cabo por fuera de cualquier procedimiento judicial o administrativo y seguía vigente al momento de la publicación de este libro. WikiLeaks ha estado llevando adelante importantes casos judiciales en diferentes jurisdicciones de todo el mundo a fin de suspender el bloqueo, con algunas victorias preliminares, y procesos legales aún abiertos. Mientras tanto, se ha interrumpido la transferencia de ingresos a WikiLeaks lo que —debido a sus altos costos— lo obliga a funcionar con fondos de reserva desde hace ya casi dos años.

El bloqueo bancario es una confirmación del poder de control sobre las transacciones financieras entre terceros. Este directamente socava las libertades económicas de los individuos. Más allá de esto, la amenaza a la existencia que plantea para WikiLeaks ejemplifica una nueva e inquietante forma de censura económica global.[31]

Algunas personas presuntamente asociadas con WikiLeaks, junto a partidarios y al personal mismo de WikiLeaks, han tenido misteriosos problemas con sus cuentas bancarias —desde inconvenientes con los detalles de sus cuentas hasta el cierre total de las mismas.

HOSTIGAMIENTO A JACOB APPELBAUM Y JÉRÉMIE ZIMMERMANN

El 17 de julio de 2010, Julian Assange tenía previsto presentarse en la conferencia de *hackers* HOPE en la ciudad de Nueva York. Assange canceló y Jacob Appelbaum dio la charla en su lugar. Desde entonces, las autoridades han montado una campaña de hostigamiento contra Appelbaum y sus allegados. Appelbaum ha sido periódicamente detenido, inspeccionado, privado de acceso a un representante legal e interrogado en cruces fronterizos cada vez que entra o sale de Estados Unidos. Su equipamiento ha sido incautado y sus derechos fueron vulnerados, episodio durante el cual fue amenazado de otras

31 «Banking Blockade», WikiLeaks: <http://www.wikileaks.org/Banking-Blockade.html> (consultado el 22 de octubre de 2012

violaciones de sus derechos. Su detención y hostigamiento ha involucrado a docenas de agencias de Estados Unidos, desde el Departamento de Seguridad Interior, el Servicio de Inmigración y Control de Aduanas al Ejército de los Estados Unidos. Estas detenciones llegaron a incluir la prohibición del uso del sanitario como método para forzar su voluntad. Durante todo esto, Appelbaum nunca ha sido acusado o informado por el Gobierno sobre los motivos de su hostigamiento.[32]

A mediados de junio de 2011, cuando se aprestaba a abordar un avión en el aeropuerto Dulles de Washington, Jérémie Zimmermann fue detenido por dos agentes que dijeron ser del FBI. Los agentes lo interrogaron sobre WikiLeaks y amenazaron con arrestarlo y enviarlo a prisión.

Appelbaum y Zimmermann están en la larga lista de amigos, partidarios o presuntos socios de Julian Assange quienes han sido objeto de hostigamiento y vigilancia por parte de las agencias de Estados Unidos, una lista que incluye a abogados y periodistas en ejercicio de sus actividades profesionales.

DECOMISO SIN ORDEN JUDICIAL DE REGISTROS ELECTRÓNICOS Y EL «CASO DEL EMPLAZAMIENTO A TWITTER»

El 14 de diciembre de 2010, Twitter recibió un «emplazamiento administrativo» de parte del Departamento de Justicia de Estados Unidos mediante el cual se le ordenaba presentar toda información que pudiese ser relevante para una investigación sobre WikiLeaks. El emplazamiento fue lo que se denomina una «orden 2703(d)», con relación a una sección de la Ley de Comunicaciones Almacenadas. Bajo esta ley, el Gobierno estadounidense se arroga la autoridad de forzar la entrega de registros electrónicos de comunicaciones privadas sin necesidad de que un juez emita una orden de allanamiento —sorteando efectivamente las protecciones de la Cuarta Enmienda frente al registro e incautación arbitrarios—.

El emplazamiento buscaba nombres de usuarios, registros de correspondencia, direcciones, números telefónicos, detalles de cuentas bancarias y números de tarjetas de crédito de cuentas y personas presuntamente asociadas con WikiLeaks, incluyendo a Jacob Appelbaum, la diputada islandesa Birgitta Jonsdottir, el empresario y pio-

---

32 Se recomienda la lectura del relato que Jacob escribió sobre sus detenciones. Véase: «Air Space—a trip through an airport detention center», boingboing, 31 de octubre de 2011: <http://boingboing.net/2011/10/31/air-space-a-trip-through-an-ai.html>. También es importante una entrevista con Jacob sobre las detenciones publicada por *Democracy Now*. «National Security Agency Whistleblower William Binney on Growing State Surveillance», *Democracy Now*, April 20, 2012: <http://www.democracynow.org/2012/4/20/exclusive_national_security_agency_whistleblower_william> (consultados el 23 de octubre de 2012).

nero de internet holandés Rop Gonggrijp y el mismo WikiLeaks. Según los términos del emplazamiento, Twitter tenía prohibido informarles de la existencia de la requisitoria. Sin embargo, Twitter apeló con éxito la cláusula de silencio obligatorio y defendió su derecho a informarles a los usuarios que se estaba solicitando sus registros.

Cuando se los notificó del emplazamiento a Twitter, el 26 de enero de 2011, Appelbaum, Jonsdottir y Gonggrijp, representados por Kecker y Van Nest, la Unión Estadounidense por las Libertades Civiles y la Fundación Electronic Frontier, ordenaron a sus abogados que presentaran una moción conjunta para anular la orden. Este se ha dado a conocer como el «caso del emplazamiento a Twitter».[33] El abogado de Appelbaum presentó más adelante una moción solicitando acceso a los expedientes judiciales secretos de los intentos del Gobierno por recabar sus datos personales a través de Twitter y otras compañías. Ambas mociones fueron denegadas por parte de un magistrado estadounidense el 11 de marzo de 2011. Los demandantes apelaron.

El 9 de octubre de 2011 el *Wall Street Journal* reveló que el proveedor de correo electrónico de California Sonic.net también había recibido un emplazamiento en la que se le exigían los datos de Jacob Appelbaum. Sonic litigó la orden del Gobierno y perdió, pero consiguió el permiso para informar de que había sido forzado a entregar la información de Appelbaum. El *Wall Street Journal* informó además que Google había recibido una orden similar, pero no dejó en claro si Google había objetado la medida o no.[34]

El 10 de noviembre de 2011, un juez federal falló en contra de Appelbaum, Jonsdottir y Gonggrijp, resolviendo que Twitter debía entregarle su información al Departamento de Justicia.[35] El 20 de enero de 2012, los demandantes nuevamente apelaron la negativa de revelar los emplazamientos que se les podrían haber enviado a otras compañías además de Twitter.[36] Al momento de la publicación del presente libro, el caso seguía abierto.

---

33 El caso es oficialmente conocido como In the Matter of the 2703(d) Order Relating to Twitter Accounts: Wikileaks, Rop_G IOERROR y BirgittaJ.

34 «Secret orders target email», *Wall Street Journal*, 9 de octubre de 2011: <http://online.wsj.com/article/SB10001424052970203476804576613284007315072.html> (consultado el 22 de octubre de 2012).

35 «Twitter Ordered to Yield Data in WikiLeaks Case», *The New York Times*, 10 de noviembre de 2011: <https://www.nytimes.com/2011/11/11/technology/twitter-ordered-to-yield-data-in-wikileaks-case.html?_r=1> (consultado el 22 de octubre de 2012),

36 «ACLU & EFF to Appeal Secrecy Ruling in Twitter/WikiLeaks Case», comunicado de prensa de la Fundación Electronic Frontier, 20 de enero de 2012: <https://www.eff.org/press/releases/aclu-eff-appeal-secrecy-ruling-twitterwikileaks-case> (consultado el 22 de octubre de 2012).

UNA MAYOR COMUNICACIÓN *VERSUS* UNA MAYOR VIGILANCIA[37]

JULIAN: Si nos retrotraemos a comienzos de los noventa, cuando surgió el movimiento criptopunk en respuesta a las restricciones estatales a la criptografía, mucha gente esperaba que el poder de internet posibilitara mantener comunicaciones libres y sin censura, comparado con lo que ocurría con los medios tradicionales. Pero los criptopunks siempre vieron que, de hecho, esto traía aparejado también el poder de vigilar todas las comunicaciones que existían. Ahora nos encontramos ante la disyuntiva de una mayor comunicación *versus* una mayor vigilancia. Una mayor comunicación significa que tienes un plus de libertades con relación a quienes están tratando de controlar las ideas y generar consensos, y una mayor vigilancia significa exactamente lo opuesto.

El control es mucho más evidente ahora que cuando la vigilancia era realizada «en volumen» solo por los estadounidenses, los británicos y los rusos y algún que otro Gobierno como el suizo o el francés. Ahora es llevado a cabo por todos o casi todos los Estados debido a la comercialización de tecnología de vigilancia masiva. Y se está dando de forma totalizadora, porque la gente está volcando todas sus ideas políticas, sus comunicaciones familiares y sus amistades a internet. De modo que no solo se da una mayora vigilancia de una comunicación existente, sino que se trata de una comunicación mucho mayor. Y no solo es un incremento en el volumen de la comunicación; es un incremento en los tipos de comunicación. Todos estos nuevos tipos de comunicación que anteriormente habrían sido privados ahora están siendo interceptados en masa.

Se está librando una batalla entre el poder que representa esta información recabada desde adentro por estos ocultos poderes estatales que están empezando a gestarse, que intercambian entre sí, y que desarrollan conexiones entre sí y con el sector privado, *versus* la cada vez más numerosa gente común muñida de internet como herramienta colectiva para que la humanidad se hable a sí misma.

Quiero pensar cómo presentar nuestras ideas. El gran problema que he tenido, por estar inmerso en la vigilancia estatal y por conocer cómo

37 Véase la nota 6.

se ha desarrollado la industria de la seguridad transnacional en los últimos veinte años, es que estoy demasiado familiarizado con ello y por ende no puedo ver esto desde una perspectiva neutral. Pero ahora nuestro mundo es el mundo de todos, porque todos han volcado lo más profundo de sus vidas a internet. Debemos comunicar de algún modo lo que sabemos mientras aún podamos.

ANDY: Sugiero no ver esto desde el punto de vista del ciudadano sino desde el punto de vista de las personas en el poder. El otro día estaba en una conferencia extraña en Washington y conocí a unos muchachos con identificación de la embajada alemana. Me acerqué a ellos y dije: «Ah, son de la embajada alemana», y ellos dijeron: «Eh, no exactamente de la embajada, somos de un lugar cerca de Múnich». Resultó que eran del Departamento de Inteligencia Internacional y durante la cena les pregunté: «Entonces, ¿cuál es el objeto de la confidencialidad?». Ellos me respondieron: «Bueno, se trata de frenar los procesos para poder controlarlos mejor». Ese es el meollo de este tipo de tareas de inteligencia, frenar un proceso entorpeciendo la capacidad de la gente para comprenderlo. Declarar ciertas cosas como confidenciales significa limitar la cantidad de personas que tienen el conocimiento y por lo tanto la capacidad para afectar el proceso.

Si piensas en internet desde la perspectiva de las personas en el poder, los últimos veinte años han sido aterradores. Ellos ven internet como una enfermedad que afecta su capacidad para definir la realidad, para definir lo que está sucediendo, que luego es usado para definir lo que la gente sabe sobre lo que está ocurriendo y su capacidad para interactuar con dicha realidad. Si pensamos por ejemplo en Arabia Saudita, donde por algún accidente histórico los líderes religiosos y los dueños de gran parte del país son las mismas personas, su interés por el cambio es casi nulo. O negativo, tal vez. Ellos seguramente ven internet como una enfermedad y les dicen a sus asesores: «¿Tienes algún remedio contra esto que anda dando vueltas? Necesitamos estar inmunes si esto infecta nuestro país, si internet se propaga». Y la respuesta es la vigilancia masiva. Es decir, «Necesitamos controlarlo en su totalidad, necesitamos filtrarlo, necesitamos saber todo lo que hacen». Y eso es lo que ha ocurrido en los últimos veinte años. Hubo enormes inversiones en vigilancia porque las personas en el poder temían que internet pudiese afectar su forma de gobierno.

JULIAN: Y, sin embargo, a pesar de esta vigilancia a gran escala, la comunicación masiva ha permitido que millones de personas pudiesen llegar a un rápido consenso. Si puedes pasar muy rápidamente de una situación de normalidad a una nueva situación de consenso masivo, aunque es posible que el Estado vea este desarrollo, no tendrá suficiente tiempo para formular una respuesta efectiva.

Dicho esto, en El Cairo se organizó en 2008 una protesta a través de Facebook. Esta tomó por sorpresa al Gobierno de Mubarak, y en consecuencia estas personas fueron identificadas a través de Facebook.[38] La primera página de un manual, uno de los documentos más importantes usados en la revolución egipcia decía: «No usar Twitter o Facebook» para distribuir el manual, y la última página decía «No usar Twitter o Facebook» para distribuir el manual.[39] Sin embargo, muchos egipcios usaron Twitter y Facebook. Pero la razón por la que sobrevivieron es que la revolución fue exitosa. Si no hubiese tenido éxito, entonces esas personas habrían estado en una posición muy delicada. Y no olvidemos que bien en un principio el presidente Mubarak cortó la conexión a internet en todo Egipto. En realidad, resulta dudoso si el apagón de internet facilitó la revolución o la perjudicó. Algunas personas piensan que la facilitó, porque la gente tuvo que salir a la calle para obtener información sobre lo que estaba aconteciendo, y una vez que estás en la calle, estás en la calle. Y la gente se vio directamente afectada porque sus teléfonos celulares y su acceso a internet no funcionaban.

De modo que si va a ser exitosa, tiene que haber una masa crítica, tiene que suceder rápidamente y tiene que ganar, porque si no gana la misma infraestructura que posibilita que se desarrolle un rápido consenso será usada para identificar y aislar a todas las personas involucradas en generar dicho consenso.

Ese fue el caso de Egipto el cual, sí era un aliado de Estados Unidos, pero que no es parte de la alianza angloparlante de Estados Unidos, el Reino Unido, Australia, Nueva Zelanda y Canadá. Ahora, en cambio, tratemos de imaginar la revolución egipcia comenzando en Estados Unidos: —¿qué ocurriría con Facebook y Twitter? Serían in-

---

38 Se trató de la protesta contra la represión de la huelga de los trabajadores textiles de Mahalla al-Kobra. Poco antes de la huelga, se conformó el grupo de Facebook «Movimiento Juvenil 6 de abril» (April 6 Youth Movement), creado para alentar a los egipcios a realizar protestas en El Cairo y otras ciudades para que coincida con la medida de fuerza en Mahalla. Las protestas no salieron como fueron planeadas, y los administradores del grupo de Facebook, Esraa Abdel Fattah, Ahmed Rashid y Ahmed Maher fueron arrestados junto a otros. Maher fue torturado para que revelara su contraseña de Facebook. El Movimiento Juvenil 6 de abril pasó a desempeñar un rol importante en la revolución egipcia de 2011. Véase «Cairo Activists Use Facebook to Rattle Regime», Wired, 20 de octubre de 2008: <http://www.wired.com/techbiz/startups/magazine/16-11/ff_facebookegypt?currentPage=all> (consultado el 23 de octubre de 2012).

39 *How to Protest Intelligently* (*Cómo protestar con inteligencia*), de autores anónimos, distribuido al comienzo del levantamiento de dieciocho días que derrocó al presidente Mubarak: <http://www.itstime.it/Approfondimenti/EgyptianRevolutionManual.pdf>. Fragmentos del documento fueron traducidos al inglés y publicados como *Egyptian Activists' Action Plan: Translated* (*Plan de acción de los activistas egipcios*), Atlantic, 27 de enero de 2011: <http://www.theatlantic.com/international/archive/2011/01/egyptian-activists-action-plan-translated/70388> (consultados el 23 de octubre de 2012).

tervenidas por el Estado. Y si la revolución no tuviese éxito estas serían investigadas a fondo, tal como ocurre ahora, por la CIA y el FBI, en busca de detalles de los principales participantes.

JÉRÉMIE: Es difícil disociar la vigilancia del control. Necesitamos atender ambas cuestiones. Eso me interesa más: el control sobre la red, ya sea por parte de los Gobiernos o de las corporaciones.

JACOB: Pienso que está bastante claro que la censura en términos generales es un subproducto de la vigilancia, ya sea que se trate de la autocensura o de censura realmente técnica, y considero que una manera importante de transmitirle esto a la gente común es haciéndolo de una forma no técnica. Por ejemplo, si construyéramos carreteras del modo en que construimos la red, cada carretera tendría que tener cámaras de vigilancia y micrófonos a los que no pudiese acceder nadie más que la Policía..., o alguien que se haya hecho pasar exitosamente por policía.

JULIAN: Están llegando a eso en el Reino Unido, Jake.

JACOB: Si construyes una carretera no hay ningún requerimiento que diga que cada centímetro pueda ser vigilado a la perfección por una tecnología que solo está disponible para un grupo secreto de personas. Explicarle a la gente común que es así como estamos construyendo carreteras en internet y esperar que use dichas carreteras, eso es algo que la gente común puede comprender cuando se dan cuenta de que los constructores originales de la carretera no siempre tendrán el control.

ANDY: Pero algunas personas ni siquiera construyen carreteras sino un jardín, e invitan a todos a desnudarse. ¡Ahora estamos hablando de Facebook! Es una idea comercial para que la gente revele su información con comodidad.

JACOB: Exacto. A la gente se la recompensaba por estar en la Stasi —la seguridad estatal de la antigua Alemania Oriental— y a la gente se la recompensa por participar de Facebook. Solo que en Facebook la gente es recompensada con créditos sociales —acostarse con su vecino— en lugar de percibir una remuneración de forma directa. Y es importante relacionarlo con el aspecto humano, porque no se trata de tecnología, se trata de ejercer control a través de la vigilancia. Es el Panóptico perfecto de algún modo.[40]

JULIAN: Me interesa mucho la filosofía de la técnica. La técnica no solo implica un dispositivo tecnológico sino, digamos, un consenso mayori-

---

40 El Panóptico fue una prisión diseñada por el filósofo Jeremy Bentham en 1787, concebida de modo tal que un solo guardia pudiese tener a todos los prisioneros en su campo visual con el fin de vigilarlos de manera encubierta. Jeremy Bentham (editado por Miran Bozovic), *The Panopticon Writings*, (Verso, 1995), disponible en internet en: <http://cartome.org/panopticon2.htm> (consultado el 22 de octubre de 2012).

tario en un directorio o en la estructura de un Parlamento: es la interacción sistematizada. Por ejemplo, me parece que los sistemas feudales derivan de la técnica de los molinos. Una vez centralizados los molinos, lo que insumió enormes inversiones y cuyo control efectivo pasó a ser más fácil de implementar en términos físicos, resultó bastante natural que se dieran relaciones feudales como resultado. Parece que con el paso del tiempo hemos desarrollado técnicas cada vez más sofisticadas. Algunas de estas técnicas pueden ser democratizadas; pueden llegarles a todos. Pero en su mayoría —debido a su complejidad— son técnicas que se gestan como resultado de organizaciones fuertemente interconectadas como Intel Corporation. Tal vez la tendencia subyacente en la técnica implica la sucesión de distintos períodos, el del descubrimiento de la técnica, el de la centralización de la técnica y el de la democratización de la técnica: cuando el conocimiento de cómo hacerlo surge en la próxima generación educada. Sin embargo, creo que la tendencia general en la técnica es la centralización del control en manos de aquellas personas que controlan los recursos físicos de las técnicas.

El ejemplo más acabado de eso sería un fabricante de semiconductores que necesita tal orden que hasta el aire en la planta de producción debe ser puro, y los miles de operarios deben usar cofias para evitar que el más ínfimo trozo de piel y el más mínimo cabello contaminen el proceso de ensamblaje de semiconductores, un proceso extremadamente complicado de múltiples etapas. Y existen literalmente millones de horas de investigación en manos de los fabricantes de semiconductores. Si estas se popularizaran —lo que ya ocurre—, y estas apuntalaran internet, entonces la liberación de internet tendría como base la producción de semiconductores. Y quien tenga el control físico de la producción de semiconductores sería capaz de obtener enormes concesiones.

Entonces, la economía de mercado neoliberal, transnacional, moderna y globalizada es lo que apuntala la revolución de las comunicaciones de alta tecnología y la libertad que hemos obtenido de esta. Se trata, en efecto, del apogeo de dicha revolución. Es el máximo nivel que la economía moderna neoliberal globalizada puede alcanzar en términos de logro tecnológico. Internet está apuntalada por interacciones comerciales extremadamente complejas entre fabricantes de fibra óptica, productores de semiconductores, compañías mineras que extraen los materiales necesarios, todos los lubricantes financieros que hacen funcionar el negocio, los tribunales que velan por la propiedad privada, etcétera. De modo que realmente se encuentra en la cima de la pirámide de todo el sistema neoliberal.

ANDY: En cuanto a la técnica, cuando Johannes Gutenberg inventó la imprenta, estuvo prohibida en algunas partes de Alemania y así fue como se diseminó por todo el país, porque cuando estaba prohibida en

una zona era trasladada a otra jurisdicción.[41] No lo estudié en detalle pero lo que sé es que afectó los intereses de la Iglesia católica porque rompió su monopolio de la impresión de libros, y cada vez que había problemas con la ley la imprenta era llevada a un lugar donde no estuviese prohibida. De algún modo esto ayudó a su difusión.

El caso de internet, me parece, fue levemente diferente porque por un lado están las máquinas que pueden ser usadas como instalaciones de producción, categoría en la que incluso entraba la Comodore 64, ya que la mayoría de las personas la usaba para otros propósitos.

JULIAN: Entonces, con cada pequeña máquina que tenías se podía ejecutar tu propio *software*.

ANDY: Sí. Y también se la podía usar para difundir ideas. Pero, por otro lado, filosóficamente, tal como dijo John Gilmore —uno de los fundadores de la Fundación Electronic Frontier con sede en Estados Unidos— a principios de los noventa, cuando internet adquirió un alcance mundial: «La red interpreta la censura como daño y la elude».[42] Como sabemos hoy, esa afirmación condensaba una interpretación técnica con una visión optimista del impacto, una suerte de expresión de deseo y un tipo de profecía autocumplida.

JULIAN: Pero fue lo que ocurrió con Usenet, un sistema de correo electrónico muchos-a-muchos, si quieres, que empezó hace unos treinta años. Para explicar Usenet, sencillamente, imaginen que no hay diferencia entre las personas y los servidores y cada persona opera su propio servidor Usenet. Uno escribe algo, y se lo pasa a una persona o dos. Ellos (automáticamente) verifican si lo tienen. Si no lo tienen todavía, lo reciben y se lo envían a todas las personas con las que estén conectadas. Y así sucesivamente. Y de esta manera el mensaje pasa por todos y todo el mundo recibe una copia. Si alguna persona comete algún acto de censura es ignorada, no hace mucha diferencia. El mensaje se propaga de cualquier modo entre las personas que no son censores. Gilmore estaba refiriéndose a Usenet, no estaba hablando de internet. Tampoco estaba hablando sobre páginas Web.

ANDY: Si bien eso es técnicamente correcto, la interpretación de sus palabras y su impacto a largo plazo iba a hacer que algunas personas se pensaran a sí mismas como internet. La gente dijo: «Bueno, existe la

---

41 Johannes Gutenberg (1398-1468) fue un herrero alemán que inventó un tipo de impresión mecánica móvil, un invento que dio origen a algunas de las más significativas transformaciones sociales en la historia. La invención de la imprenta es la analogía histórica más cercana a la creación de internet.

42 John Gilmore es uno de los criptopunks originales, el fundador de la Fundación Electronic Frontier y un defensor de las libertades civiles. La frase citada por Andy apareció por primera vez en: «First Nation in Cyberspace», *Revista Time*, 6 de diciembre de 1993. Véase el sitio de John Gilmore: <http://www.toad.com/gnu> (consultado el 22 de octubre de 2012).

censura, vamos a evitarla», frente a lo que un político sin conocimientos técnicos pensaría: «Caramba, existe una nueva tecnología que limita nuestro control sobre la esfera informática». Entonces pienso que Gilmore —quien fue uno de los primeros ideólogos del criptopunk—, hizo un gran trabajo marcando el camino, lo cual inspiró toda una tendencia cripto-anarquista de contar con una forma propia de comunicación anónima sin temor a ser rastreado.

JÉRÉMIE: Yo veo una diferencia respecto de lo que describimos como la difusión de la tecnología, porque en el caso del molino y la imprenta uno debía ver un ejemplar para comprender cómo funcionaba, mientras que ahora la tecnología incluye cada vez más control. El control viene incorporado. Si observas una computadora moderna, en la mayoría de los casos ni siquiera puedes abrirla para conocer todos sus componentes. Y todos los componentes se encuentran dentro de pequeños compartimentos —uno no puede saber qué es lo que están haciendo—.

ANDY: ¿Debido a la complejidad?

JÉRÉMIE: Debido a la complejidad y también a que la tecnología en sí no está pensada para ser entendida. Ese es el caso del *software* propietario.[43] Cory Doctorow lo describe en su artículo «The War on General-Purpose Computing» («La guerra contra la computación de propósito múltiple»).[44] Con una computadora en tanto dispositivo genérico puedes hacer cualquier cosa. Puedes procesar cualquier información en tanto *input*, y transformarlo en cualquier cosa como *output*. Y cada vez más construimos dispositivos que son computadoras de uso general pero que están limitados a ser solo GPS o teléfonos o reproductores de mp3. Estamos construyendo más y más máquinas con controles incorporados, para prohibirle al usuario hacer determinadas cosas.

JULIAN: Se trata de control incorporado para impedir que la gente entienda la tecnología y haga algo diferente a lo que el fabricante quiso, pero ahora la situación es peor, porque los dispositivos están conectados a la red.

JÉRÉMIE: Sí, puede tener la función de vigilancia del usuario y de sus datos. Este es el motivo por el cual el *software* libre es tan importante para una sociedad libre.

---

43 «Los *softwares* propietarios son cualquier tipo de sistema, herramienta o proceso técnico que esté desarrollado por y para una entidad comercial específica. Usualmente se considera que las ideas presentadas y desarrolladas por los empleados son propiedad del empleador, permitiéndoles que de este modo califiquen como *software* propietario.» Definición extraída de wiseGEEK: <http://www.wisegeek.com/what-is-proprietary-technology.htm> (consultado el 22 de octubre de 2012).

44 Cory Doctorow, «The coming war on general-purpose computing», boingboing, 10 de enero de 2012 (basado en el discurso de apertura pronunciado en el Chaos Computer Congress, diciembre de 2011): <http://boingboing.net/2012/01/10/lockdown.html> (consultado el 15 de octubre de 2012).

ANDY: Estoy totalmente de acuerdo con que necesitamos la máquina de uso general, pero esta mañana cuando estaba tratando de volar hacia aquí desde Berlín, el avión abortó el despegue —es la primera vez que me sucede—. El avión fue hasta un costado y el capitán dijo: «Damas y caballeros, hemos tenido una falla en el sistema eléctrico así que decidimos apagar y reiniciar el sistema». Yo pensaba: «Mierda, suena como el reinicio de Windows, Control+Alt+Delete —¡tal vez funcione!». Entonces, en realidad, no estaría tan mal que un avión sea una máquina de propósito único que solo haga lo que tienen que hacer y lo haga muy bien. Si estoy sentado a bordo de una máquina voladora no quiero que los pilotos se distraigan jugando al Tetris o tengan Stuxnet o algo por el estilo.[45]

JÉRÉMIE: El avión no procesa tus datos personales por su cuenta, no tiene control sobre tu vida.

ANDY: Bueno, una máquina voladora sí tiene control sobre mi vida durante algún tiempo.

JACOB: Lo que mejor describe el argumento de Cory, me parece, es decir que no hay más autos, no hay más aviones, no hay más audífonos, sino que hay computadoras con ruedas, computadoras con alas y computadoras que te pueden ayudar a oír. Y parte de esto no tiene que ver con si son o no computadoras de propósito único, sino si podemos o no verificar que hacen lo que dicen que hacen, y si podemos o no comprender cuán bien lo hacen. A menudo la gente trata de sostener que tiene el derecho de poner eso bajo llave y mantenerlo en secreto, y hace computadoras complejas o hace que sea legalmente difícil comprenderlas. En realidad, eso es peligroso para la sociedad porque sabemos que la gente no siempre actúa teniendo en cuenta el bienestar común, y también sabemos que la gente comete errores —no de forma maliciosa— y poner estas cosas bajo llave es muy peligroso en

---

45 Stuxnet es un gusano informático altamente sofisticado que se cree que fue desarrollado por Estados Unidos e Israel para atacar equipos Siemens presuntamente usados por Irán para enriquecer uranio. Para acceder a un resumen sobre Stuxnet, véase Wikipedia: <http://en.wikipedia.org/wiki/Stuxnet>.
Véase también, «WikiLeaks: US advised to sabotage Iran nuclear sites by German thinktank», *The Guardian*, 18 de enero de 2011: <http://www.guardian.co.uk/world/2011/jan/18/wikileaks-us-embassy-cable-iran-nuclear>.
WikiLeaks realizó uno de los primeros informes sobre los efectos que según se cree ahora fueron resultado de Stuxnet —el accidente nuclear en las instalaciones nucleares Natanz en Irán. Véase, «Serious nuclear accident may lay behind Iranian nuke chief's mystery resignation», WikiLeaks, 17 de julio de 2009: <http://wikileaks.org/wiki/Serious_nuclear_accident_may_lay_behind_Iranian_nuke_chief%27s_mystery_resignation>.
La evidencia de la compañía de inteligencia global Stratfor, filtrada por WikiLeaks, da a entender la participación israelí. Véase Email ID 185945, The Global Intelligence Files: <http://wikileaks.org/gifiles/docs/185945_re-alpha-s3-g3-israel-iran-barak-hails-munitions-blast-in.html> (todos los *links* fueron consultados el 16 de octubre de 2012).

una serie de niveles, entre los que se cuenta que todos somos imperfectos. Eso es un hecho. La capacidad de acceder a los diagramas de los sistemas que subyacen a nuestras vidas es parte del motivo por el cual el *software* libre es importante, pero también de por qué el *hardware* libre es importante. Este mejora nuestra capacidad de realizar inversiones sustentables libremente, mejora los sistemas que usamos y determinar si estos sistemas funcionan tal como lo esperamos.

Pero independientemente de la libertad, también es el motivo por el cual es importante comprender estos sistemas, porque cuando no los comprendemos usualmente recurrimos a la autoridad, a quienes sí los comprenden o son capaces de ejercer control sobre ellos, incluso si no entienden la esencia del sistema mismo. Lo que explica por qué se habla tanto sobre la guerra cibernética: es porque algunas personas que parecen tomar las decisiones en cuanto a la guerra empiezan a hablar sobre tecnología como si supieran lo que dicen. Estas personas con frecuencia hablan de guerra cibernética pero ninguno de ellos, ni siquiera uno, habla sobre paz cibernética, ni de nada relacionado con la consolidación de la paz. Siempre hablan sobre la guerra porque ese es su negocio y ellos tratan de controlar los procesos tecnológicos y legales como un medio de promoción de sus propios intereses. Entonces, cuando no tenemos control de nuestra tecnología, tales personas desearán usarla para sus propios fines, específicamente para la guerra. Esa es la receta para cosas bastante terroríficas —que es como pienso que llegamos a Stuxnet— y personas por lo demás sensatas sugieren que, mientras Estados Unidos está en guerra, tales tácticas de algún modo evitarán los conflictos bélicos. Ese tal vez sea un argumento razonable para un país que no esté invadiendo activamente otras naciones, pero resulta poco creíble en el contexto de una nación involucrada en múltiples invasiones en curso.

LA MILITARIZACIÓN DEL ESPACIO CIBERNÉTICO

JULIAN: Ahora hay una militarización del espacio cibernético, a modo de ocupación militar. Cuando te comunicas a través de internet, cuando te comunicas usando teléfonos celulares, que ahora están fusionados con internet, tus comunicaciones están siendo interceptadas por organizaciones de inteligencia militar. Es como tener un tanque en tu habitación. O un soldado entre tu esposa y tú mientras envías un mensaje de texto. Todos vivimos bajo la ley marcial en lo que a nuestras comunicaciones respecta, solo que no podemos ver los tanques, pero están allí. En ese sentido, internet, que se suponía que era un espacio civil, se ha convertido en un espacio militarizado. Pero internet es nuestro espacio, porque todos lo usamos para comunicarnos entre nosotros y con nuestros seres queridos. Las comunicaciones con nuestro entorno más íntimo ahora pasan por internet. Entonces nuestras vidas privadas en efecto han ingresado a un espacio militarizado. Es como tener un soldado bajo la cama. Esta es una militarización de la vida civil.

JACOB: Poco antes de venir aquí, fui invitado a ser entrenador en la competencia Universitaria de Ciber-Defensa de la costa del Pacífico para el equipo del Laboratorio de Investigaciones en Seguridad y Privacidad de la Universidad de Washington. A último momento me ofrecieron ser asesor. Invertimos mucho tiempo para competir en un evento sobre guerra cibernética en el que SPAWAR —un brazo civil de la Marina de Estados Unidos que brinda servicios de evaluación de seguridad informática, y realiza tareas de piratería informática ofensivas y defensivas—, jugó el rol generalmente llamado de Equipo Rojo.[46] Lo que hacen es atacar a todos los demás participantes y el deber de cada equipo es defender sus sistemas informáticos, que les fueron entregados al comienzo del evento sin ningún conocimiento previo real. No se sabe qué tipo de sistema defenderás y ni siquiera está claro cómo se anotan los puntos de modo que uno trata de hacer lo mejor que puede.

---

46 *Pentesting*, contracción de «penetration testing» (evaluación de penetración), es un término proveniente de la ingeniería en seguridad informática que significa llevar a cabo un ataque de forma legalmente autorizado contra una computadora o una red, tal como podría hacerlo un usuario autorizado, con el fin de evaluar cuán segura es. Los investigadores en materia de seguridad son a menudo reclutados de la comunidad *hacker* para realizar *pentesting* de sistemas seguros.

JULIAN: ¿Estás seguro de que realmente se trata de un juego? ¡Tal vez no sea un juego!

JACOB: No, a uno le dan una serie de computadoras y tiene que protegerlas, y ellos irrumpen y se apoderan de los sistemas. Es como una versión infantil de Capturar la Bandera en una conferencia de *hackers* o algo así, y es interesante porque estos tipos cuentan con muchas herramientas, han escrito *software*.[47]

JULIAN: ¿Cuál es el objetivo desde la perspectiva de la Marina estadounidense?

JACOB: Bueno, en su caso solo están auspiciando esto porque quieren formar a los soldados cibernéticos del mañana y, por ejemplo, traje conmigo un bloc de notas de la CIA porque estaban reclutando. Había un tipo llamado Charlie —Charlie de la CIA— quien decía que si querías ingresar a la CIA, esa era una gran oportunidad para trabajar en el mundo real. Y también estaba la gente de SPAWAR, y Microsoft también estaba reclutando. La idea era capacitar a todas estas personas, a todos estos equipos, con el fin de clasificar para el Campeonato Nacional y consagrarse ganadores y «defender a la nación», y luego ser capaces de perpetrar ataques en tanto ciberguerreros, no solo como ciberdefensores. Obtuvimos como 4000 puntos en este juego, lo cual ascendía al puntaje del segundo, tercero y cuarto puesto combinados. Obtuvimos un puntaje aún mayor que el de todos ellos juntos.

JULIAN: Sí, sí, sí.

JACOB: No fue gracias a mí —mi cita motivadora fue algo así como: «Siempre que llovió, paró», y no creo ser particularmente bueno como entrenador—, estos muchachos son realmente buenos. Pero fue interesante porque todo el evento estaba enmarcado en términos bélicos, algo que se solía decir era: «Eh, queremos escuchar tu grito de guerra». Y mi respuesta era: «Disculpa, ¿cómo dices?». Eso era lo que se decía durante el almuerzo, por ejemplo, cuando tomábamos un descanso de defender nuestros sistemas. Ellos enmarcaban todo en términos de atacar sistemas y la guerra y la guerra cibernética y la grandeza de esta forma de pensar. Y lo más interesante, no en el equipo con el que estaba trabajando, es que notaba que había mucha gente molesta, porque no les estaban enseñando el arte de la guerra —se parecía más a una Copa Sysadmin, gente que defiende sistemas— y me resultó desagradable.[48] Me pareció muy extraño porque estaba toda esta

---

47 Capturar la bandera es originalmente un juego al aire libre que normalmente involucra a dos equipos en el que ambos equipos mantienen una posición y resguardan una bandera. El objetivo es capturar la bandera del equipo contrario, y regresarla a la base. En las conferencias de *hackers*, los *hackers* juegan una versión virtual de este juego en el que los equipos atacan y defienden computadoras y redes.

48 Sysadmin Cup es una contracción de System Administrator Cup (Copa de Adminis-

gente formada en la guerra, cuyo punto de vista era la guerra, pero no estaban enseñando estrategia, sino que estaban muy concentrados en la retórica de la defensa de estos sistemas, o del ataque de estos sistemas, y había tanta beligerancia en la forma en que se manejaban que terminaban arengando a los participantes para despertar en ellos una suerte de fervor patriótico. No estaban promoviendo el pensamiento creativo o algún tipo de marco de trabajo para el análisis independiente, sino que estaban fomentando una suerte de mentalidad de «engranaje de la maquinaria», alguien que sigue órdenes para el bien de la nación. Nunca antes había visto algo por el estilo. Me descompuse y gran parte de mi equipo tuvo graves problemas para sobrellevar la situación o incluso tomarla seriamente.

JULIAN: ¿Crees que esa es la formación estándar de la Marina estadounidense, y que ahora están tratando de aplicarla a otro sector? ¿Se trata de una decisión del comando del área cibernética de mando —una decisión estratégica internacional— de las Fuerzas Armadas de Estados Unidos?

ANDY: Suena a los campos que tenían los nazis para las juventudes hitlerianas donde se adoctrinaba a niños.

JACOB: *Sie können das sagen weil du bist Deutsche*. Pueden decir eso porque eres alemán. No, no era así. La participación de la Marina estadounidense se debe solamente a que el Gobierno de Estados Unidos está auspiciando todo esto. Me pidieron que fuera entrenador porque necesitaban a alguien que hiciera eso y accedí porque me agradaban los participantes, los estudiantes universitarios. Pero realmente se reduce al Gobierno estadounidense tratando de convencer a personas de hacer esto y lo están haciendo desde la perspectiva del nacionalismo. Es un evento muy extraño en el cual participar porque, por un lado, es bueno saber cómo mantener tu sistema a salvo y es bueno comprender la infraestructura de la que toda nuestra vida depende; pero, por otro lado, no se estaba tratando de convencer a la gente de que lo entienda, se estaba tratando de contagiarles una suerte de fervor para que estén contentos de hacer este tipo de trabajos.

ANDY: Lamentablemente, el interés de Estados Unidos por mantener los sistemas a salvo es totalmente limitado porque ellos quieren sistemas vulnerables para poder controlarlos. La estrategia de controlar la criptografía a nivel mundial no ha tenido el alcance que Estados Unidos quiso originalmente allá por 1998, cuando el subsecretario de comercio de Estados Unidos se embarcó en una gira mundial para

---

tradores de Sistemas). Un administrador de sistemas es una persona que trabaja en el sector informático manteniendo y operando una red de computadoras o un sistema informático. Jacob está diciendo que el ejercicio era como un torneo para administradores de sistemas.

conseguir que Washington tuviera acceso a las contraseñas de codificación de todo el mundo.[49] Pero la codificación todavía es considerada como una tecnología de uso dual (civil y militar) y su exportación a muchos países en forma de productos para usuarios finales está limitada por ley, algo aceptado mundialmente conforme al Acuerdo de Wassenaar.[50] Esto puede parecer razonable en el contexto de considerar a países y sus acciones como «malvados», pero demuestra la dimensión del doble discurso, ya que la tecnología de vigilancia de las telecomunicaciones hasta ahora no está limitada por los controles a la exportación.[51]

JULIAN: Andy, durante años diseñaste teléfonos criptográficos. ¿Qué tipo de vigilancia masiva existe en las telecomunicaciones? Dime ¿cuáles son los últimos avances en lo referente a la industria de inteligencia gubernamental y vigilancia masiva?

ANDY: El almacenamiento masivo —o sea de todas las telecomunicaciones, todas las llamadas, todo el tráfico de datos, cualquier forma de Servicio de Mensajes Simples (SMS)—, pero también las conexiones a internet, en algunos casos como mínimo limitado al correo electrónico. Si comparas el presupuesto militar con el costo de la vigilancia y el de los soldados cibernéticos, verás que las armas normales cuestan mucho dinero. Los ciberguerreros o la vigilancia masiva son superbaratos si se los compara con una aeronave. Un avión militar cuesta alrededor de...

JULIAN: Alrededor de cien millones.

ANDY: Y el almacenamiento se vuelve cada año más barato. De hecho, hicimos algunos cálculos en el Chaos Computer Club: se puede conseguir almacenar todas las llamadas telefónicas de un año en bue-

---

49 «Araon says encryption protects privacy, commerce» (Aarón dice que la encriptación protege la privacidad y el comercio), USIS Washington File, 13 de octubre de 1998: <http://www.fas.org/irp/news/1998/10/98101306_clt.html> (consultado el 21 de octubre de 2012).

50 Sitio Web del Acuerdo de Wassenaar: <http://www.wassenaar.org> (consultado el 21 de octubre de 2012).

51 Andy se refiere a varias etapas de las «Primeras guerras criptográficas» de los noventa. Cuando los activistas criptopunk empezaron a divulgar sólidas herramientas criptográficas como *software* libre, la administración estadounidense tomó medidas para impedir que dichas herramientas criptográficas fueran usadas efectivamente. Washington clasificó la criptografía como munición de guerra y restringió su exportación; trató de imponer tecnologías deliberadamente vulnerables para que las autoridades siempre pudiesen desencriptar la información, y trató de implementar el polémico esquema de «depósito en custodia de claves». Durante un breve período luego del cambio de siglo estaba ampliamente aceptado que estas iniciativas habían sido exhaustivamente derrotadas. No obstante, actualmente hay una «Segunda Guerra Criptográfica» en curso, que incluye campañas legislativas y técnicas para proscribir o de otro modo limitar el uso de criptografía. Véase <https://www.eff.org/deeplinks/2010/09/government-seeks>.

na calidad de voz por unos 30 millones de euros incluyendo gastos administrativos, de modo que el mero almacenamiento cuesta unos 8 millones de euros.[52]

JULIAN: Existen incluso compañías como VASTech en Sudáfrica que venden estos sistemas a 10 millones de dólares al año.[53] «Interceptamos todas sus llamadas, almacenamos masivamente todas sus llamadas interceptadas.» Pero en los últimos años la situación ha pasado de interceptar todo lo que iba de un país a otro e identificar a quiénes quieres espiar, a interceptar todo y almacenar todo de forma permanente.

ANDY: Para explicarlo en términos más o menos históricos, en los viejos tiempos alguien era identificado por su posición diplomática, por la compañía en la que trabajaba, porque estaba sospechado de hacer algo o de estar vinculado con personas que realmente hicieron algo, y luego se aplicaban medidas de vigilancia sobre dicha persona. Hoy en día, gracias a las tecnologías de almacenamiento a largo plazo, se considera mucho más eficiente decir: «Registramos y almacenamos todo y luego buscamos». La manera más sencilla de describir estos dos aspectos de la industria son con un enfoque «táctico» y otro «estratégico». Táctico significa: «En este preciso momento, necesitamos intervenir esta reunión, necesitamos que alguien entre con un micrófono, un receptor o contar con un sistema de vigilancia GSM en un automóvil apostado en las inmediaciones, capaz de interceptar lo que la gente está diciendo de forma inmediata sin necesidad de interceptar la compañía que opera la red, conseguir una orden de allanamiento ni nada por el estilo, sin necesidad de un procedimiento legal, simplemente hacer todo esto». El enfoque estratégico es hacerlo de modo predeterminado, registrándolo simplemente todo, para luego realizar búsquedas usando sistemas analíticos.

JULIAN: Entonces, la interceptación estratégica es captar todo lo que un satélite de telecomunicaciones está transmitiendo, captar todo lo que pase por un cable de fibra óptica.

ANDY: Porque nunca sabes cuándo alguien es un sospechoso.

---

52 El cálculo fue para los 196.400 millones de minutos de llamadas a líneas fijas realizadas en Alemania en 2010, digitalizados con un codificador de voz de 8 Kbps (Kilobytes por segundo), lo que asciende a una cantidad de 11.784 Petabytes (Pb), redondeado con gastos administrativos hasta 15 Pb. Asumiendo un costo de almacenamiento aproximado de 500.000 dólares por Pb, eso equivale a 7,5 millones de dólares o 6 millones de euros. A esto hay que añadirle los costos de un centro de cómputos decente, energía de procesamiento, conexiones y mano de obra. Aunque se incluyan todos los 101.000 millones de minutos de llamadas entre teléfonos celulares en Alemania en 2010, lo que equivaldría a otros 50 Pb y 18,3 millones de euros, el precio sigue siendo menor a un solo avión militar como el Eurofighter (que cuesta 90 millones de euros) o el F22 (que cuesta 150 millones de dólares).

53 Para más información sobre VASTech véase Buggedplanet: <http://buggedplanet.info/index.php?title=VASTECH> (consultado el 21 de octubre de 2012).

JACOB: En Estados Unidos existen los casos NSA AT&T, entre ellos el caso Hepting *vs.* AT&T. En Folsom, California, Mark Klein, un extécnico del gigante de las telecomunicaciones AT&T, reveló que la Agencia Nacional de Seguridad (NSA, por sus iniciales en inglés), estaba almacenando todos los datos que AT&T les podía suministrar. Registraban básicamente todo, al por mayor —los datos y también las llamadas telefónicas— por lo tanto sabemos que cada vez que yo levantaba el teléfono o me conectaba a internet en San Francisco durante el período sobre el cual Mark Klein ha informado, la NSA estaba registrándolo todo.[54] Estoy bastante seguro de que han usado ese material en las

54 El escándalo de inteligencia nacional sin autorización judicial por parte de la NSA es el caso más significativo de vigilancia masiva en la historia de Estados Unidos. Aprobada en 1978, La Ley de Vigilancia e Inteligencia Extranjera de Estados Unidos (FISA, por sus iniciales en inglés) establecía que era ilegal que las agencias de Estados Unidos espiaran a ciudadanos estadounidenses sin orden judicial. Después del 11 de septiembre de 2001, la NSA empezó a incurrir en masivas violaciones de la ley FISA, con la autorización de una orden ejecutiva secreta de George W. Bush. Dicha administración se arrogó la autoridad ejecutiva para hacer esto bajo legislación de emergencia aprobada por el Congreso en 2001: La Autorización para el Uso de la Fuerza Militar (AUMF, por sus iniciales en inglés) y la Ley Patriota. El programa de espionaje nacional sin orden judicial de la NSA —que involucró la cooperación de compañías privadas, incluyendo AT&T— permaneció en secreto hasta 2005, cuando fue revelado por el *The New York Times*. Véase «Bush Lets U.S. Spy on Callers Without Courts», *The New York Times*, 16 de diciembre de 2005: <http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all>.
Periodistas de *The New York Times* habían sido contactados por un informante anónimo quien había filtrado la existencia del programa de vigilancia no autorizado. En 2004, el entonces editor ejecutivo de *The New York Times*, Bill Keller, acordó retener la noticia durante un año a instancias de la administración Bush, hasta que George W. fuera reelecto. En 2005, el *The New York Times* publicó la historia a las apuradas cuando se enteró de que la administración Bush estaba buscando aplicar una posible censura previa al estilo de los Papeles del Pentágono. La administración Bush negó ilegalidad alguna en el programa de la NSA. El Departamento de Justicia comenzó una investigación inmediata de la fuente de la filtración, que involucró a veinticinco agentes federales y cinco fiscales. Altos funcionarios del partido republicano pidieron el juicio del matutino neoyorquino bajo la Ley de Espionaje. Tras la publicación de la nota en el *The New York Times* otros informantes se contactaron con la prensa, presentando gradualmente un panorama detallado de anarquía y despilfarro en los más altos estamentos de la NSA. Se presentó una serie de demandas conjuntas por parte de grupos de defensa como la Unión Estadounidense por las Libertades Civiles (ACLU, por sus iniciales en inglés) y la Fundación Electronic Frontier (EFF, por sus siglas en inglés). En uno de estos casos, ACLU *vs.* NSA, no se permitió que los querellantes declararan porque no podían demostrar que habían sido personalmente espiados. En Hepting *vs.* AT&T, Mark Klein, un informante que denunció a AT&T, presentó una declaración jurada que revelaba el alcance de la cooperación entre AT&T y el programa nacional de espionaje. Véase la sección Hepting *vs.* AT&T en el sitio Web de EFF: <https://www.eff.org/cases/hepting>.
El testimonio de Mark Klein, un exempleado de la filial de AT&T en Folsom, San Francisco, daba cuenta de la existencia de la «Sala 641A», unas instalaciones de interceptación estratégica operada por AT&T para la NSA. Las instalaciones brindaban acceso a los caños de fibra óptica que contenían el tráfico operativo de internet, lo que le daba capacidad de realizar operaciones de vigilancia de todo el tráfico de internet que pasara por el edificio, tanto nacional como internacional. Otro denunciante de NSA, William Binney, ha estimado que existen hasta veinte instalaciones por el estilo, ubicadas todas en puntos clave de la red de telecomunicaciones de Estados Unidos.

investigaciones que han llevado a cabo contra particulares en Estados Unidos, que presenta todo tipo de problemas constitucionales interesantes porque pueden conservarlo para siempre.

La declaración jurada de Klein aporta información importante sobre el carácter del programa de vigilancia de la NSA, aspecto que quedó confirmado por los informantes que denunciaron a dicha agencia. Este es un ejemplo de «interceptación estratégica» —todo el tráfico de internet que pasa por Estados Unidos es copiado y almacenado indefinidamente. Puede saberse con certeza que el tráfico doméstico también es interceptado y almacenado en Estados Unidos porque, desde el punto de vista de la ingeniería, cuando se maneja este volumen de tráfico es imposible examinarlo para lo cual se requeriría una orden conforme a la ley FISA. La interpretación actual de dicha legislación sostiene que solo ha ocurrido una «interceptación» cuando se accede a una comunicación local ya interceptada y almacenada por la NSA en su base de datos, y que solo en esta instancia es cuando se requiere una orden judicial. Los ciudadanos estadounidenses deben asumir que el tráfico de todas sus telecomunicaciones (incluyendo las llamadas telefónicas, SMS, correos electrónicos y búsquedas en internet) son vigilados y almacenadas para siempre en centros de datos de la NSA. En 2008, en respuesta al alto volumen de litigios tras el escándalo de escuchas telefónicas, el Congreso estadounidense aprobó una serie de enmiendas a la ley FISA de 1978 que fueron inmediatamente firmadas por el presidente. Estas permitían el otorgamiento de la muy polémica «inmunidad retroactiva» contra procesos por violaciones a la ley FISA. Durante su campaña presidencial, el senador Barack Obama había hecho de la «transparencia» una parte integral de su plataforma, y prometió proteger a los informantes, pero cuando asumió la presidencia en 2009 su Departamento de Justicia siguió adelante con las políticas de la administración Bush y, con el tiempo, ganó el caso Hepting y otros con el otorgamiento de «inmunidad retroactiva» para AT&T. Si bien la investigación del Departamento de Justicia de la fuente original de la nota de *The New York Times* no logró develar al informante, sí consiguió identificar a otros informantes que habían contactado a la prensa luego de la nota. Uno de ellos fue Thomas Drake, un ex alto ejecutivo de la NSA, quien durante años se había quejado internamente ante Comités Parlamentarios de Supervisión de Inteligencia por la corrupción y el despilfarro dentro del programa «Trailblazer» de la NSA. Las quejas internas eran silenciadas, al igual que cualquier empleado del Gobierno que quisiera investigarlas. Luego de la nota de *The New York Times*, Drake le acercó el material sobre Trailblazer al periódico *Baltimore Sun*. Drake fue imputado tras una investigación de un Gran Jurado, tildado de «enemigo del Estado», acusado bajo la Ley de Espionaje. Véase «The Secret Sharer», *The New Yorker*, 23 de mayo de 2011:<http://www.newyorker.com/reporting/2011/05/23/110523fa_fact_mayer?currentPage=all>.
El juicio contra Drake colapsó en junio de 2011 luego de un amplio interés público, y tras intentos fallidos por hacer que Drake brindara una declaración de culpabilidad pactada, el Departamento de Justicia aceptó su declaración de culpabilidad por un delito menor. Drake fue sentenciado a un año de libertad condicional. Las repercusiones del escándalo de inteligencia de la NSA continúan. La ACLU está litigando para apelar la constitucionalidad de las enmiendas a la ley FISA de 2008 en Amnesty *et al. vs.* Clapper. Véase «FISA Amendment Act Challenge», ACLU, 24 de septiembre de 2012: <http://www.aclu.org/national-security/amnesty-et-al-v-clapper>. En Jewel *vs.* NSA, la EFF está buscando ponerle fin a la vigilancia no autorizada por parte de la NSA. El caso fue desestimado en 2009 luego de que la administración Obama alegara inmunidad en virtud de secretos de seguridad nacional. Véase la página de la EFF sobre Jewel *vs.* NSA: <https://www.eff.org/cases/jewel. Sin embargo, el Noveno Tribunal de Apelaciones permitió la reapertura del caso en diciembre de 2011. Thomas Drake y otros informantes que denunciaron a la NSA como William Binney y J. Kirk Wiebe están aportando evidencias en Jewel *vs.* NSA. La administración Obama —que hizo de la transparencia un pilar de su plataforma presidencial— ha enjuiciado a más informantes bajo la Ley de Espionaje que todas las administraciones anteriores combinadas. (Todos los *links* de esta nota fueron consultados el 23 de octubre de 2012).

JÉRÉMIE: También está el ejemplo de Eagle, el sistema vendido por la compañía francesa Amesys a la Libia de Gadafi, cuyo documento comercial decía: «Mecanismo de interceptación nacional». Es una gran caja que colocas en algún lugar y escuchas la comunicación de todo tu pueblo.[55]

JULIAN: Hace diez años esto era visto como una fantasía, esto era algo en lo que solo creían las personas paranoicas. Pero los costos de la interceptación en masa han bajado tanto ahora que incluso un país como Libia, que dispone de relativamente pocos recursos, lo está haciendo con tecnología francesa. De hecho, en lo que respecta a la mera interceptación, la mayoría de los países ya pueden hacerlo. La eficiencia en la comprensión y en la respuesta ante lo interceptado y lo almacenado es lo que va a constituir el próximo gran salto. Hoy en día, muchos países cuentan con tecnología de interceptación de todo el tráfico que entra y sale del país, pero las acciones subsiguientes, como bloquear automáticamente cuentas bancarias, desplegar efectivos de policía o aislar a determinados grupos o liberar a otros, es algo que está a punto de ocurrir. Siemens tiene a la venta una plataforma para agencias de inteligencia que de hecho realiza acciones automatizadas. De modo que cuando un blanco A, de acuerdo a sus registros de interceptación móvil, se encuentra a una determinada distancia de un blanco B y el blanco A recibe un correo electrónico mencionando algo —una contraseña por ejemplo— entonces se desencadena una acción. Estamos cerca de poder hacer eso.

55 Véase la entrada del Sistema Eagle en buggedplanet: <http://buggedplanet.info/index.php?title=AMESYS#Strategic_.28.22Massive.22.29_Appliances> (consultado el 22 de octubre de 2012).

COMBATIR LA VIGILANCIA TOTAL CON LAS LEYES DEL HOMBRE

JÉRÉMIE: Es un hecho que la tecnología ahora permite una vigilancia total de cada comunicación. Pero luego está el otro lado de la moneda, qué es lo que se hace con ese registro. Podríamos admitir que, para lo que se denomina vigilancia táctica existen algunos usos legítimos —investigadores que vigilan a chicos malos y a redes de malechores podrían necesitar, bajo la supervisión de autoridades judiciales, usar dichas herramientas— pero la pregunta es cómo limitar esta supervisión judicial, cómo limitar el control ciudadano al uso de estas tecnologías. Esta es una cuestión de política pública. Cuando observamos estas políticas vemos que hay funcionarios a quienes se les pide que firmen documentos sin comprender la tecnología subyacente, y creo que nosotros en tanto ciudadanos tenemos el deber, no solo de explicarles a los políticos y al resto de la comunidad cómo funciona la tecnología en su totalidad, sino de participar de los debates políticos que abarcan el uso de dichas tecnologías. Sé que en Alemania hubo un movimiento masivo contra la ley de Retención de Datos que dio lugar a su anulación por un tribunal constitucional.[56] En la Unión Europea hay un debate abierto sobre la consulta de la Directiva de Retención de Datos.[57]

ANDY: Te referís en teoría a un Estado democrático que, por supuesto, necesita identificar a los delincuentes y escuchar sus llamadas telefónicas a partir de una decisión judicial, con la debida supervisión para garantizar que esté hecho de forma adecuada. Las autoridades necesitan actuar conforme a la ley. Si no lo hacen entonces ¿de qué sirven? Justamente con ese enfoque estratégico, los Estados democráticos en Europa están comprando masivamente estas máquinas que les permiten actuar fuera de la ley respecto de la interceptación,

---

56 «German court orders stored telecoms data deletion», *BBC*, 2 de marzo de 2010: <http://news.bbc.co.uk/1/hi/world/europe/8545772.stm> (consultado el 15 de octubre de 2012).

57 La Directiva 2006/24/EC del Parlamento y Consejo Europeos les exige a los Estados europeos almacenar los datos de las telecomunicaciones de los ciudadanos durante seis a veinticuatro meses. Fue la aplicación de esta Directiva a la ley alemana la que fue declarada inconstitucional en Alemania. En mayo de 2012 la Comisión de la UE remitió a la nación germana al Tribunal Europeo de Justicia por no atenerse a la Directiva (véase el comunicado de prensa de la Comisión: <http://europa.eu/rapid/press-release_IP-12-530_en.htm> (consultado el 15 de octubre de 2012).

ellos pueden simplemente encender estas máquinas y hacerlo, y esta tecnología no puede ser controlada.

JULIAN: Pero ¿hay acaso dos enfoques para lidiar con la vigilancia estatal masiva: las leyes de la física y las leyes del hombre? El primero sería usar las leyes de la física para construir dispositivos que impidan la interceptación. El segundo sería implementar controles democráticos conforme a la ley para garantizar la necesidad de órdenes judiciales a fin de conseguir cierta responsabilidad regulatoria. Pero la interceptación estratégica no puede ser parte de eso, no puede estar realmente constreñida por la regulación. La interceptación estratégica se basa en interceptar a *todos* sin importar su inocencia o culpabilidad. Debemos recordar que llevar a cabo tal operación de inteligencia es un elemento medular del *establishment*. Siempre faltará voluntad política para poner al descubierto el espionaje estatal. Y la tecnología es inherentemente tan compleja, y su implementación práctica tan secreta, que no puede haber una efectiva supervisión democrática.

ANDY: O espías a tu propio Parlamento.

JULIAN: Pero esas son excusas —la mafia y el espionaje internacional— son excusas que la gente aceptará para erigir un sistema de estas características.

JACOB: Los cuatro jinetes del info-pocalipsis: la pornografía infantil, el terrorismo, el lavado de dinero y la guerra contra algunas drogas.

JULIAN: Una vez que tienes montada la vigilancia, dada su complejidad y que está diseñada para operar en secreto, ¿no es cierto acaso que no puede ser regulada mediante políticas? Pienso que —excepto en naciones muy pequeñas como Islandia—, a menos que se den condiciones revolucionarias, resulta simplemente imposible controlar la interceptación masiva con leyes y políticas públicas. Simplemente no va a suceder. Es muy barato y muy fácil eludir los controles políticos para llevar a cabo una interceptación. Los suecos aprobaron una ley de interceptación en 2008, conocida como la FRA-lagen, que le permitía a la Agencia sueca de Inteligencia de las Comunicaciones (FRA por sus siglas en sueco) interceptar legalmente todas las comunicaciones que pasaban por el país para enviarlas a Estados Unidos, con algunas limitaciones.[58] Entonces, ¿cómo puedes hacer respetar dichas limitaciones una vez que han montado el sistema de interceptación y la organización que lo hizo una agencia de espionaje? Es imposible. Y de hecho han aparecido casos en los que la FRA actuó ilegalmente en una

58 Véase «Sweden approves wiretapping law», *BBC*, 19 de junio de 2008: <http://news.bbc.co.uk/1/hi/world/europe/7463333.stm>.
Para más información sobre la ley FRA-lagen, véase Wikipedia: <http://en.wikipedia.org/wiki/FRA_law> (ambos *links* consultados el 10 de octubre de 2012).

serie de ocasiones antes de dicha ley. Muchos países simplemente lo hacen por fuera de la ley sin resguardo legislativo alguno. De modo que podríamos decir que tenemos suerte si, como en el caso de Suecia, ellos decidieran que para protegerse de ser llevados ante la Justicia ellos quieren regularizar su situación modificando la ley. Y ese es el caso de la mayoría de los países, donde se da una interceptación a granel, y cuando se presenta una propuesta legislativa, es para proteger a quienes la llevan a cabo.

Esta tecnología es muy compleja; por ejemplo en el debate que se dio en Australia y el Reino Unido sobre la legislación propuesta para interceptar todos los metadatos, la mayoría de las personas no entendió la importancia de los metadatos ni el concepto mismo.[59] Interceptar todos los metadatos significa que tienes que construir un sistema que físicamente intercepte todos los datos y luego se deshaga de todo excepto los metadatos. Pero no se puede confiar en un sistema de estas características. Solo ingenieros altamente calificados con autorización para verificar qué es lo que está sucediendo precisamente pueden determinar si en efecto se está interceptando y almacenando solamente los metadatos, y no hay voluntad política para otorgar este tipo de acceso. El problema está empeorando porque la complejidad y la confidencialidad son una mezcla explosiva. Ocultos por la complejidad. Ocultos por la confidencialidad. La impunidad está incorporada. Viene incluida. Es peligrosa de fábrica.

JÉRÉMIE: No digo que el enfoque estratégico pueda funcionar. Estoy diciendo que esta es la teoría de cómo funcionaría un sistema democrático, y en efecto, incluso dentro de esta teoría existen servicios secretos con permiso de ir más allá de donde tienen permitido ir las fuerzas regulares policiales u otras. De modo que, aunque enmarquemos adecuadamente la conducta de las fuerzas regulares, habrá otras capaces de usar esas tecnologías. Pero la verdadera pregunta es si se debe regular o no la mera posibilidad de comprar y ser poseedores de esas tecnologías en lugar de regular su uso.

---

59 Los metadatos son «datos sobre datos». En el contexto de esta discusión, los metadatos refieren a datos fuera del «contenido» de la comunicación electrónica. Se trata del frente del sobre, más que de los contenidos. Es toda la información sobre los contenidos: a quién fue enviado el correo o por quién, las direcciones IP (y por tanto las ubicaciones) desde donde fueron enviados, la hora y la fecha de cada correo electrónico, etcétera. El tema es, no obstante, que la tecnología para interceptar metadatos es la misma tecnología usada para interceptar los contenidos. Si le concedes a alguien el derecho de vigilar tus metadatos, sus dispositivos también interceptarán el contenido de tus comunicaciones. Además de esto, la mayoría de las personas no se da cuenta de que «los metadatos conforman un contenido»: cuando todos los metadatos son reunidos ofrecen una descripción asombrosamente detallada de las comunicaciones de una persona.

JULIAN: Te refieres a los equipos de interceptación en masa que pueden interceptar medio país o una ciudad.

JÉRÉMIE: Sí, como un arma nuclear: no es fácil vender una bomba nuclear, y puede que algunos países quieran construir una pero se toparán con problemas. Cuando hablamos sobre sistemas armamentísticos lo que se regula es la tecnología y no el uso que se hace con las armas. Pienso que el debate debería centrarse en si estas tecnologías pueden ser consideradas como de guerra.

JACOB: Depende. Cuando se usan como armas —y no hay duda de que los dispositivos de vigilancia constituyen un arma en lugares como Siria o Libia— las usan específicamente para dirigir ataques contra personas por motivos políticos. La compañía francesa Amesys vigiló a personas en el Reino Unido usando dispositivos franceses cuyo uso era ilegal en Francia, y lo vendieron a sabiendas de eso.[60]

ANDY: Ellos nunca harían eso, ¿correcto?

JACOB: Bueno, Amesys fue atrapada con sus propios documentos internos en *The Spy Files*.[61] Si nos vamos a referir a esto en términos armamentísticos, debemos recordar que no es como venderle un camión a un país. Es como venderle un camión, un mecánico y un equipo a bordo del camión que selectivamente apunta contra las personas para luego disparar contra ellas.

JULIAN: Es como venderle toda una flota de camiones.

ANDY: Es interesante que la criptografía esté regulada. Existe el Acuerdo de Wassenaar, que rige internacionalmente y prohíbe la exportación de tecnología de codificación, lo que ayuda a proteger de la tecnología de vigilancia a aquellos países considerados enemigos o, por la razón que sea, problemáticos. Pero si comercializas equipos de vigilancia *sí* puedes vender tecnología de codificación internacionalmente. No existen restricciones a las exportaciones de eso. La razón, diría, es que incluso los Gobiernos democráticos tienen interés en el ejercicio del control. Y aunque trates con países «malvados» y les suministres equipos de vigilancia para ser usados con fines malignos, saldrás beneficiado porque te enterarás de lo que están escuchando,

---

60 Amesys es parte del grupo Bull, otrora competencia de Dehomag de IBM en la venta de sistemas de tarjetas perforadas a los nazis. Véase Edwin Black, *IBM and the Holocaust* (Crown Books, 2001). Para más información sobre cómo Gadafi espiaba a los libios en el Reino Unido usando equipo de vigilancia Amesys, véase: «Exclusive: How Gaddafi Spied on the Fathers of the New Libya», OWNI.eu, 1 de diciembre de 2011: <http://owni.eu/2011/12/01/exclusive-how-gaddafi-spied-on-the-fathers-of-the-new-libya> (consultado el 22 de octubre de 2012).

61 WikiLeaks empezó a publicar *The Spy Files*, revelando el alcance de la vigilancia en masa, en diciembre de 2011. Se puede acceder a ellos en <http://wikileaks.org/the-spyfiles.html>.

de aquello a lo que temen, de quiénes son las personas más importantes de la oposición que se oponen al Gobierno que organizan actos políticos, etcétera. De modo tal que podrás predecir acontecimientos futuros, auspiciar acciones y demás. Entramos al juego muy sucio que está ocurriendo entre países, y esa es la realidad por la cual los sistemas de vigilancia no están regulados.

JULIAN: Quisiera indagar en esta analogía de la vigilancia a gran escala como arma de destrucción masiva. La posibilidad de fabricar una bomba atómica fue un hecho de la física, y cuando se fabricó la bomba atómica la geopolítica cambió, y entonces la vida de muchas personas cambió de maneras diferentes, algunas para bien, quizás, otras al borde del apocalipsis. Una iniciativa regulatoria aplicó controles y hasta ahora dichos controles, con la excepción de Japón, nos han salvado de la guerra nuclear. Pero resulta fácil determinar cuándo tales armas son usadas y cuándo no. Con el aumento en la sofisticación y la disminución del costo de la vigilancia en masa de los últimos diez años, nos encontramos en un momento en el que la población humana se está duplicando aproximadamente cada veinticinco años —pero la capacidad de la vigilancia se está duplicando cada dieciocho meses. La curva de crecimiento de la vigilancia está dominando la curva poblacional. No hay salida. Hoy en día con solo 10 millones de dólares puedes comprar una unidad para almacenar de forma permanente las interceptaciones en masa de un país mediano. Entonces, me pregunto si lo que precisamos no es una acción equivalente. Esto realmente es una amenaza para la democracia y la libertad a nivel mundial que necesita una respuesta, tal como la amenaza de la guerra nuclear la necesitó, para tratar de controlarla, mientras aún podamos.

ANDY: Veía cómo en Libia el movimiento democrático ingresó a las estaciones de vigilancia encontró grabaciones y evidencias de que compañías occidentales ayudaron al régimen de Gadafi a reprimir actividades políticas, y luego, el nuevo gobierno pasó a operar esas mismas instalaciones que ahora están funcionando a toda capacidad.[62] Entonces si bien estoy de acuerdo en que debería controlarse esta tecnología, soy un poco escéptico en cuanto a la capacidad que tienen los intereses de los ciudadanos en contrarrestar los intereses de quienes están en el poder. Ni siquiera son necesariamente los Gobiernos, porque quienes tengan la capacidad de escuchar todas las llamadas telefónicas tienen el poder. Esto también tiene que ver con los precios de las acciones: uno puede beneficiarse mucho económicamente si sabe lo que está ocurriendo.

---

62 Para más detalles véase buggedplanet: <http://buggedplanet.info/index.php?title=LY>.

JULIAN: Los países que cuentan con leyes que definen cuáles deberían ser los blancos de sus principales agencias de espionaje electrónico —como la NSA de Estados Unidos, el Cuartel General de Comunicaciones del Gobierno (GCHQ, por sus iniciales en inglés) del Reino Unido, la Dirección de Señales de Defensa (DSD, por sus siglas en inglés) de Australia— han modificado dicha legislación para incluir la inteligencia económica. Por ejemplo, supongamos que Australia y Estados Unidos están compitiendo por cerrar un negocio de trigo, ellos pueden espiar a todas las personas involucradas en el negocio. Esto ya ha estado ocurriendo durante mucho tiempo, al menos desde hace diez años que es público. Comenzó con la venta de armas, en las que compañías como Lockheed Martin, Raytheon y Northrup que estaban negociando armas, también estaban involucradas en la construcción de sistemas de interceptación en masa. Estos recibieron favores de sus amigos y realizaron interceptaciones del negocio armamentístico bajo el paraguas de la seguridad nacional. Pero ahora se aplica a cualquier cosa que pudiese beneficiar económicamente a un país, lo cual puede ser casi cualquier cosa.

JACOB: Una buena analogía planteada por algunas personas en el Congreso de Chaos Communication en diciembre de 2011 fue la idea de tratar la tecnología de vigilancia, especialmente la de vigilancia táctica pero también la de vigilancia estratégica, como a las minas terrestres.[63] Pienso que es una analogía muy potente. Porque que sea posible no significa que sea inevitable recorrer ese camino, ni llegar al punto tal que toda persona esté bajo vigilancia. Sin embargo, hay algunos incentivos económicos en nuestra contra. Por ejemplo, alguien me explicó que el sistema telefónico noruego solía funcionar de manera tal que hacía andar un medidor que, dependiendo de cuán lejos uno llamaba, andaba más rápido o más lento. Pero no era legal que la compañía telefónica de Noruega mantuviera un registro de los metadatos de las llamadas realizadas, como el número discado, debido específicamente a razones de privacidad que surgieron en torno a la segunda guerra mundial. Entonces es posible construir la misma tecnología de manera que no viole la privacidad pero que haga posible de todos modos un enfoque mercantil, que haga lugar a retribuciones económicas. Con todo no podemos ganar, por ejemplo, frente a tecnologías GSM (móvil). En este momento, por cómo están armados estos sistemas, no solo en cuanto a la facturación sino a su arquitectura, implica que no haya privacidad ni de la ubicación ni del contenido.

JULIAN: Un teléfono celular es un dispositivo de rastreo que también efectúa llamadas.

---

63 El Congreso Chaos Communication es un encuentro anual *hacker* internacional, organizado por el Chaos Computer Club.

JACOB: Exactamente. Si decimos que todos están siendo espiados en el Tercer Mundo, realmente, ¿qué significa eso? Significa que sus sistemas telefónicos, que son su nexo con el resto del mundo, son dispositivos de espionaje cuando alguien decide usar los datos almacenados con esos fines.

ANDY: He visto que hay países africanos que están recibiendo toda la infraestructura para internet, que incluye cables de fibra óptica y conexiones troncales, como regalo de los chinos.

JACOB: ¿Un regalo de ZTE o algo por el estilo?[64]

ANDY: Sí, y por supuesto que como los chinos tienen interés en los datos, en lugar que les retribuyan en dinero, se quedan con los datos. Ellos son la nueva moneda.

64 Jacob se refiere a ZTE, uno de los dos productores chinos (el otro es Huawei) de artículos electrónicos que se sospecha que contienen «puertas traseras» o sea que el fabricante retiene medios técnicos para introducirse en los productos que distribuye. Jacob quiere decir que el «regalo» de infraestructura de comunicaciones viene con el costo de que por cómo está diseñado son susceptibles a la vigilancia china.

ESPIONAJE POR PARTE DEL SECTOR PRIVADO

JÉRÉMIE: La vigilancia realizada por el Estado es en efecto un tema importante que desafía la estructura misma de todas las democracias y la forma en que estas funcionan, pero también existe vigilancia por parte del sector privado y potencialmente también recolección masiva de datos. Pensemos solamente en Google. Si eres un usuario estándar, Google sabe con quién te estás comunicando, a quién conoces, qué estás buscando, potencialmente tu orientación sexual, y tus creencias religiosas y filosóficas.

ANDY: Sabe más sobre ti que tú mismo.

JÉRÉMIE: Más que tu madre y posiblemente más que tú mismo. Google sabe cuándo estás conectado y cuándo no.

ANDY: ¿Sabes lo que buscaste hace dos años, hace tres días y hace dos horas? No lo sabes, Google sí.

JÉRÉMIE: Realmente, trato de no usar Google por estas mismas razones.

JACOB: Es como el movimiento Kill Your Television (Mata a tu televisor) del siglo XXI.[65] Una protesta que sería efectiva si no fuera que el efecto de red impide su articulación.[66] ¡Elimina tu televisión, hermano!

JÉRÉMIE: Bueno, no es una protesta, es más mi forma personal de ver las cosas.

ANDY: Vi una película hermosa en la que la gente arrojaba sus televisores por la ventana desde el tercer piso de sus casas.

JÉRÉMIE: No solo se trata de la vigilancia estatal, es la cuestión de la privacidad, la forma en que los datos son manejados por terceros y el conocimiento que las personas tienen de lo que se hace con los datos. No uso Facebook así que no sé mucho al respecto. Pero sé que en Facebook uno ve usuarios que alegremente revelan cualquier tipo de información personal, y ¿puedes acaso culpar a las personas por

---

65 Kill Your Television es el nombre de una forma de protesta contra las comunicaciones masivas, en la que las personas descartan la televisión en favor de actividades sociales.

66 El «efecto de red» es el efecto que la actividad realizada por una persona tiene sobre la probabilidad de que otra persona lleve a cabo dicha actividad.

no saber dónde está el límite entre lo público y lo privado? Hace unos años, previo al estallido de la tecnología digital, la gente que tenía una vida pública era la del mundo del espectáculo, de la política o eran periodistas, y ahora todo el mundo está a un clic de distancia de poder tener una vida pública. «Publicar» significa hacer que algo sea público, significa darle al resto del mundo acceso a estos datos —y, por supuesto, cuando ves a adolescentes enviando fotos de sí mismos alcoholizados o lo que fuera, lo más probable es que no tengan noción de que es «al resto del mundo», potencialmente por mucho, mucho tiempo—. Facebook hace un negocio de desdibujar la línea que divide lo privado, los amigos y lo público. Y esto se da cuando Facebook guarda los datos que tú pensabas eran para tus amigos y tus seres queridos. De modo que sea cual fuera el grado de publicidad que quieras darles a tus datos, cuando haces clic en «publicar», primero se los das a Facebook, y luego Facebook les da acceso a algunos usuarios de la red social.

JULIAN: Incluso se desdibuja la línea que separa a los Gobiernos de las corporaciones. Si observas la expansión del sector de contratistas militares en Occidente verás que la NSA, la mayor agencia de espionaje del mundo, hace diez años, trabajaba con diez contratistas. Hace dos años lo hacía con más de mil. De modo que también se borronea la frontera entre el Gobierno y el sector privado.

JÉRÉMIE: Y podría sostenerse que las agencias de espionaje estadounidenses tienen acceso a todos los datos almacenados por Google.

JULIAN: Y lo tienen.

JÉRÉMIE: Y a todos los datos de Facebook, de modo que en un sentido Facebook y Google podrían ser consideradas extensiones de estas agencias.

JULIAN: ¿Ha habido una citación legal a Google, Jake? ¿Recibió Google la orden de entregar la información relacionada a tu cuenta de Jake? WikiLeaks se vio afectada por oficios secretos recibidos por Dynadot, la empresa de registro de nombres de dominio en California, donde está inscripto wikileaks.org. Se trataba de emplazamientos provenientes de la investigación secreta sobre WikiLeaks llevada a cabo por el Gran Jurado, solicitando registros financieros, registros de *logins*, etcétera, que fueron entregados.[67]

67 Para más información sobre la investigación del Gran Jurado, véase «Nota sobre los varios intentos por reprimir a WikiLeaks y a las personas vinculadas al proyecto» más arriba.

JACOB: El *Wall Street Journal* informó que Twitter, Google y Sonic.net, tres servicios que uso o he usado en el pasado, recibieron todos un oficio 2703(d), que es esta forma inusual de emplazamiento secreto.[68]

JULIAN: ¿Bajo la Ley Patriota (*Patriot Act*)?

JACOB: No. Esta es la Ley de Comunicaciones Almacenadas (Stored Communications Act), esencialmente. El *Wall Street Journal* dice que cada uno de estos servicios afirma que el Gobierno quería los metadatos, y el Gobierno afirmó que tiene derecho de hacer esto sin orden judicial. Hay un caso abierto en la Justicia sobre el derecho del Gobierno a mantener sus tácticas en secreto, no solo del público sino de los registros judiciales. Yo lo supe al leer *Wall Street* como cualquier persona.

JULIAN: Entonces Google se puso gustosamente del lado del Gobierno estadounidense cuando este le solicitó tus registros en el marco de la investigación del Gran Jurado sobre WikiLeaks —no se trató de un emplazamiento convencional, sino de una suerte de oficio de inteligencia—. Pero a principios de 2011 trascendió que Twitter que había recibido una serie de emplazamientos del mismo Gran Jurado, apeló para poder notificar a las personas cuyas cuentas fueron solicitadas y quedara sin efecto la cláusula de confidencialidad. No

---

68 Según el *Wall Street Journal*: «El Gobierno estadounidense ha conseguido un polémico tipo de oficio secreto para forzar a Google Inc. y al pequeño proveedor de internet Sonic.net Inc. a revelar información sobre las cuentas de correo electrónico del colaborador de WikiLeaks Jacob Appelbaum, según documentos consultados por el *Wall Street Journal*. (...) A comienzos de este año el caso WikiLeaks se convirtió en un banco de pruebas para la interpretación de la ley cuando Twitter apeló un emplazamiento que le ordenaba revelar los registros de las cuentas de partidarios de WikiLeaks incluyendo las de Appelbaum. (...) La orden buscaba las direcciones de «Protocolo de internet», o direcciones IP, de los dispositivos desde los cuales las personas ingresaron a sus cuentas. La dirección IP es un número único asignado a un dispositivo que se conecta a internet. La orden también buscaba dar con las direcciones de correo electrónico de las personas con las que dichas cuentas se habían comunicado. El emplazamiento fue presentado en secreto, pero Twitter obtuvo el permiso de la Corte para notificar a los usuarios cuya información fue solicitada. (...) Las órdenes judiciales consultadas por *Wall Street Journal* buscaban el mismo tipo de información que se le pedía a Twitter. El oficio secreto que recibió Google es del 4 de enero y le ordena al gigante de las búsquedas entregar la dirección IP desde la que Appelbaum ingresó a su cuenta de gmail.com y los correos electrónicos y direcciones IP de los usuarios con los que él se comunicó desde el 1 de noviembre de 2009 hasta la fecha. No está claro si Google apeló dicha orden o si entregó lo requerido. El emplazamiento a Sonic está fechado el 15 de abril y le ordena a la compañía a entregar el mismo tipo de información de la cuenta de correo de Appelbaum desde el 1 de noviembre de 2009 hasta la fecha. El 31 de agosto, la Corte aprobó levantar el secreto de la orden para que Sonic entregara una copia a Appelbaum». «Secret orders target email», *Wall Street Journal*, 9 de octubre de 2011: <http://online.wsj.com/article/SB10001424052970203476804576613284007315072.html>. (consultado el 11 de octubre de 2012). Para más detalles, véase «Nota sobre los varios intentos por reprimir a WikiLeaks y a las personas vinculadas al proyecto» más arriba.

tengo cuenta de Twitter, por lo que no recibí requisitoria alguna, pero mi nombre y el de Bradley Manning fueron incluidos en todos los emplazamientos como la información que se estaba buscando. Jake, tú tenías una cuenta de Twitter, por lo que Twitter recibió un emplazamiento con relación a ti. Google también recibió un oficio, pero no apeló para hacerlo público.[69]

JACOB: Presuntamente. Eso es lo que leí en el *Wall Street Journal*. Es posible que yo no esté autorizado a mencionarlo excepto que sea en conexión con el *Wall Street Journal*.

JULIAN: ¿Esto se debe a que las citaciones tienen la obligación de mantenerlas en secreto? Se determinó que eso era inconstitucional, ¿verdad?

JACOB: Tal vez no. En cuanto al caso de Twitter, trascendió públicamente que perdimos la moción que sostenía que entregarle estos datos al Gobierno causaría un daño irreparable ya que ellos no pueden olvidar esta información una vez que la reciben. Ellos dijeron: «Sí, bueno, su moción ha sido denegada, Twitter debe entregar estos datos». Estamos en proceso de apelación, específicamente en lo referente al secreto del sumario —y no puedo hablar acerca de eso— pero tal como está ahora, la Corte dijo que no se puede esperar tener privacidad en internet cuando uno voluntariamente revela información a un tercero y, por cierto, en internet todo el mundo es un tercero.

JULIAN: Aunque la organización como Facebook o Twitter diga que mantendrá la información en secreto.

JACOB: Sin duda. Y aquí es donde se desdibuja el límite que separa al Estado de la corporación. Probablemente este sea el elemento más importante a tener en cuenta, que la NSA y Google conforman una sociedad de ciberseguridad por motivos de defensa nacional estadounidense.

ANDY: Sea lo que ciberseguridad signifique en este contexto. Ese es un concepto amplio.

JACOB: Están tratando de hacer que todo quede eximido de la Ley de Libertad de Información (Freedom of Information Act) y mantenerlo en secreto. Así es como el Gobierno estadounidense afirma que tiene el derecho de enviar un emplazamiento administrativo, que posee un carácter inferior a una orden de allanamiento, en el que quien lo recibe tiene prohibido informarle al respecto al investigado, y este no tiene

---

69 «WikiLeaks demands Google and Facebook unseal US subpoenas», *The Guardian*, 8 de enero de 2011: <http://www.guardian.co.uk/media/2011/jan/08/wikileaks-calls-google-facebook-us-subpoenas> (consultado el 16 de octubre de 2012). Para más información, véase «Nota sobre los varios intentos por reprimir a WikiLeaks y a las personas vinculadas al proyecto» más arriba.

derecho a resistirse porque quien lo recibe es quien está directamente involucrado y tampoco tiene respaldo constitucional para proteger tus datos.

JULIAN: Siendo el emplazado Twitter, Facebook o tu proveedor de servicios de internet.

JACOB: O quien sea. Dijeron que se trataba de algo idéntico al secreto bancario y el uso de un teléfono. Al usarlo uno voluntariamente revela su número telefónico a la compañía telefónica. Sabías eso, ¿no? Al usar tu teléfono, cuando discas esos números, obviamente dices: «No tengo pretensión de privacidad». No es tan obvio con una computadora, ya que la gente no entiende cómo funciona internet —tampoco entiende cómo funcionan las redes de telefonía— pero los tribunales han fallado consistentemente que esto es así, y en el caso de Twitter, sobre lo que lamentablemente no puedo hablar porque no vivo realmente en un país libre, hasta ahora vienen afirmando esencialmente lo mismo.[70]

Es para volverse loco imaginar que les cedemos todos nuestros datos personales a estas compañías, y estas han devenido en policías secretas privatizadas. Y —en el caso de Facebook— hemos democratizado la vigilancia. En lugar de remunerar a los informantes como hacía la Stasi en Alemania Oriental, se los compensa por ser parte de una cultura: ahora consiguen con quien tener sexo. Ellos informan sobre sus amigos: «Tal y tal se comprometieron», «Oh, tal y tal se separaron», «Oh, sé a quién llamar ahora».

ANDY: Hubo quienes lograron presionar a Facebook, bajo la ley europea de Protección de Datos, para que entregara todos los datos almacenados sobre ellos y la cantidad de datos más pequeña era de 350 MB, la más grande rondaba los 800 MB.[71] Lo que resulta interesante es que la estructura de la base de datos de Facebook ha quedado al descubierto con esta ley. Cada vez que te conectas, el número IP queda almacenado, cada vez, cada clic que haces, además de la cantidad de tiempo que permaneces en una página lo que les permite asumir que te gusta, que no te gusta, etcétera. Pero esto reveló que el identificador clave de la estructura de la base de datos era la palabra «target» (blanco). Ellos no se refieren a estas personas como «suscriptores» o «usuarios», sino que los llaman *targets*, claro uno podría decir: «Bueno, ese es un término de marketing».

JULIAN: Pero era de uso interno era privado.

ANDY: Sí, pero en un sentido militar podría también significar blanco

---

70 Véase «Nota sobre los varios intentos por reprimir a WikiLeaks y a las personas vinculadas al proyecto» más arriba.

71 Para más detalles sobre el sitio Web Facebook *vs.* Europa: <http://www.europe-v-facebook.org/EN/Data_Pool/data_pool.html> (consultado el 24 de octubre de 2012).

(de ataques), podría significar blanco en el sentido de operaciones de inteligencia. De modo que solo es cuestión de las circunstancias en las que los datos son usados.

JULIAN: Bueno. Eso es lo que lo hace tan alarmante.

ANDY: Pienso que eso es muy útil. Solíamos decir que en Facebook el usuario no es realmente el cliente. El usuario de Facebook en realidad es el producto, y el verdadero cliente son las compañías publicitarias. Esa es la explicación menos paranoica y más inocua de lo que está sucediendo aquí.

Pero el problema es que uno no puede culpar a una compañía por acatar las leyes del país. Se lo denomina normal, y se lo denomina criminal si las compañías no acatan las leyes del país. De modo que resulta extraño decir: «Eh, están acatando la ley». ¿Qué tipo de acusación es esa?

JACOB: No; hay algo que tengo para cuestionarle a eso. Si tienes un sistema que lo registra todo sobre una persona y sabes que vives en un país con leyes que te forzarán a revelar toda esa información, entonces tal vez no deberías construir ese tipo de sistema. Y esta es la diferencia de enfoques entre privacidad por política y privacidad por diseño para desarrollar sistemas seguros. Cuando tu objetivo son las personas en el sentido de «target» y sabes que vives en un país que explícitamente vigila personas, entonces que Facebook coloque sus servidores en la Libia de Gadafi o en la Siria de Assad es un acto de negligencia. Y, sin embargo, ninguna de las Cartas de Seguridad Nacional[72] que fueron enviadas, el año pasado o hace dos años me parece,

---

72 Una Carta de Seguridad Nacional (NSL por sus iniciales en inglés), es una orden de una agencia estatal estadounidense solicitando «registros sin contenido» o «metadatos», como registros de transacciones financieras, registros de IP o contactos de correo electrónico. Cualquiera que reciba una NSL debe entregar los datos solicitados o atenerse a las acciones judiciales correspondiente. Una NSL no requiere de autorización judicial —puede ser emitida directamente por una agencia federal. Por este motivo, es similar a lo que se denomina un «emplazamiento administrativo» —una orden para presentar información que solo requiere supervisión administrativa y no judicial. En base a esto, podría decirse que las NSL violan las protecciones de la Cuarta Enmienda contra pesquisas e incautaciones. Las NSL además contienen una «mordaza», que prohíbe a quien recibe una NSL hablarle al respecto a otra persona lo que constituye un acto criminal. Y de esta manera, podría decirse que las NSL violan las protecciones de la Primera Enmienda de la libertad de expresión. En el caso Doe *vs*. Gonzales, la mordaza de las NSL fue declarada inconstitucional. Se modificó la ley para concederles a quienes reciban NSL el derecho a apelar la citación en la Justicia, lo que significó que para el Segundo Tribunal de Apelaciones la aplicación de la mordaza dejase de ser inconstitucional. Este derecho de apelación no siempre es ejercitado, ya que el secreto protege a quien podría hacerlo ya que el objeto de la investigación no sabe de su existencia. Las NSL siguen siendo objeto de críticas de grupos defensores de las libertades civiles y apeladas en la Justicia. El uso de las NSL aumentó sustancialmente luego de la aprobación de la Ley Patriota en 2001. Ilustra cuán difícil es justificar esto, el video de la Consejera General Adjunta del FBI intentando responder a la pregunta de Jacob Appelbaum, «¿Cómo se supone que

fueron por terrorismo. Por ejemplo, 250.000 de ellas fueron enviadas por otros motivos, pero no por terrorismo. Entonces sabiendo que esa es la realidad, estas compañías tienen una responsabilidad ética que surge del hecho que son ellos quienes están construyendo estos sistemas y quienes han tomando la decisión económica de traicionar a sus usuarios. Y esto ni siquiera es una cuestión técnica. Esto no tiene nada que ver con la tecnología, se trata de economía. Ellos han decidido que es más importante colaborar con el Estado, traicionar a sus usuarios, violar su privacidad y ser parte de un sistema de control —para ser retribuidos por ser parte de la cultura de la vigilancia por ser parte de la cultura del control— que resistirse; y de este modo pasan a formar parte de él. Son cómplices y responsables.

ANDY: La responsabilidad ética no es exactamente un atractivo comercial, ¿cierto?

---

voy a acudir a un juez si la otra parte tiene prohibido informarme que soy objeto de una investigación suya?» Su respuesta resulta escalofriante: «Hay ocasiones en las que debemos implementar cosas como esas», resulta escalofriante: <http://youtu.be/dTuxoLDnmJU> (también se encuentra acompañado de más material accesorio en Privacy SOS: <http://privacysos.org/node/727>). Según la Fundación Electronic Frontier, «De todos los peligrosos poderes la vigilancia estatal ampliados bajo la Ley Patriota, el poder de las NSL bajo el código estadounidense número 18, sección 2709, tal como fuera ampliado por la sección 505 de la Ley Patriota, es uno de los más aterradores e invasivos. Estas cartas enviadas a proveedores de servicios de comunicación como compañías telefónicas e IP le permiten al FBI solicitar en secreto datos sobre las comunicaciones privadas y la actividad en internet de ciudadanos estadounidenses comunes sin ninguna supervisión significativa o revisión judicial previa. Los destinatarios de las NSL están sujetos a una mordaza que les prohíbe para siempre revelar la existencia de dicha carta a sus compañeros de trabajo, a sus amigos o incluso a sus familiares y mucho menos al público». Véase <https://www.eff.org/issues/national-security-letters>. Véase también la colección de documentos relacionados a las NSL enviadas bajo la Ley de Libertad de Información de la Fundación Electronic Frontier: <https://www.eff.org/issues/foia/07656JDB> (todos los *links* fueron consultados el 23 de octubre de 2012).

RESISTIENDO LA VIGILANCIA TOTAL CON LAS LEYES DE LA FÍSICA

JÉRÉMIE: Un interrogante que podría surgir en esta instancia es cuál sería la solución tanto para un usuario individual como para la sociedad en su totalidad. Existen soluciones técnicas: servicios descentralizados, que todo el mundo aloje (*hosting*) sus propios datos, datos codificados, que todos confíen en proveedores afines que les brindan servicios de codificación y asistencia, etcétera. Y también están las políticas públicas de las que hemos hablado. No estoy seguro de que en este momento podamos responder a la pregunta de cuál de los dos enfoques es mejor. Creo que debemos desarrollar ambos en paralelo. Necesitamos contar con *software* libre que todo el mundo pueda entender, que todo el mundo pueda modificar, y que todo el mundo pueda examinar con el fin de estar seguro de lo que está haciendo. Creo que el *software* libre es una de las bases de una sociedad en línea libre, para poder controlar siempre a la máquina y no permitir que la máquina te controle a ti. Debemos tener una potente criptografía para asegurarnos de que tus datos si así lo deseas sean solo leídos por ti, y que nadie más pueda leerlos. Necesitamos herramientas de comunicación como Tor, o como Cryptophone, para poder comunicarte solo con las personas con las que te quieres comunicar. Pero el poder del Estado y de algunas compañías siempre superará el poder de los fanáticos de la informática (*geeks*) que somos, y nuestra capacidad de construir y difundir dichas tecnologías. También podríamos necesitar, mientras construimos estas tecnologías, leyes y herramientas que estén en manos de los ciudadanos para poder controlar lo que se esté haciendo con tal tecnología —aunque no sea en tiempo real— y para sancionar a aquellos que la usen de manera no ética y de forma tal que viole la privacidad de los ciudadanos.

JULIAN: Quisiera indagar en esta diferencia que veo entre la perspectiva criptopunk estadounidense y la europea. La Segunda Enmienda estadounidense consagra el derecho a portar armas. Hace poco vi unas imágenes que un amigo tomó en Estados Unidos en torno al derecho de portar armas, y en la marquesina de una tienda de armas había un cartel que rezaba: «Democracia, asegurada y cargada». Así es como te aseguras que no haya regímenes totalitarios: la gente está

armada y si se cabrea lo suficiente simplemente saca sus armas y retoma el control por la fuerza. Resulta muy interesante preguntarse si ese argumento es aún válido o no debido a la forma en que han cambiado los distintos tipos de armas en los últimos treinta años. Podemos remitirnos a la declaración de que la producción de códigos —criptografía secreta que el Gobierno no podría espiar— constituía en los hechos una munición. Luchamos esta gran guerra en los noventa para lograr que la criptografía esté disponible para todos, guerra que ampliamente ganamos.[73]

JACOB: En Occidente.

JULIAN: En Occidente ganamos ampliamente y están en todos los navegadores,[74] aunque es posible que ahora esté siendo subvertida y deformada de diferentes maneras. El tema es que no puedes confiar que un Gobierno implemente las políticas que dice estar implementando, de modo que nosotros debemos suministrar las herramientas básicas, herramientas criptográficas que nosotros controlamos, como una suerte de uso de la fuerza. Si la codificación es efectiva a pesar de todos los esfuerzos que haga un Gobierno no podrá entrometerse directamente en tus comunicaciones.

JACOB: La fuerza de casi toda la autoridad moderna proviene del ejercicio de la violencia o de la amenaza del ejercicio de violencia. Hay que reconocer que con la criptografía no hay suficiente violencia que pueda resolver un problema matemático.

JULIAN: Exactamente.

JACOB: Esto es la clave. No significa que no vayan a torturarte, no significa que no vayan a poner micrófonos en tu casa o a profanarla de algún modo, significa que si encuentran un mensaje cifrado no podrán resolver ese problema matemático por más que cuenten con la fuerza del aparato estatal. Esto, sin embargo, no resulta evidente para las personas sin conocimiento técnico, y tiene que quedar en claro. Si pudiésemos resolver esos problemas matemáticos, sería otra historia y por supuesto el primero sería el Gobierno.

JULIAN: Pero resulta que es un hecho de la realidad, como que se pueden construir bombas atómicas, la existencia de problemas matemáticos que uno puede crear y que incluso el Estado más poderoso no puede resolver. Pienso que eso fue tremendamente atractivo para los libertarios californianos y algunos otros que creían en esta suerte de idea de «democracia asegurada y cargada» porque es una forma muy

---

73 Véase nota 51 más arriba sobre las «Primeras guerras criptográficas» de los noventa.

74 Julian está haciendo referencia a SSL/TLS, que es un protocolo criptográfico que ahora se incluye de forma estándar en todos los navegadores, y que es usado para explorar de forma segura como, por ejemplo, para realizar transacciones bancarias.

intelectual de hacerlo: un par de tipos muñidos de criptografía enfrentados a todo el poder de la potencia más fuertes del mundo.

De modo que sí existe un atributo universal que está del lado de la privacidad, porque algunos algoritmos de codificación resultan imposibles de romper para el Gobierno que sea, jamás. Sabemos de otros que son extremadamente difíciles de romper incluso para la NSA. Lo sabemos porque ellos recomiendan esos algoritmos a los contratistas del Ejército estadounidense para proteger las comunicaciones militares secretas de Estados Unidos, y si hubiera algún tipo de resquicio en ellos los rusos o los chinos pronto lo encontrarían, lo que tendría severas consecuencias para quien haya tomado la decisión de recomendar un código inseguro. Los cifrados son muy buenos actualmente, confiamos bastante en ellos. Lamentablemente, uno no puede confiar a ciegas en la máquina en la que estás procesando dichos códigos, y eso es un problema. Pero eso no refiere a una vigilancia masiva sino a la interceptación de las computadoras de determinadas personas. A menos que seas un experto en seguridad, es muy difícil resguardar realmente una computadora. Pero la criptografía puede resolver gran parte del problema de la interceptación, y el problema de la interceptación a gran escala es lo que constituye una amenaza para la civilización mundial, la individual no es el peligro.

No obstante, soy de los que opinan que estamos lidiando con fuerzas económicas y políticas muy grandes, tal como dijo Jérémie, y el resultado más probable si tenemos en cuenta la eficiencia propia a las tecnologías de vigilancia y el número de seres humanos es que lentamente terminaremos viviendo en una sociedad totalitaria de vigilancia global. Por totalitaria me refiero a vigilancia total y entonces tal vez solo queden las últimas personas libres: aquellas que comprendieron cómo usar la criptografía para defenderse de esa vigilancia completa y total, y aquellos que vivan aislados de la sociedad, neoludistas que se han ido a las cuevas, o tribus tradicionales que no tienen ninguna de las comodidades de la economía moderna y que por tanto su capacidad de actuar es muy limitada. Por supuesto que cualquiera puede permanecer al margen de internet, pero entonces les resultará difícil ejercer alguna influencia. Ellos pierden la posibilidad de tener peso al hacer eso. Es lo mismo que con los teléfonos celulares, uno puede elegir no tener teléfono celular, pero de ese modo reduce su capacidad de influencia. No es la forma de avanzar.

JÉRÉMIE: Si lo analizas desde un punto de vista mercantil, estoy convencido de que existe un nicho de mercado en materia de privacidad que no ha sido muy explotado, tal vez haya un incentivo económico para que compañías desarrollen herramientas que den a los usuarios la capacidad individual de controlar sus datos y sus comunicaciones. Tal vez esta sea una forma para resolver ese problema. No estoy segu-

ro de que pueda funcionar por sí solo, pero puede que esto ocurra y que no lo sepamos aún.

JULIAN: La criptografía va a estar en todas partes. Está siendo utilizada por las principales organizaciones en todo el mundo, asemejándose a ciudades-Estado interconectadas. Si piensas en las vías de comunicación en internet —rápidos flujos de dinero entre países, organizaciones transnacionales, intercomunicaciones entre partes de organizaciones— todos esos flujos de información pasan por canales de comunicación poco confiables. Es como un organismo sin piel. Existen organizaciones y Estados que se están superponiendo y borroneando —cada red de influencia mundial compite por sacar ventajas— y sus flujos de información quedan expuestos a oportunistas, competidores estatales y demás. De modo que se están construyendo nuevas redes en la cúspide de internet, prácticamente redes privadas, y su privacidad proviene de la criptografía. Es por eso que el poder industrial es una de las razones que está impidiendo la prohibición de la criptografía.

Si tomamos el teléfono Blackberry por ejemplo, tiene un sistema de cifrado incorporado que funciona dentro de la red Blackberry. Research In Motion, la compañía canadiense que lo administra puede descodificar el tráfico de los usuarios y cuenta con centros de cómputos, como mínimo, en Canadá y el Reino Unido y por tanto la alianza anglo-estadounidense de inteligencia puede acceder a las comunicaciones mundiales entre Blackberrys. Pero las grandes compañías lo están usando por su mayor seguridad. Los Gobiernos occidentales estaban tranquilos al respecto hasta que trascendió a las corporaciones y llegó a los individuos, y luego vimos exactamente las mismas reacciones políticas hostiles que vimos en el Egipto de Mubarak.[75]

Pienso que la única defensa efectiva contra la inminente distopía de control es tomar uno mismo medidas para salvaguardar su propia privacidad, porque quienes cuentan con la capacidad de interceptarlo todo no tienen motivación para restringir sus actividades. Una analogía histórica podría ser la forma en que la gente aprendió a lavarse las manos. Para eso fue necesario que se estableciera primero y se popularizara después la teoría de los gérmenes como causante de las enfermedades, y que se instalara la paranoia respecto de la propagación de enfermedades a través de partículas que uno no podía ver, tal como uno no puede ver la interceptación en masa. Una vez que hubo suficiente conocimiento, los fabricantes de jabones empezaron a hacer productos para que la gente mitigara su miedo. Es necesario instalar

75 Para un ejemplo entre muchos, véase, «Blackberry, Twitter probed in London riots», Bloomberg, 9 de agosto de 2011: <http://www.bloomberg.com/news/2011-08-09/blackberry-messages-probed-in-u-k-rioting-as-police-say-looting-organized.html> (consultado el 16 de octubre de 2012).

el miedo en la gente para que comprenda el problema antes de que se genere suficiente demanda para resolverlo.

También hay un problema del lado opuesto de la ecuación, que es que los programas que afirman ser seguros, que afirman contar con criptografía incorporada, son a menudo fraudes, porque la criptografía es compleja, y el fraude puede estar oculto en la complejidad.[76]

Entonces las personas tendrán que pensar al respecto. La única pregunta es: ¿en cuál de las dos formas pensarán? ¿Pensarán, «necesito ser cuidadoso con lo que digo, necesito contenerme», todo el tiempo, en cada interacción? ¿O pensarán, «necesito dominar los pequeños componentes de esta tecnología e instalar lo necesario para estar protegido y poder expresar mis pensamientos en libertad y comunicarme libremente con mis amigos y seres queridos»? Si la gente no piensa de la segunda manera entonces tendremos una universalización de lo políticamente correcto e incluso cuando se comuniquen con sus amigos más cercanos aplicarán la auto-censura y dejarán de ser actores políticos del mundo.

76 Por ejemplo, un miembro del grupo LulzSec que expuso las fallas de seguridad de Sony cuando esta compañía divulgó los datos personales de sus clientes fue arrestado luego de que su identidad fuese obtenida del sitio proxy HideMyAss.com, mediante una orden judicial en Estados Unidos. Véase, «Lulzsec hacker pleads guilty over Sony attack», BBC, 15 de octubre de 2012: <http://www.bbc.com/news/technology-19949624> (consultado el 15 de octubre de 2012).

INTERNET Y POLÍTICA

JÉRÉMIE: Es interesante ver el poder de los *hackers* —«hacker» en el sentido primario de la palabra, no es un criminal. Un *hacker* es un aficionado a la tecnología, alguien a quien le gusta entender cómo funciona la tecnología, para no estar atrapado en la tecnología sino para hacerla funcionar mejor. Supongo que cuando uno tenía cinco o siete años tenía un destornillador y trataba de abrir artefactos para ver cómo era el interior. Esto es lo que significa ser un *hacker*, y los *hackers* construyeron internet por muchos motivos, entre ellos porque era divertido, y han desarrollado y compartido internet con todos. Entonces, compañías como Google y Facebook vieron la oportunidad de construir modelos comerciales basados en la recopilación de los datos personales de los usuarios. Pero aún vemos una forma de poder en manos de los *hackers*. Mi principal interés estos días es que estos *hackers* están acumulando poder, incluso en el terreno político. En Estados Unidos se han propuesto las leyes SOPA (Ley de cese de piratería en línea) y PIPA (Ley de protección de propiedad intelectual): agresivas legislaciones sobre derechos de autor que básicamente le dan a Hollywood el poder de ordenarle a cualquier compañía de internet que restrinja el acceso y censure contenidos en línea.[77]

---

77 SOPA se refiere a la Ley de cese de piratería en línea y PIPA, a la Ley de protección de propiedad intelectual. Son leyes propuestas por Estados Unidos que adquirieron preponderancia mundial a comienzos de 2012. Ambas son transparentes expresiones normativas del deseo de la industria de contenidos, representada por organismos como la Asociación de Industria Discográfica de Estados Unidos (RIAA, por sus iniciales en inglés), de hacer cumplir las leyes de protección de la propiedad intelectual a nivel global, y tan severamente como sea posible, en respuesta a la distribución gratuita/libre de productos culturales en línea. Ambas leyes proponían concederles amplios y severos poderes de censura a internet a agencias estatales estadounidenses, que amenazaban con «descomponer la red». Dichas leyes provocaron la ira de considerables porciones de la comunidad en línea internacional y generaron una fuerte reacción de actores de la industria cuyos intereses están en una red libre y abierta. A comienzos de 2012, Reddit, Wikipedia y varios miles de sitios más interrumpieron sus servicios a modo de protesta contra las leyes, lo que suscitó una fuerte presión de los usuarios sobre sus representantes públicos. Otros proveedores de servicios en línea, como Google, alentaron peticiones. En consecuencia, ambas leyes quedaron en suspenso, hasta que se reconsiderara y se debatiera si representan la mejor solución para el problema de la protección de la propiedad intelectual en línea. El episodio es visto como el primer descubrimiento y reafirmación del poder de *lobby* parlamentario efectivo por parte de la industria de internet.

JULIAN: Y bloqueos bancarios como el que está sufriendo WikiLeaks.[78]

JÉRÉMIE: Exactamente. Lo que le ocurrió a WikiLeaks con las instituciones bancarias devino en el método estándar de lucha contra los malvados piratas del derecho de autor que acabaron con Hollywood. Y fuimos testigos de un tremendo alboroto por parte de la sociedad civil en internet —y no solo en Estados Unidos—. No podría haberse logrado lo que se obtuvo si solo hubiesen sido ciudadanos estadounidenses quienes se levantaron contra las leyes SOPA y PIPA. Fueron personas de todo el mundo las que participaron, y los *hackers* estuvieron en el centro de la escena suministrando las herramientas para ayudar a los demás a participar en el debate público.

JULIAN: Para ayudar a armar la campaña.

JÉRÉMIE: ¿Fue acaso Tumblr o un sitio por el estilo en el que la página principal te permite ingresar tu número telefónico y recibes una llamada que te pone en contacto con el Congreso? Y así uno podía empezar a hablar con alguien y decirle: «Sí, esto es una porquería».

JACOB: Internet fue usada en defensa de sí misma.

JÉRÉMIE: Pienso que nosotros, los *hackers*, tenemos responsabilidad por las herramientas que construimos y le entregamos al resto del mundo. Y es posible que estemos empezando a ver cuán eficientemente pueda ser ejercida esta responsabilidad cuando lo hacemos de forma colectiva. Hoy en día, en la Unión Europea (UE) se está dando el debate en torno al Acuerdo comercial anti-falsificación (ACTA); es un tratado multinacional en el que se basaron las leyes SOPA y PIPA.[79] Acabo de regresar del Parlamento Europeo donde nosotros, individuos barbudos y hediondos, fuimos quienes les dimos letra a los miembros de un comité parlamentario. Les enseñamos artículos de las reglas de procedimiento del Parlamento Europeo que aparentemente estaban

---

78 Véase «Nota sobre los varios intentos por reprimir a WikiLeaks y a las personas vinculadas al proyecto» más arriba.

79 ACTA se refiere al Acuerdo comercial anti-falsificación. Es un tratado multinacional negociado en secreto durante años, con Estados Unidos y Japón a la cabeza, que en parte instituye nuevas y rigurosas obligaciones de proteger la propiedad intelectual. Los borradores iniciales del ACTA tomaron estado público en 2008 después de ser filtrados por WikiLeaks, provocando protestas generalizadas por parte de activistas por la libre cultura y defensores de internet. Véase la sección ACTA en WikiLeaks:<http://wikileaks.org/wiki/Category:ACTA>.
Cables diplomáticos estadounidenses compartidos con La Quadrature du Net por parte de WikiLeaks a comienzos de 2011 mostraban que el ACTA fue negociado en secreto explícitamente para acelerar la creación de extremas normas de verificación de IP, que más adelante podrían ser impuestas sobre países más pobres que no firmaron el acuerdo. Véase «WikiLeaks Cables Shine Light on ACTA History», La Quadrature du Net, 3 de febrero de 2011: <http://www.laquadrature.net/en/wikileaks-cables-shine-light-on-acta-history> (consultado el 23 de octubre de 2012).
En julio de 2012, tras una campaña encabezada por La Quadrature du Net y Jérémie Zimmermann, el ACTA fue derrotado en el Parlamento Europeo.

viendo por primera vez y les dijimos cómo comportarse, y luego se llevó a cabo una votación que ganamos por 21 a 5 que arrinconó al relator británico. Esta es una diminuta parte de un pequeño aspecto procesal en el camino hacia la derrota del ACTA, este monstruoso acuerdo global que ha sido diseñado a nuestras espaldas para evadir la democracia misma. Pero nosotros, en tanto ciudadanos, podremos acabar con ese monstruo —fácilmente, con herramientas de internet, las listas de correo, los sitios wiki, las salas de chat IRC, etcétera— y pienso que podríamos estar siendo testigos de la maduración, de la adolescencia de internet, y del modo en que puede ser usada por la sociedad en su conjunto para tratar de lograr el cambio. Creo que es tremendamente importante que nosotros, los *hackers*, estemos aquí con nuestro conocimiento técnico para guiar a las personas y decirles: «Deberían usar esta tecnología que les permite tener control sobre su privacidad en lugar de Facebook o Google», y que los dos se articulan juntos muy bien —o podrían articularse bastante bien. Esto nos hace sentir un poco de optimismo.

JULIAN: Jake, en cuanto a esta radicalización política de la juventud en internet, especialmente en los dos últimos años has estado por todo el mundo hablando sobre Tor, hablando con gente que desea el anonimato, quienes quieren privacidad respecto de su propio gobierno, y seguro has visto este fenómeno en muchos países diferentes. ¿Te parece algo significativo?

JACOB: Sin duda. Creo que es absolutamente significativo. El ejemplo más claro en el que puedo pensar inmediatamente es Túnez, adonde fui luego de la caída del régimen de Ben Ali y hablamos sobre Tor en una clase de ciencias de la computación, que cuenta con algunos docentes muy calificados, y una estudiante levantó la mano y dijo: «Y ¿qué hay con los malos?». Y ella recitó de memoria los cuatro jinetes del info-pocalipsis —el lavado de dinero, las drogas, el terrorismo y la pornografía infantil—. «¿Qué hay con los malos?». Como está claro que debemos acabar con esos cuatro grupos siempre son traídos a colación y se usa el miedo que producen para echar por tierra las tecnologías para preservar la privacidad. Entonces le pregunté a la clase: «¿Quién de los presentes ha visto alguna vez la página Ammar 404?» que es como allí llaman al mensaje «404 Not Found» que aparecía cuando se intentaba acceder a un sitio censurado durante el régimen de Ben Ali. Todos en el aula, excepto la persona que hizo esa pregunta, pero incluido el profesor de la clase, levantaron sus manos. Y yo miré a la muchacha que había formulado la pregunta y dije: «Mira a toda la gente a tu alrededor. Son todos tus compañeros de clase. ¿Realmente crees que valió la pena oprimir a cada una de las personas en este aula para luchar contra los malos?». Y ella dijo: «En realidad, yo también debo levantar la mano».

Fue un poco más prolongado que eso pero esencialmente cuando lo planteas en contexto, esas personas se dan cuenta de cuál es el punto de vista más sensato. Eso cambia la situación dramáticamente. Y esto ocurre en todo el mundo, todo el tiempo, pero usualmente a posteriori, lo que significa que la gente ve en retrospectiva que podrían haber usado la tecnología: «Ah, sí, resulta que no solo se trata de malas personas porque, de hecho, yo soy una mala persona si digo lo que pienso y a una persona en el poder no le gusta lo que estoy diciendo». Y uno ve una cierta toma de conciencia.

Pero es erróneo decir que solo ocurrió en los últimos años. Lamento hacerte esto Julian, pero tú eres parte de la radicalización de mi generación. Yo sería un criptopunk de tercera generación si tuviese que ponerlo en esos términos. El trabajo que tú y Ralf Weinmann hicieron sobre el sistema de archivos *rubberhose* fue parte de lo que me inspiró a trabajar en sistemas de archivos codificados. El sistema que diseñé, llamado MAID, fue en respuesta a los poderes regulatorios de investigación del Reino Unido, en el marco de los cuales el Estado ha decidido que la solución a la criptografía es la regulación negativa, con la que pueden confiscar tu contraseña.[80] Por supuesto, en el caso de Julian cuando crearon esto se debió a que regímenes totalitarios estaban torturando a personas para extraerles una contraseña de modo que uno debía poder entregar diferentes contraseñas para poder ceder ante los tormentos. Mi sistema de archivos criptográficos, MAID, fue diseñado para ser usado en un sistema legal en el que el acusado tiene el derecho a guardar silencio pero puede demostrar, si se lo obliga, que está diciendo la verdad sin violar la confidencialidad. Me di cuenta cuando vi el trabajo de Julian que uno podía usar la tecnología para

---

80 MAID, la Destrucción de Información Mutua Asegurada, es «una estructura que suministra un depósito remoto de claves con límite de tiempo y autenticación verificable con código de destrucción opcional. Automáticamente destruye claves criptográficas después de que se supera un límite de tiempo configurado por el usuario»: <https://www.noisebridge.net/wiki/M.A.I.D.>. Leyes como la Ley de Regulación de Poderes de Investigación de 2000, (RIPA, por sus iniciales en inglés), convierte al Reino Unido en un régimen bastante hostil para la criptografía. Bajo RIPA, los individuos pueden ser obligados a desencriptar datos o suministrar una contraseña por orden de un agente de policía. No se requiere supervisión judicial. Negarse a cumplir con la solicitud puede conducir a cargos criminales. En un posible juicio, si el acusado/a afirma haber olvidado la contraseña, se revierte la carga de la prueba. Para evitar ser condenado el acusado/a debe demostrar que se ha olvidado la contraseña. Esto, según sostienen críticos de la ley, efectúa una presunción de culpabilidad. En comparación, si bien ha habido muchos litigios vinculados a las mismas cuestiones en Estados Unidos, y la situación dista de ser ideal, se han obtenido muchos mejores resultados invocando la Primera y Cuarta Enmiendas en circunstancias similares. Véase el informe, «Freedom from Suspicion, Surveillance Reform for a Digital Age», publicado por JUSTICE, 4 de noviembre de 2011, disponible en: <http://www.justice.org.uk/resources.php/305/freedom-from-suspicion>. Para más información sobre el sistema de archivos *rubberhose*, véase «The Idiot Savants' Guide to Rubberhose», Suelette Dreyfus: <http://marutukku.org/current/src/doc/maruguide/t1.html> (todos los *links* fueron consultados el 24 de octubre de 2012).

que personas comunes tuvieran el poder para cambiar el mundo. Retrotrayéndonos hasta la antigua lista de correo criptopunk con Tim May, uno de los miembros fundadores, y leyendo los viejos comentarios de Julian en dicha lista, eso es lo que hizo que toda una generación se radicalizara, porque las personas se dieron cuenta de que ya no estaban atomizados, de que podían tomarse algún tiempo para escribir un *software* que pudiese fortalecer a millones de personas.[81]

Existen algunas consecuencias no intencionadas en la forma en que esto avanzó, porque la gente que creó Google no empezó sabiendo que lo iba a hacer ni que iba a originar la mayor máquina de control de la historia. Pero en los hechos eso es lo que pasó, y ni bien la gente empiece a darse cuenta empezarán a enviar las NSL, ¿no?

JÉRÉMIE: Pienso que hay tres elementos cruciales en lo que acabas de decir.

JACOB: ¿Solo tres?

JÉRÉMIE: Entre otros.

ANDY: Bueno, déjame añadir tal vez el cuarto elemento, ¿sí?

JACOB: No sabes a lo que me refiero aún.

JÉRÉMIE: Veo tres elementos imbricados. No digo que deban ser tomados por separado, pero uno de ellos son los regímenes autoritarios y los poderes que estos tienen en esta era de tecnologías digitales. En el caso del régimen de Ben Ali —lo que es obvio en tantos regímenes de hoy en día— se decidía aquello que la gente podía saber, o con quién comunicarse. Esto significa un tremendo poder y debería ser contrarrestado, e internet —una internet libre— es una herramienta para contrarrestar eso. Otro elemento es construir herramientas y una mejor tecnología, una tecnología capaz de evitar problemas tales como la censura, pero básicamente construir herramientas que sean parte de esa infraestructura que nos ayuda a derrocar dictadores. Y otro elemento aún es el relato político, esa fábula, que evocaste de los cuatro jinetes del info-pocalipsis, los pretextos usados a diario por políticos a través de los medios: «¿Moriremos todos por el terrorismo? Por lo tanto, necesitamos una Ley Patriota»; «Hay consumidores de pornografía infantil por todos lados»; «Hay pedófilos nazis por todo internet, por lo tanto necesitamos la censura».

JACOB: ¿Pedófilos nazis?

---

81 Puede descargarse un archivo de la antigua lista de correo criptopunk en: <http://cryptome.org/cpunks/cpunks-92-98.zip>.
Tim May fue un miembro fundador de la lista de correo criptopunk. Véase su Cypher-nomicon, una serie de preguntas frecuentes sobre la historia y filosofía criptopunk: <http://www.cypherpunks.to/faq/cyphernomicron/cyphernomicon.html> (ambos *links* fueron consultados el 24 de octubre de 2012).

JÉRÉMIE: Pedófilos nazis, sí —pedo-nazi.com tal como ya está registrado—. «Los artistas van a morir y ya no habrá cine, por lo tanto queremos darle a Hollywood el poder de ejercer la censura en internet», etcétera. Creo que aquí nuevamente internet es una herramienta, un antídoto para el relato político, que depende del estado emotivo y del marco temporal de los medios que es extremadamente breve: la información aparece y desaparece veinticuatro horas después y es reemplazada por nueva información. Con internet, tengo la sensación de que estamos dándole forma a lo que yo denomino el marco temporal de internet. Como internet nunca olvida, podemos armar expedientes durante años, día tras día, y podemos elaborar, podemos analizar. Esto es lo que hemos estado haciendo en los últimos tres años contra el ACTA. Una vez más, WikiLeaks ha sido una inspiración para nosotros porque el primer borrador de ACTA que se filtró fue publicado por WikiLeaks en 2008.[82]

JULIAN: Sí, nosotros lo levantamos.

JÉRÉMIE: Nosotros también filtramos dos versiones. Existieron cinco versiones de ese texto a lo largo de tres años que pudimos tomar y decir, párrafo por párrafo, línea por línea, este está haciendo esto, esta es la industria pidiendo esto, e involucrar a expertos en leyes y tecnología y construir una versión del relato político que era diferente de la oficial: «Oh, necesitamos el ACTA para salvar la cultura y salvar a los niños de los medicamentos adulterados», etcétera. Entonces construimos nuestra propia línea política con el marco temporal de internet, con análisis preciso, con mucho trabajo, conectando a las personas para que participen en eso.

JULIAN: Es verdad, y pienso que esa forma de ver el ACTA ha ganado a la opinión pública.

JÉRÉMIE: Hasta ahora todo bien.

JULIAN: Pienso que ese será el punto de vista histórico, pero tras bambalinas el denominado Acuerdo comercial anti-falsificación, que tiene su origen en la industria estadounidense de propiedad intelectual ha sido usado en realidad en muchos acuerdos bilaterales para tratar de crear un nuevo régimen internacional sobre qué es y no es legal en lo que a la publicación de contenidos respecta, y qué mecanismos existen para impedirlo. Este estandariza una versión más estricta del sistema estadounidense DMCA (El Acta de Derechos de Autor Digitales del Milenio), bajo el cual si le envías una carta a alguien exigién-

82 «Proposed US ACTA plurilateral intellectual property trade agreement (2007)», WikiLeaks, 22 de mayo de 2008: <http://wikileaks.org/wiki/Proposed_US_ACTA_multilateral_intellectual_property_trade_agreement_%282007%29> (consultado el 21 de octubre de 2012).

dole que borre algo de internet, este debe hacerlo, y existe una suerte de proceso de dos semanas durante el cual se pueden presentar contraargumentos pero como a cualquier editor de ISP le resulta caro ir a juicio simplemente lo bajan de inmediato, y permiten que el autor o quien lo haya subido dé esa batalla por su cuenta. El efecto de esto ha sido bastante fuerte en Estados Unidos, consiguiendo la remoción de muchísimo contenido. La cienciología abusó de este sistema para bajar literalmente miles de videos de YouTube.[83]

Entonces asumamos que el ACTA, al menos esta versión del tratado, ha quedado sin efecto en el Parlamento Europeo, con éxito de hecho. Pero parece que el ACTA sigue desarrollándose de todos modos —se ha dado el debate democrático, el ACTA ha sido demonizado en la esfera pública, hemos vencido en lo que al relato respecta, pero tras bambalinas se han estado firmando acuerdos bilaterales que están consiguiendo el mismo resultado, alterando el proceso democrático. Por ejemplo, WikiLeaks obtuvo e hizo público el nuevo acuerdo de libre comercio entre la UE e India, que incluye grandes pasajes del ACTA.[84] Eso ha estado ocurriendo con una serie de otros acuerdos y leyes. Puede que se decapite el ACTA pero su cuerpo será dividido en partes que conformarán nuevos tratados bilaterales. De modo que se pueden festejar victorias democráticas en la superficie pero por lo bajo se siguen haciendo las mismas cosas. Lo que muestra que no pienso que políticas públicas o reforma legislativa sean el camino; aunque no debes facilitarle la tarea a tu oponente porque sacará ventaja. De modo que es importante revisar dichos tratados de diversos enfoques, tal como está siendo verificado el ACTA. Los desacelera. Pero incluso una victoria en el Parlamente con respecto a la legislación no detiene esta actividad silenciosa.

JACOB: Algo que debe ser señalado, creo, es lo que dice Roger Dingledine, uno de los creadores de Tor, una suerte de mentor para mí y quien realmente me ha hecho pensar mucho acerca de cómo eludir la censura y el anonimato en línea, sobre cómo los *firewalls*, por ejemplo, no son técnicamente exitosos —y es importante comprender la tecnología detrás de los *firewalls* si quieres desarrollar una tecnología para resistirlos— aunque son socialmente exitosos. La gente que está luchando contra el ACTA está usando la tecnología para resistir, pero es la acción de la gente común lo que hay que comprender, la jerga técnica no es tan importante. Lo que importa es que la gente realmente se involucre en esta problemática y la cambie mientras tiene el poder de hacerlo, y el

83 «Massive Takedown of Anti-Scientology Videos on YouTube», Fundación Electronic Frontier, 5 de septiembre de 2008: <https://www.eff.org/deeplinks/2008/09/massive-takedown-anti-scientology-videos-youtube> (consultado el 16 de octubre de 2012).

84 «EU-India Free Trade Agreement draft, 24 Feb 2009», WikiLeaks, 23 de junio de 2009: <http://wikileaks.org/wiki/EU-India_Free_Trade_Agreement_draft,_24_Feb_2009> (consultado el 21 de octubre de 2012).

aspecto humano de eso es, de hecho la parte central. WikiLeaks ha difundido documentos que posibilitan eso, y compartir la información es importante, pero también lo son las personas que toman esa información y se la transmiten a la persona indicada. Porque está el argumento de que puede que muchos de nosotros vivamos en una democracia, que seamos libres, que se supone que somos gobernados a través del consenso. Y si todo el mundo comprende lo que está pasando y descubrimos que no es algo a lo que consentimos, entonces será muy difícil seguir adelante y aprobar esas leyes sin el apoyo de la ciudadanía.

JÉRÉMIE: Se trata de incrementar el costo político de tomar esas malas decisiones para quienes las toman, y nosotros podemos hacer eso de forma colectiva con una internet libre en tanto esté en nuestras manos.

JACOB: Pero se podría hacer sin internet también, porque —históricamente— hemos tenido sociedades libres antes de internet, solo que económicamente era más costoso, era más difícil en ciertos aspectos, y este es en realidad el motivo por el cual es tan importante el movimiento P2P.[85]

ANDY: El cuarto elemento, me parece, es que la dimensión arquitectónica de los sistemas descentralizados constituye un aspecto central que también debe ser accesible a la gente, porque ahora tenemos la computación centralizada en la nube.[86]

JULIAN: Facebook está completamente centralizado. Twitter está completamente centralizado. Google está completamente centralizado. Todos en Estados Unidos; todos pasibles de ser controlados por quien sea que controle las fuerzas coercitivas. Al igual que la censura que comenzó a implementarse luego de que WikiLeaks difundiera el Cablegate, cuando Amazon bajó nuestro sitio de sus servidores.[87]

---

85 *Peer-to-peer*, o P2P, se refiere a una red en la cual cada computadora puede funcionar como un cliente o servidor para todas las demás (cada computadora puede tanto enviar como recibir información), posibilitando el rápido intercambio de contenidos como música, videos, documentos o cualquier tipo de información digital.

86 La computación en la nube es aquella en la que muchas de las funciones tradicionalmente realizadas por una computadora, como almacenar datos (incluyendo los datos de los usuarios para varias aplicaciones), alojar y hacer funcionar *software*, y proveer la capacidad de procesamiento para correr el *software*, es realizado de forma remota, por fuera de la computadora misma, «en la nube» —generalmente por compañías que ofrecen estos servicios a través de internet—. En lugar de necesitar una computadora personal, todo lo que el usuario necesita es un dispositivo que pueda acceder a internet, y el resto le es provisto a través de internet. La metáfora «en la nube» no deja ver el hecho de que todos los datos y metadatos del usuario en realidad están en una computadora lejana en un centro de cómputos en algún lugar, que posiblemente sea controlado por una gran compañía como Amazon, y así los usuarios ya no tienen un control total sobre dichos datos.

87 Véase «Nota sobre los varios intentos por reprimir a WikiLeaks y a las personas vinculadas al proyecto» más arriba.

ANDY: Y la computación en la nube también ofrece un incentivo económico para que las compañías dispongan de una forma más barata de procesar sus datos en los denominados centros de cómputos internacionales administrados por corporaciones de Estados Unidos, lo que significa ingresar los datos a jurisdicción estadounidense, al igual que las compañías de pagos, etcétera.

JULIAN: Existe una tendencia dentro del viraje hacia la computación en la nube que resulta bastante preocupante. Existen enormes grupos de servidores en un solo lugar, porque es más eficiente estandarizar el control del entorno y el sistema de pagos. Es una técnica competitiva porque apilar servidores en un solo lugar es más barato que tenerlos dispersos. Gran parte de las comunicaciones que tienen lugar en internet, excepto *streaming* de películas, se da entre servidores, de modo que si colocas los servidores cerca se reducirán los costos. Entonces, terminamos teniendo estos grandes polos de servidores que se comunican entre sí. Tiene sentido para Google, por ejemplo, colocar sus servidores cerca de los grandes proveedores de contenido, o al revés, porque las páginas son indexadas por Google para que sean pasibles de ser buscados. De modo que en Estados Unidos hay enormes edificios que están llenos de servidores de diferentes compañías. Es allí donde la NSA instala sus nodos de interceptación en masa. Internet podría existir sin esta centralización, no es que tecnológicamente sea imposible, solo que resulta más eficiente contar con dicha centralización. En una competencia económica, la versión centralizada gana.

ANDY: Es muy importante entender la arquitectura del fenómeno — las infraestructuras centralizadas facilitan el control y el abuso del poder— esto es como eliminar el pequeño supermercado de barrio por un concepto de hipermercado centralizado.

JULIAN: Y como ir a una gran multinacional como Safeway.

ANDY: Sí, lo mismo que ocurrió con las compras minoristas. Es muy importante mantener una concepción de infraestructura descentralizada. Cuando formaba parte de ICANN, la Corporación de Internet para la Asignación de Nombres y Números, que provee y regula los nombres de los dominios en internet, aprendí algo de Vince Cerf, quien inventó al menos parte del protocolo TCP/IP, el protocolo fundamental de comunicación en internet. Él siempre solía decir: «Sabes, lo bueno de los Gobiernos es que nunca son singulares, siempre son plurales». De modo que incluso dentro de los Gobiernos, están los que quieren tener su esfera descentralizada de poder, e incluso dentro de los Gobiernos hay diferentes facciones luchando entre sí. Eso es lo que en última instancia nos salvará del Gran Hermano, porque habrá demasiados queriendo ser el Gran Hermano y tendrán que luchar entre sí.

JULIAN: No lo creo, Andy. Pienso que en el pasado había elites nacionales que competían entre sí, y ahora están conectándose entre sí y aprovechándose de sus respectivas poblaciones.

ANDY: Se están conectando, tienes razón en ese aspecto —y no estoy tan seguro de que eso vaya a salvar nuestro pellejo— pero realmente existe la posibilidad de conservar nuestra propia identidad. Debemos aferrarnos a nuestra propia infraestructura. Esa es la lección que debemos aprender aquí —que si queremos oponernos a un Estado de vigilancia estatal, *al* Gran Hermano, número 1 debemos estudiar qué es eso, si es en efecto una conexión de Estados centrales que dicen: «Eh, si sumamos fuerzas podemos ganar más poder aún». Y necesitamos saber cuál es nuestro rol aquí: nuestro rol es seguir descentralizados, contar con nuestra propia infraestructura y no depender de la computación en la nube y demás tonterías, sino contar con nuestra propia infraestructura.

JULIAN: Puede que tengamos el dominio de la técnica. Si es un hecho que resulta más fácil usar Twitter que crear tu propio Twitter; si es un hecho que es más fácil usar Facebook que DIASPORA, o alguna alternativa; si es un hecho que la computación en la nube es más barata, entonces esas técnicas y esos servicios dominarán.[88] La cuestión no es decir que debemos empezar nuestros propios servicios locales, porque estos simplemente no serán competitivos, y solo serán usados alguna vez por una pequeña minoría. Necesitamos algo mejor que decir que debemos contar con una versión de Facebook hecha por un hombre común y esperamos que la gente la use.

ANDY: Bueno, volviendo a la Iglesia católica, nos retrotraemos a tiempos en los que solo había un gran editor de libros, como Amazon que está tratando de controlar toda la cadena de suministro de libros electrónicos, de modo que es importante mantener nuestra capacidad de edición y producción. Puede que esto suene extralimitado, pero hemos visto lo que estas compañías pueden hacer si ellas o las agencias gubernamentales de las que dependen a nivel local quieren evitar que sucedan algunas cosas. Y pienso que el próximo paso obviamente tendrá que ser que podamos disponer de nuestro propio dinero, de modo que aunque no les guste el hecho de que apoyamos proyectos como WikiLeaks o lo que sea, tengamos nuestra propia forma de hacerlo sin depender de una infraestructura central que hace que todo pase por una jurisdicción.

---

88 DIASPORA es una red social que le permite a cada usuario funcionar como su propio servidor luego de instalar el *software* DIASPORA, permitiéndoles retener el control de sus propios datos. Fue creado como una alternativa más respetuosa de la privacidad que Facebook. Es propiedad de los usuarios y no tiene fines de lucro: <http://diasporaproject.org>.

JÉRÉMIE: Me gustaría estar de acuerdo con Andy. Pienso que la arquitectura importa y esto es un aspecto central de todo lo que impulsamos. Pero este es un mensaje que debemos transmitirle al público, porque lo entendemos, en tanto *hackers*, en tanto técnicos que construimos la red y jugamos con la red día a día. Y tal vez esta sea la manera de ganarnos las mentes y los corazones de la generación más joven. Pienso que este es el motivo por el cual las guerras sobre propiedad intelectual son tan esenciales, porque con las tecnologías *peer-to-peer*, desde Napster en 1999, la gente simplemente entendió que compartiendo archivos entre individuos...

JULIAN: Uno es un criminal.

JÉRÉMIE: No, uno contribuye al desarrollo de una cultura mejor.

JULIAN: No, uno es un criminal.

JÉRÉMIE: Ese es el relato, pero si uno contribuye al desarrollo de una mejor cultura para ti mismo, todo el mundo usará Napster.[89]

ANDY: La historia de la raza humana y la historia de la cultura es la historia de copiar ideas, modificarlas y procesarlas, y si denominas eso robar, entonces eres igual a todos los cínicos.

JÉRÉMIE: ¡Exactamente, exactamente! La cultura es para compartir.

JULIAN: Bueno, en Occidente, desde los cincuenta hemos tenido una industria de la cultura. Nuestra cultura se ha convertido en un producto industrial.

JÉRÉMIE: Estamos provocando al *troll* porque está jugando al abogado del diablo y lo está haciendo muy bien.

JACOB: No voy a caer. Es una estupidez tan obvia.

JÉRÉMIE: Es una estupidez. En el relato político se llama robar, pero quisiera dejar en claro que todos los que usaron Napster en 1999 se convirtieron en fanáticos de la música y luego asistieron a conciertos y empezaron a decirle a todo el mundo: «Debes escuchar a este grupo, debes ir a ese concierto» y así sucesivamente. De modo que la gente pudo experimentar cómo la tecnología *peer-to-peer* descentralizaba la arquitectura. En realidad, Napster estaba un poco centralizado en aquel entonces, pero sembró la idea de una arquitectura descentralizada. Todo el mundo vio cómo una arquitectura descentralizada le hacía bien a la sociedad, y cuando se trata de compartir cultura es exactamente lo mismo que cuando se habla de compartir conocimien-

89 El Napster original (1999-2001) fue un sistema pionero *peer-to-peer* para compartir música. Fue enormemente popular pero pronto fue dado de baja debido a las demandas legales por violación a las leyes de propiedad intelectual presentadas por la RIAA. Después de su quiebra, el nombre Napster fue comprado y usado para un tienda virtual de venta de música.

to. Compartir conocimiento es aquello a lo que nos referimos cuando hablamos de evitar la censura, o de atravesar el relato político para construir un mejor sistema democrático y una mejor sociedad.

Entonces, tenemos ejemplos en los que los servicios descentralizados y los individuos compartiendo conocimiento mejoran las cosas, y el contraejemplo es el abogado del diablo que Julian está encarnando, en el que una industria viene y dice: «Este está robando y este está aniquilando a todos, a los actores, a Hollywood, al cine, a los gatos, a todo». Ellos han ganado batallas en el pasado y es posible que ahora nosotros hagamos lo propio con el ACTA. Y una vez más tengo que diferir con el abogado del diablo que Julian estaba encarnando antes. El ACTA ha sido el ejemplo más acabado de incumplimiento de los principios democráticos, de sentarse frente al Parlamento, a las instituciones internacionales y la opinión pública e imponer medidas inaceptables por debajo de la mesa. Si logramos terminar con eso, entonces sentaremos un precedente y tendremos la oportunidad de promover una agenda positiva, y decir: «El ACTA está acabado, ahora hagamos algo que esté a favor del público». Y nosotros estamos trabajando con ese objetivo y algunos miembros del Parlamento Europeo ahora entienden que cuando los individuos comparten cosas, cuando comparten archivos sin fines de lucro, no deberían ir a la cárcel, no deberían ser castigados. Creo que si logramos eso tendremos un caso contundente para mostrarle al resto del mundo que compartir conocimiento, compartir información, hace que las cosas mejoren, que debemos promoverlo y no combatirlo, y que cualquier intento —ya sea legislativo o de un dictador o de una compañía— de alterar nuestra capacidad de compartir información y conocimiento de forma descentralizada debe ser contrarrestada; punto. Creo que podemos ganar suficiente impulso.

JULIAN: ¿Qué hay del debate sobre PIPA y SOPA en Estados Unidos? ¿Esta nueva legislación propuesta en el Congreso estadounidense para trabar embargos financieros y bloquear páginas de internet para proteger industrias estadounidense?

JACOB: Fue creada específicamente para atacar a WikiLeaks y a todo lo relacionado o similar a WikiLeaks.

JULIAN: El bloqueo financiero contra nosotros fue específicamente mencionado en el Congreso como una herramienta eficaz.[90]

JÉRÉMIE: Y se trató de entregarle esta herramienta a Hollywood.

JULIAN: Hicimos una gran campaña comunitaria contra el bloqueo y con el tiempo Google, Wikipedia y otros se sumaron a la campaña. Pero no dijimos: «Bueno, genial, hemos ganado la batalla». Eso me

90 Véase «Nota sobre los varios intentos por reprimir a WikiLeaks y a las personas vinculadas al proyecto» más arriba.

aterrorizó, porque Google de repente se vio a sí mismo como actor político y no solo como distribuidor, y sintió ese tremendo y enorme poder sobre el Congreso.

JÉRÉMIE: Google solo fue una parte de esa coalición contra SOPA y PIPA.

JACOB: Sí, pero Tumblr, me parece, tuvo una mayor incidencia.

ANDY: Tumblr y Wikipedia, miles de iniciativas individuales, acciones muy pequeñas sobre las que posiblemente nunca hayas escuchado, tuvieron incidencia. Hubo miles de estas actuando en paralelo —yendo en la misma dirección— y eso, nuevamente, es acción política descentralizada. Es un movimiento de política descentralizada del que hemos sido testigos. Posiblemente Google haya sido el mayor actor que notaste entre los otros.

JULIAN: Bueno, es lo que el Congreso dijo haber notado.

JACOB: Vuelvo a algo que Jérémie dijo anteriormente respecto a que tú esencialmente promueves la idea de una vanguardia política. No creo que haya sido premeditado, pero lo hiciste, y quisiera detenerte ahí mismo, porque el movimiento *peer-to-peer* está explícitamente en contra de una vanguardia política. Es la idea de que somos todos pares (*peers*) y que entre nosotros podemos compartir; puede que ofrezcamos diferentes servicios o que tengamos una funcionalidad diferente. Una vez Ross Anderson me dijo: «Cuando ingresé al movimiento *peer-to-peer* hace cincuenta años», lo que me pareció una apertura fantástica. Me explicó que quería asegurarse de que nunca des-inventásemos la imprenta. Porque cuando empezamos a centralizar servicios, cuando empezamos a centralizar el control operativo de los sistemas de información, en realidad empezamos a des-inventar la imprenta en el sentido que la *Encyclopedia Britannica* ya no imprime libros y solo edita CD —si no dispones de una computadora personal que pueda leer esos CD no tendrás acceso a ese conocimiento—. Ahora, en el caso de la *Encyclopedia Britannica* ya no importa porque tenemos Wikipedia y un montón de otro material. Pero no creo que en tanto sociedad estemos preparados.

ANDY: No estoy seguro de que Wikipedia sea tan bueno como fuente. No confío en una sola página de ese sitio que no haya reescrito yo mismo.

JACOB: Pero la *Encyclopedia Britannica* no es diferente. Es solo una fuente de muchas, y lo que importa es la verificación de los datos. Todo lo que quiero decir es que no deberíamos promover esta idea de vanguardia porque es muy peligrosa.

JULIAN: Un momento... ¿por qué? Yo constituyo una suerte de vanguardia. ¿Qué problema hay con las vanguardias?

JÉRÉMIE: No estoy hablando de vanguardias, solo estoy diciendo que ahora tenemos las herramientas en nuestras manos. Estábamos hablando de la imprenta. Otro visionario, un amigo mío, Benjamin Bayart, tal vez menos conocido por fuera del mundo franco-parlante, dijo: «La imprenta le enseñó a la gente a leer; internet le enseñó a escribir».[91] Esto es algo muy nuevo, esta es una nueva herramienta para que todos puedan escribir y expresarse.

ANDY: Sí, pero filtrar se está volviendo cada vez más importante estos días.

JÉRÉMIE: Seguro porque todo el mundo habla, y muchas personas dicen tonterías. Tal como el académico y activista Larry Lessig y, se me ocurre, tantos otros docentes te dirían: les enseñamos a las personas a escribir pero cuando los estudiantes presentan sus trabajos, noventa y nueve coma algo por ciento de ellos son un desastre, pero sin embargo les enseñamos a escribir.[92] Y entonces, por supuesto que la gente va a decir tonterías en internet: es obvio. Pero poder usar esta habilidad para expresarte en público mejora más y más tu destreza para participar en debates complejos y tu forma de expresarte a lo largo del tiempo. Y todos los fenómenos que estamos describiendo están construidos en torno a una compleja ingeniería que necesitamos descomponer en pequeñas partes para poder comprenderlas y debatir tranquilamente. No se trata de una vanguardia política sino de canalizar esta nueva capacidad de expresión que todos tenemos en nuestras manos a través del sistema político, de compartir nuestras ideas, de participar del conocimiento común sin pertenecer a un partido político, o a una empresa de medios, o a la estructura centralizada que sea que era necesaria en el pasado para poder expresarte.

---

91 Benjamin Bayart es el presidente de la Red Francesa de Datos (FDN, por sus iniciales en inglés), el ISP activo más antiguo de Francia, y defensor de la neutralidad en la red y del *software* libre. Véase su entrada en Wikipedia (en francés): <http://fr.wikipedia.org/wiki/Benjamin_Bayart> (consultado el 15 de octubre de 2012).

92 Larry Lessig es un académico y activista estadounidense mejor conocido por sus opiniones sobre propiedad intelectual y la cultura libre: Su blog es: <http://lessig.tumblr.com> (consultado el 15 de octubre de 2012).

INTERNET Y ECONOMÍA

JULIAN: Quisiera examinar las tres libertades básicas. Cuando entrevisté al líder del Hezbollah, Hassan Nasrallah...

JACOB: ¿Dónde está ese maldito ataque de aviones no tripulados? ¿Qué está ocurriendo allí arriba?

JULIAN: Bueno, él está bajo su propio tipo de arresto domiciliario también porque no puede abandonar su ubicación secreta.

JACOB: No estoy seguro de que yo haría esa comparación. Por favor no hagas esa comparación.

JULIAN: No está claro si Hezbollah reúne las características de un Estado —¿acaso se ha convertido en un Estado realmente? Esto es algo que se menciona en los cables de la embajada estadounidense, que Hezbollah ha desarrollado su propia red de fibra óptica en el sur del Líbano.[93] Por ende, cuenta con los tres principales ingredientes de un Estado —tiene el control de las fuerzas armadas dentro de una región determinada, tiene el control de la infraestructura de comunicaciones y tiene el control de la infraestructura financiera. Y podemos pensar en esto en función de las tres libertades básicas. La libertad de desplazamiento, la libertad física de movimiento — tu capacidad de viajar de un lugar a otro, que no desplieguen las fuerzas armadas en tu contra—. Podemos pensar en la libertad de pensamiento y la libertad de comunicación, que está inherentemente inserta en la libertad de pensamiento —si sobre ti pesa una amenaza por hablar en público, la única forma de salvaguardar tu derecho a comunicarte es hacerlo en privado—. Y finalmente, la libertad de interacción económica, que también está emparentada, al igual que la libertad de comunicación, a la privacidad de interacción económica. Entonces, hablemos de estas ideas, que han estado gestándose dentro del movimiento criptopunk desde los noventa, de tratar de

---

93 Hay mucho contenido fascinante en los cables diplomáticos estadounidenses publicados por WikiLeaks sobre este tema. Para algún debate interesante, consultar los siguiente cables (según referencia de identificación de cables, todos los *links* fueron consultados el 24 de octubre de 2012):
07BEIRUT1301: <http://wikileaks.org/cable/2007/08/07BEIRUT1301.html>.
08BEIRUT490: <http://wikileaks.org/cable/2008/04/08BEIRUT490.html>.
08BEIRUT505: <http://wikileaks.org/cable/2008/04/08BEIRUT505.html>.
08BEIRUT523: <http://wikileaks.org/cable/2008/04/08BEIRUT523.html>.

consagrar esta tan tercera libertad importante, que es la libertad de interacción económica.

JÉRÉMIE: Pero ¿por qué necesitarías solo tres libertades? En mi Carta Europea para los Derechos Fundamentales hay más.

JULIAN: La privacidad resulta importante desde el punto de vista de las comunicaciones, lo que significa que necesitas privacidad para comunicarte y pensar libremente, o la necesitas de algún modo para tu interacción económica. Por lo tanto pienso que hay más libertades derivadas, pero estas —las primeras tres que enumeré— son las libertades fundamentales de las que se desprenden otras libertades.

JÉRÉMIE: Bueno, existe una definición legal de libertad fundamental.

JULIAN: Pero yo he leído la Carta de la Unión Europea y puedo decirte que es un verdadero desastre en lo que a consensos se refiere.

JÉRÉMIE: Sí, bueno, y los diferentes *lobbies* lograron incluir la propiedad intelectual en la Carta de la UE.

JULIAN: Todo tipo de locuras.

ANDY: Pienso que hay un punto en el que podemos acordar, que es que el sistema monetario, la infraestructura económica para intercambiar dinero, es un desastre total en este momento. E incluso cualquiera que solo tenga una cuenta de eBay estará abiertamente de acuerdo con eso, porque lo que está haciendo PayPal, lo que están haciendo Visa y MasterCard, es poner realmente a las personas en una situación de monopolio de facto. También había algo muy interesante en los cables de WikiLeaks que decía que el Gobierno ruso trató de negociar una forma tal que los pagos de Visa y MasterCard de ciudadanos rusos dentro de Rusia tuviesen que ser procesados en Rusia, y Visa y MasterCard se negaron.[94]

JULIAN: Sí, el poder de la embajada estadounidense y Visa combinados fue suficiente para impedir que Rusia pudiera tener su propio sistema de pagos con tarjeta dentro del país.

ANDY: Lo que significa que incluso los pagos de ciudadanos rusos entre comercios rusos serán procesados por centros de cómputos estadounidenses. De modo que el Gobierno estadounidense tendrá control jurisdiccional, o al menos acceso a la información.

JULIAN: Sí, por ende cuando Putin sale a comprar una Coca-Cola, treinta segundos después Washington DC toma conocimiento de ello.

94 Véase identificación del cable 10MOSCOW228, WikiLeaks: <http://wikileaks.org/cable/2010/02/10MOSCOW228.html> (consultado el 24 de octubre de 2012).

ANDY: Y eso, por supuesto, es una situación muy poco satisfactoria, independientemente de mi opinión de Estados Unidos. Es simplemente muy peligroso tener en un país un lugar central donde todos los pagos estén almacenados, porque invita a todo tipo de usos de dichos datos.

JACOB: Una de las cosas fundamentales que los criptopunks reconocieron es que la arquitectura realmente define la situación política, de modo que si cuentas con una arquitectura centralizada, aunque los más aptos estén a cargo de ella, atraerá imbéciles y los imbéciles hacen cosas con su poder que los diseñadores originales (de dicha arquitectura) no harían. Y es importante saber que eso ocurre a cambio de dinero.

JULIAN: Como los pozos petroleros en Arabia Saudita: la maldición del petróleo.

JACOB: Sin importar dónde busquemos podremos ver, especialmente dentro de sistemas financieros, que no basta con que las personas efectivamente tengan las mejores intenciones. La arquitectura es la verdad. Es la verdad en internet respecto de las comunicaciones. Los denominados sistemas legales de interceptación, que es solo una linda forma de decir espiar a la gente...

JULIAN: Es un eufemismo, interceptación legal.

JACOB: Absolutamente, como un asesinato legal.

ANDY: O la tortura legal.

JACOB: ¿Has escuchado hablar sobre los ataques legales perpetrados por aviones no tripulados contra ciudadanos estadounidenses por parte del presidente Obama? Cuando mató al hijo de dieciséis años de Anwar al-Awlaki en Yemen, fue considerado un asesinato legal o muerte selectiva (*targeted killing*) como ellos lo denominan.[95] Lo que se denomina interceptación legal es lo mismo: solo colocas el término legal después de todo y de repente como el Estado lo hace, resulta que es legítimo. Pero en realidad es la arquitectura del Estado, la arquitec-

---

95 Para más información sobre el asesinato de ciudadanos estadounidenses sin el debido proceso véase Glenn Greenwald, «The due-process-free assassination of U.S. citizens is now reality», Salon, 30 de septiembre de 2011: <http://www.salon.com/2011/09/30/awlaki_6>. Y «The killing of Awlaki's 16-year-old son», Salon, 20 de octubre de 2011: <http://www.salon.com/2011/10/20/the_killing_of_awlakis_16_year_old_son>.
«Resulta literalmente imposible imaginar un repudio más violento del fundamento básico de la república que el desarrollo del brazo ejecutor de una agencia secreta y totalmente impune que simultáneamente recoge información sobre todos los ciudadanos y luego aplica una «matriz de disposición» para determinar qué castigo debe ser impuesto. Esta es una clásica distopía política hecha realidad»—Glenn Greenwald, «Obama moves to make the War on Terror permanent», *The Guardian*, 24 de octubre de 2012: <http://www.guardian.co.uk/commentisfree/2012/oct/24/obama-terrorism-kill-list> (todos los *links* fueron consultados el 24 de octubre de 2012).

tura de las leyes y la arquitectura de la tecnología las que le permiten hacer eso, al igual que la arquitectura de los sistemas financieros.

Lo que los criptopunks quisieron hacer fue crear sistemas que permitiesen compensarnos mutuamente de forma verdaderamente libre y que no se puedan interferir. Como las monedas chaumianas, que son divisas electrónicas diseñadas de acuerdo con las especificaciones de David Chaum, el creador de eCash (una moneda electrónica totalmente anónima), si bien se puede sostener que están más centralizadas de lo necesario. La idea es poder crear monedas electrónicas, a diferencia de Visa/MasterCard, que son divisas rastreables. Si bien están construidas en torno a una autoridad central, las monedas chaumian usan protocolos criptográficos inventados por David Chaum que posibilitan transacciones anónimas.[96]

JULIAN: Entonces, básicamente se trata de dinero electrónico pero sin el número de serie de los billetes, digamos.

JACOB: O números de serie que te permiten establecer que se trata de dinero válido pero no te dejan saber que Julian le pagó a Andy ni cuál fue el monto.

JÉRÉMIE: En realidad se está recreando el efectivo en el mundo digital.

JULIAN: Crear una divisa electrónica es un asunto complejo precisamente porque el control del medio de cambio es uno de los tres ingredientes del Estado, como dije con respecto a Hezbollah. Si le quitas al Estado el monopolio de los medios de interacción económica, le quitas uno de los tres principales ingredientes del Estado. En el modelo de Estado en tanto mafia, este vende «protección» y le saca dinero a la gente de toda manera posible. El control del flujo de divisas es importante para la recaudación de fondos del Estado, pero también es importante simplemente para controlar lo que la gente hace: incentivando una cosa, retirándole el apoyo a otra, prohibiendo por completo alguna actividad determinada u organización o interacciones entre organizaciones. Entonces, tomemos el extraordinario bloqueo financiero que pesa sobre WikiLeaks por ejemplo: no fue el libre mercado el que decidió bloquear a WikiLeaks, porque no se trata de libre mercado. Las regulaciones impuestas por el Gobierno

96 David Chaum es un criptógrafo e inventor de protocolos criptográficos. Es un pionero de las tecnologías en materia de divisas digitales e introdujo eCash, una de las primeras monedas electrónicas anónimas mediante criptografía. Las monedas chaumian son emitidas de forma central, pero hacen uso de la criptografía para garantizar las transacciones anónimas. Las monedas chaumian contrastan con bitcoin, otra moneda electrónica sobre la que se habla largamente más adelante, en que todas las transacciones son públicas, pero la divisa no tiene autoridad central. Para más información consultar *The Anonymity Bibliography, Selected Papers in Anonymity*, por Roger Dingledine y Nick Mathewson: <http://freehaven.net/anonbib> (consultado el 24 de octubre de 2012).

han declarado reyes a algunos actores financieros y no permiten el ingreso de otros. La libertad económica ha sido sitiada por una elite capaz de operar tanto sobre las regulaciones como sobre los principios implicados en estos bancos.[97]

ANDY: Es triste, pero este es el problema irresuelto del mundo electrónico en este momento. Dos compañías de crédito, ambas con infraestructura electrónica para realizar transacciones en suelo estadounidense —lo que significa tener acceso a la información dentro de los Estados Unidos— controlan gran parte de los pagos con tarjeta de crédito del planeta. Compañías como PayPal, que también está en jurisdicción estadounidense, aplican políticas estadounidenses, ya sea bloquear la venta de cigarros cubanos en sitios alemanes o los pagos a WikiLeaks por fuera de la jurisdicción estadounidense. Significa que el Gobierno estadounidense tiene acceso a los datos y la opción de imponer controles sobre movimientos a nivel mundial.

Si bien es posible que los ciudadanos estadounidenses sostengan que esta es la mejor democracia que el dinero pueda comprar, para los ciudadanos europeos esto simplemente no tiene precio.

JULIAN: En nuestro mundo tradicional hemos tenido libertad de movimiento hasta cierto punto, y no tanta en algunos casos.

JACOB: ¿Estás seguro, Julian? Creo que tu libertad de movimiento es un ejemplo clásico de lo libres que realmente somos.

JULIAN: Bueno, no. El Reino Unido ha anunciado que va a poner a 100.000 personas al año en mi misma situación.[98] Entonces pienso que hasta cierto punto ese es un daño colateral.

---

97 Para más información sobre el bloqueo a WikiLeaks véase «Nota sobre los varios intentos por reprimir a WikiLeaks y a las personas vinculadas al proyecto» más arriba.

98 Julian se refiere a los planes del Gobierno británico de incrementar el uso de dispositivos electrónicos. Véase «Over 100,000 offenders to be electronically tagged», The Guardian, 25 de marzo de 2012: <http://www.guardian.co.uk/society/2012/mar/25/prisons-and-probation-criminal-justice> (consultado el 22 de octubre de 2012).
Al momento de la presente conversación, Julian se encontraba bajo arresto domiciliario a la espera del resultado de su caso de extradición. Luego de su reclusión en solitario sin acusación en su contra en diciembre de 2010, Julian obtuvo el beneficio del arresto domiciliario tras pagar una fianza de 300.000 libras esterlinas. Como condición de su arresto domiciliario, debía estar recluido en un domicilio particular en determinadas horas, y este régimen era controlado por un dispositivo electrónico fijado a su tobillo, operado por una firma de seguridad privada contratada por el Gobierno del Reino Unido. Los movimientos de Julian eran controlados al punto que debía presentarse en una dependencia policial a diario, durante un lapso de tiempo, durante más de 550 días. Al momento de la publicación del presente libro, Julian se encontraba recluido en la embajada ecuatoriana en Londres, que está rodeada por la policía metropolitana de Londres las 24 horas del día. En junio de 2012 Julian ingresó a la embajada en busca de asilo político de la persecución que sufría del Gobierno estadounidense y sus aliados. Obtuvo el asilo en agosto de 2012.

JACOB: Este es el motivo por el cual los fundadores de mi país dispararon contra personas de Gran Bretaña. Existe un motivo por el que les disparamos a los británicos. ¡Y hoy todavía existe ese motivo! La tiranía existe.

JÉRÉMIE: No te lo tomes como algo personal.

ANDY: Lo que Estados Unidos, tu país, está haciendo es privatizar prisiones y negociar contratos que garanticen una tasa de ocupación del 90% para las compañías privadas que dirigen estas cárceles anteriormente administradas por el Gobierno estadounidense.[99] Y bien, ¿qué es eso? Esa es la expresión más absurda del capitalismo.

JULIAN: Hay más personas en prisiones estadounidenses que las que había en toda la Unión Soviética.

JACOB: Esta es la falacia en la que, porque yo cuestiono algo que está mal, tú puedes sugerir que yo soy parte de algo que está igualmente mal. No estoy sugiriendo que Estados Unidos sea perfecto. Pienso en realidad que Estados Unidos es un gran país en muchos sentidos, pero en particular en lo referente a la retórica de los Padres Fundadores.

JULIAN: La retórica de los Padres Fundadores está en un franco proceso de disolución de hace diez años a la fecha.

JACOB: No debemos olvidar que gran parte de la percepción de la retórica de los Padres Fundadores es una mitología y debemos ser cuidadosos en cuanto a idolatrarlos. Por lo tanto, sí, por supuesto. Todo lo que quiero decir con mi comentario sobre la tiranía británica y la situación en la que se encuentra Julian es que esto en realidad es un asunto cultural. Aquí es donde entra la sociedad y donde la sociedad tiene mucha importancia, y es muy difícil que la tecnología reemplace eso. Y las cuestiones financieras son el tema más peligroso para trabajar. Existe una razón por la que la persona que creó la otra moneda electrónica, bitcoin, lo hizo de forma anónima. No te conviene ser la persona que inventa la primera divisa electrónica realmente exitosa.[100]

---

99 «Is CCA Trying to Take Over the World?» Unión Estadounidense por los Derechos Civiles (ACLU, por sus siglas en inglés) 21 de febrero de 2012: <http://www.aclu.org/blog/prisoners-rights/cca-trying-take-over-world>.
«Passing House Bill will worsen already pressing civil rights issue», ANNARBOR.com, 2 de agosto de 2012: <http://annarbor.com/news/opinion/passing-house-bill-will-worsen-already-pressing-civil-rights-issue>.
Véase además «Goldman Sachs to invest $9.6m in New York inmate rehabilitation», *The Guardian*, 2 de agosto de 2012: <http://www.guardian.co.uk/society/2012/aug/02/goldman-sachs-invest-new-york-jail> (todos los *links* fueron consultados el 24 de octubre de 2012).

100 Bitcoin (<htt://bitcoin.org>) es la primera implementación verdaderamente exitosa de un clásico concepto criptopunk: la divisa criptográfica digital. A continuación se habla ampliamente de Bitcoin, pero se puede hallar una excelente explicación introductoria de la tecnología y la filosofía detrás de ella en «Understanding

JULIAN: Los que hicieron e-gold terminaron siendo llevados a juicio en Estados Unidos.[101]

JACOB: Es tan increíblemente frustrante.

JULIAN: Quisiera volver sobre estas tres libertades fundamentales: la libertad de comunicación, la libertad de movimiento y la libertad de interacción económica. Si observamos la forma en que nuestra sociedad adoptó internet a nivel global, cuando hicimos esa transición, la libertad de movimiento quedó esencialmente intacta. La libertad de comunicación en ciertos sentidos se vio enormemente mejorada, ya que ahora podemos comunicarnos con muchas más personas. Por otro lado, también se ha visto tremendamente degradada porque ya no hay privacidad, y por tanto nuestras comunicaciones pueden ser y son espiadas y almacenadas y, en consecuencia, pueden ser usadas en nuestra contra. Y por ende esa interacción elemental que tenemos con las personas físicamente se ve degradada.

ANDY: La privacidad está disponible pero tiene su costo.

JULIAN: Nuestras interacciones económicas han sufrido precisamente las mismas consecuencias. Ya que, tradicionalmente, ¿quién se enteraba de ellas? La gente que te veía ir al mercado. Ahora, ¿quién se entera de tus transacciones económicas? Si le compras algo a tu vecino con tu tarjeta Visa, lo que en una sociedad mercantil tradicional podrías haber hecho de forma casi privada, ¿quién se entera al respecto?

JACOB: Todo el mundo.

JULIAN: Todo el mundo se entera. Las principales potencias occidentales comparten la información sobre las transacciones y las almacenan para siempre.

ANDY: Julian, no está mal lo que estás diciendo, pero no estoy seguro de que realmente se pueda distinguir la libertad de comunicación de la libertad de interacción económica, porque internet tal como lo conocemos hoy es la infraestructura de todas nuestras interacciones económicas, culturales y políticas.

JACOB: Sin duda la de la libertad de movimiento.

Bitcoin», Al Jazeera, 9 de junio de 2012: <http://www.aljazeera.com/indepth/opinion/2012/05/201253094379316 77.html> (consultado el 22 de octubre de 2012).

101 e-gold fue un emprendimiento y moneda digitales creado en 1996. Los dueños y propietarios fueron imputados por el Departamento de Justicia de Estados Unidos por «conspiración para lavado de dinero». Ellos se declararon culpables, quedaron en libertad condicional cumpliendo arresto domiciliario y realizando servicios comunitarios. El juez que los sentenció afirmó que ellos merecían penas poco severas porque no habían participado intencionadamente de actividades ilegales. Véase, «Bullion and Bandits: The Improbable Rise and Fall of E-Gold», Wired, 9 de junio de 2009: <http://www.wired.com/threatlevel/2009/06/e-gold> (consultado el 22 de octubre de 2012).

ANDY: Sea cual fuera la arquitectura de la comunicación, el dinero es solo bits. Este es solo uno de los usos que se le dan a internet. Entonces si el sistema económico está basado en la infraestructura electrónica, la arquitectura de la infraestructura electrónica dice algo sobre cómo fluye el dinero, sobre cómo está siendo controlado, sobre cómo está siendo centralizado, etcétera. Internet tal vez no fue pensada como la infraestructura de todo al comienzo pero la lógica económica estableció: «Bueno, es más barato hacer eso con internet». Los bancos y las tarjetas de crédito previamente tenían cajeros automáticos con interfaces X.25, que era una red aparte hace diez o veinte años, y ahora todos tienen TCP/IP porque es más barato.[102] De modo que la arquitectura de la tecnología se está convirtiendo en un asunto central porque afecta a todas las otras áreas, y eso es lo que debemos realmente repensar, lo que significa que si queremos una forma descentralizada de manejar nuestros pagos, debemos tomar la infraestructura en nuestras manos.

JACOB: Bitcoin esencialmente es una moneda electrónica

ANDY: Que no tiene inflación.

JACOB: Tiende a darse de forma descentralizada, entonces en lugar de la Reserva Federal hay una serie de personas por todo el mundo que en conjunto acuerdan cuál es la inflación real, y cuánto vale su moneda.

JULIAN: Y existen algunos programas de computación que ayudan a hacer esto.

JACOB: Quisiera explicarlo de forma no-técnica. Bitcoin es una divisa electrónica que se parece más a un *commodity* que a una divisa en el sentido que es la gente la que determina cuántos euros vale un bitcoin. De modo que en ese aspecto se parece un poco al oro y lo que se denomina la extracción de bitcoins tiene su costo, cuando haces una búsqueda en una computadora para hallar un bitcoin, y la idea es que existe una complejidad informática ligada al valor de la cosa. Entonces, en términos no-técnicos, es una forma de enviarle divisas a Julian y que Julian confirme su recepción sin que Andy sea realmente capaz de interferir o impedirlo. No obstante, existen algunos problemas: no es realmente una divisa anónima, y esto en mi opinión es un aspecto realmente negativo.

---

102 Previo a internet, la red X.25 era la principal red global para intercambio de datos que existía en paralelo a la red telefónica. La facturación sobre X.25 estaba basada en la cantidad de datos enviados y recibidos, no en la duración de la conexión como ocurre en la red telefónica. Las puertas de enlaces (las denominadas PAD) permitían la conexión a la red X.25 desde la red telefónica con módems o acopladores acústicos. Para más detalles véase Wikipedia: <http://en.wikipedia.org/wiki/X.25> (consultado el 24 de octubre de 2012).

JULIAN: Bitcoin es un híbrido muy interesante, ya que los titulares de las cuentas son completamente privados y se puede crear una cuenta cuando uno lo desea, pero las transacciones de toda la economía Bitcoin son completamente públicas. Y así es cómo funciona; necesita ser así para que todo el mundo concuerde en que una transacción ha tenido lugar; que la cuenta de origen ahora tiene menos dinero y la cuenta de destino tiene más. Esa es una de las pocas maneras de administrar un sistema distribuido de divisas que no requiera de un servidor central, que sería un blanco atractivo para el control coercitivo. Lo realmente innovador de Bitcoin es la distribución y los algoritmos que la hacen posible para que no tengas que confiar en ninguna parte de la red financiera de Bitcoin. En cambio, la confianza está distribuida. Y la aplicación no se realiza por medio de la ley o de la regulación o la auditoría, sino que se hace mediante la complejidad criptográfica que cada parte de la red debe atravesar para probar que está haciendo lo que afirma estar haciendo. De modo que la honestidad de la red bancaria Bitcoin está incorporada en la arquitectura misma del sistema. Los cómputos se traducen en costos de electricidad para cada sede de la banca Bitcoin, de modo que podemos asignarle un costo a la comisión de fraude, en términos de precios de electricidad. En términos de costos de electricidad, el trabajo necesario para cometer fraude siempre será mayor que el beneficio económico resultante. Es muy innovador, no porque estas ideas no hayan sido exploradas antes (han sido estudiadas en papel durante más de veinte años), pero Bitcoin logró un equilibrio casi perfecto e incorporó una idea muy importante en cuanto a la manera de probar un verdadero consenso global respecto de las transacciones de la economía Bitcoin, asumiendo incluso que muchos bancos eran fraudulentos y que cualquiera podía crear uno.

Por supuesto que como con cualquier otra divisa, debes comprarla con alguna otra cosa; con trabajo, o los bitcoins son intercambiados por otra moneda —existen grupos de cambio que se encargan de eso—. Existen algunas otras limitaciones. Tiene un tiempo de liquidación de diez minutos aproximadamente: insume más o menos diez minutos de trabajo informático entre que una parte entrega el dinero y que la otra está segura de que existe un consenso global sobre la realización de la transacción. Es exactamente como el efectivo, de modo que tiene todos los problemas del robo que tiene el efectivo. Y también tiene todos los beneficios del efectivo: una vez que está en tu poder estás seguro de que has recibido el pago, el cheque no puede ser cancelado, el banco no puede dar marcha atrás. Se cortan los lazos de las relaciones de fuerza coercitiva. Por otro lado, debes cuidar bien del efectivo. Ese es, en mi opinión, su mayor problema. No obstante, es bastante fácil protegerlo con fideicomisos donde depositas tus bitcoins en un

servicio que está específicamente diseñado para mantenerlos a salvo y a resguardo contra robo.

JACOB: Lo que es interesante es que si quienes crearon Bitcoin hubiesen hecho que fuera obligatorio usar Tor para no crear una cuenta sino algunos identificadores criptográficos, habría sido posible —si todo pasara por Tor como diseño central— tener anonimato en cuanto a ubicación, aunque tuvieras identificadores a largo plazo que te localizaran para poder interconectar tus transacciones.

JÉRÉMIE: Sin entrar en consideraciones técnicas, podríamos acordar que Bitcoin tiene conceptos excelentes, pero presenta algunas fallas. Tiene una naturaleza deflacionista, porque el dinero tiende a desaparecer de Bitcoin. De modo que no puede funcionar a largo plazo, pero establece conceptos que pueden ser mejorados. Está en su versión 0.7 o 0.8 ahora.

JACOB: Esto es como David Chaum pero reelaborado.

ANDY: Bitcoin fue el intento más exitoso por implementar una moneda digital en los últimos diez años, diría yo.

JULIAN: Lograron un equilibrio casi perfecto. Creo que Bitcoin seguirá existiendo. Es una moneda eficiente; puedes crear una cuenta en diez segundos, y para transferir dinero no hay más gastos generales que el costo de la conexión a internet y unos pocos minutos de electricidad. Es altamente competitiva comparada a cualquier otra forma de transferencia de dinero. Pienso que prosperará. Mira lo que ocurrió luego de varios robos a Bitcoin y repercusiones negativas en la prensa en el verano (boreal) de 2011 que hicieron bajar la tasa de cambio a tres dólares.[103] Bitcoin ha vuelto a subir gradualmente a doce dólares. No ha subido o bajado bruscamente, ha subido siguiendo una curva gradual que parece mostrar una amplia demanda de la divisa. Sospecho que gran parte de la demanda radica en el comercio de drogas blandas, marihuana por correo, etcétera.[104] Pero Bitcoin tiene bajos gastos generales en tanto moneda. Varios ISP, especialmente en lugares donde no se puede acceder fácilmente a servicios de tarjetas de crédito, como la ex Unión Soviética, están empezando a usarla.

Si continúa creciendo veremos una embestida contra Bitcoin. Eso no lo hará desaparecer, porque la criptografía impide que funcione

---

103 Sobre el efecto negativo de la prensa, véase «Bitcoin implodes, falls more than 90 percent from June peak», arstechnica, 18 de octubre de 2011: <http://arstechnica.com/tech-policy/2011/10/bitcoin-implodes-down-more-than-90-percent-from-june-peak> (consultado el 22 de octubre de 2012).

104 Véase, por ejemplo, «The Underground Website Where You Can Buy Any Drug Imaginable», Gawker, 1 de junio de 2011: <http://gawker.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable> (consultado el 22 de octubre de 2012).

cualquier ataque por la fuerza coercitiva, pero el tipo de servicios de cambio que convierten de y a Bitcoin podrían ser tomados como blanco mucho más fácilmente. Por otro lado, estas operaciones pueden darse en cualquier lugar del mundo, de modo que hay unas cuantas jurisdicciones que sortear antes de que no haya más intercambios de este tipo, y luego el mercado negro tiene su propia lógica de cambio de divisas. Creo que la maniobra que debe ser ejecutada con Bitcoin es ser adoptada por los ISP y la industria de servicios de internet para estos pequeños juegos que compras en Facebook, porque es tan eficiente, y una vez que esté suficientemente adoptada por una variedad de industrias, estas formarán un grupo de presión para impedir que sea prohibida. Así es como la criptografía fue adoptada. Solía estar clasificada como tráfico de armas, y algunos de nosotros como tratantes de armas, pero una vez que estuvo presente en buscadores y empezó a ser usada para operaciones bancarias a través de internet, surgió un *lobby* lo suficientemente poderoso como para impedir que se prohíba —aunque concedo que existen nuevas iniciativas en ese sentido.

JACOB: El problema es que las preocupaciones por la privacidad son incorrectas. Seamos honestos. Es un error sugerir que es diferente con internet que sin internet. Cuando vine aquí y compré libras esterlinas tuve que presentar mi número de seguridad social, que es mi número de identificación personal en Estados Unidos, tuve que decir mi nombre, tuve que vincularlo a una cuenta de banco, tuve que darles dinero. Ellos tomaron nota de todos esos números y luego tomaron toda esa información y se la remitieron al Gobierno Federal. Esto es similar. En realidad, en Estados Unidos es más difícil conseguir divisas extranjeras debido a lo alejados que estamos del resto del mundo. Pero existe una tendencia histórica de control de divisas y no solo vemos este control respecto a internet. De hecho, según entiendo hay cajeros automáticos en los bancos que registran los números de serie de los billetes y luego los rastrean para realizar análisis de flujo del efectivo para determinar dónde ha sido gastado y quién ha hecho qué con él.

Si analizamos esos sistemas y luego analizamos la forma en que funciona internet, podemos concluir que la privacidad no mejoró cuando migramos a internet: de hecho, siguió siendo tan grave como lo era en un principio. Por eso pienso que es muy importante observar las tendencias del mundo previo a internet para ver hacia dónde vamos. Lo que vemos es que si tienes muchísimo dinero puedes pagar para mantener tu privacidad, y si no tienes muchísimo dinero casi seguramente no goces de privacidad. Y es peor con internet. Algo como Bitcoin es un paso en la dirección correcta porque cuando se lo combina con un canal de comunicaciones anónimas, como Tor por ejemplo, Bitcoin realmente te permite enviarle dinero a WikiLeaks a través de Tor y cualquiera que esté observando esta transacción verá a un

usuario de Tor enviando un bitcoin y a otro recibiendo uno. Es posible hacerlo, eso es mucho mejor que el efectivo en algunos sentidos.

JULIAN: Todos hablamos de la privacidad de la comunicación y del derecho a la divulgación. Eso es algo bastante fácil de entender —es una larga historia— y, en efecto, a los periodistas les encanta hablar al respecto porque están protegiendo sus propios intereses. Pero si comparamos ese valor con el valor de la privacidad y la libertad de interacción económica, cada vez que la CIA ve una transacción económica puede ver que se trata de esta parte en este lugar con esta parte en este otro lugar, y ellos saben cuánto vale y cuán importante es dicha interacción. Entonces, ¿no es acaso la libertad, o privacidad, de las interacciones económicas en realidad más importante que la libertad de expresión porque son estas las que realmente apuntalan toda la estructura de la sociedad?

JACOB: Están inherentemente conectadas. Pienso que puedes percibir la diferencia entre los criptopunks estadounidenses y los europeos en ese aspecto porque la mayoría de los criptopunks estadounidenses diría que son exactamente lo mismo. Porque en una sociedad que tiene libre mercado uno sostendría que respalda con acciones (o dinero) lo que expresa en palabras.[105]

JULIAN: Donde pones tu dinero es donde ubicas tu poder.

JACOB: Exactamente. No estoy diciendo que eso sea lo correcto, esa es casi una actitud de derecha, que posiblemente no sea lo que queremos. Tal vez queremos un capitalismo socialmente limitado, por ejemplo.

JULIAN: Si solo lo analizamos desde una simple perspectiva de inteligencia: cuentas con un presupuesto de inteligencia de 10 millones de dólares. Puedes espiar los correos electrónicos de las personas o puedes realizar una vigilancia total de sus interacciones económicas. ¿Cuál preferirías?

ANDY: Bueno, hoy en día ellos dirán: «Bueno, simplemente forzaremos a las compañías de pago y a los bancos a usar internet, para tener ambos». Y eso es lo que hicieron. Entonces el punto en efecto es que aquí no hay escape directo. Puedes hacer cosas como usar Tor para proteger tus comunicaciones, puedes cifrar tus llamadas telefónicas, puedes enviar y recibir mensajes seguros. Con respecto al dinero, es mucho más complicado y tenemos leyes contra el lavado de dinero y demás, y nos dicen que las organizaciones terroristas y narcotraficantes están abusando de la infraestructura para hacer cosas ilegales.

JACOB: Son los jinetes del info-pocalipsis.

---

105 En el original: «*you put your money where your mouth is*», dicho, uno de cuyos significados es que se apoya lo que se cree, en particular con dinero.

ANDY: En realidad, me interesaría mucho que haya más transparencia en las compañías de vigilancia y en lo que el Gobierno gasta en estas cosas. La pregunta es qué compramos cuando se ofrece el anonimato total del sistema monetario solamente. ¿Qué es lo que ocurriría en realidad? Creo que esto daría lugar a que aquí y allá gente con un poco más de tranquilidad diga: «Bueno, sabes, puedo alzar la voz, puedo acudir al Parlamento, pero puedo también simplemente sobornar a algunos políticos».

JÉRÉMIE: Estás describiendo a Estados Unidos, ¿verdad?

JACOB: No hay anonimato.

ANDY: No estoy seguro de que esto se limite a Estados Unidos. En Alemania no lo llamamos corrupción, lo llamamos fundaciones que compran pinturas firmadas por esposas de políticos, y por ende pasa por el mercado del arte u otros sectores. Tenemos mejores nombres para eso. Tal vez en Francia lo denomines partidos de la amistad y otros lo llaman contratar prostitutas.

JÉRÉMIE: Estados Unidos es un caso particular porque el nexo entre el sistema político y el dinero es muy estrecho. Lawrence Lessig dijo —después de trabajar durante diez años sobre propiedad intelectual—, que dejó de tratar de batallar (él en realidad no se rindió) porque descubrió que el problema no era la comprensión de lo que sería una buena política pública sobre derechos de propiedad intelectual por parte de los políticos, sino que había demasiados nexos con los actores industriales que estaban fomentando un mal régimen de propiedad intelectual.[106] Entonces nos encontramos frente a un verdadero problema.

JULIAN: ¿Estás seguro de que es un problema, Jérémie? Tal vez en los hechos es un buen atributo que aquellas industrias que son productivas...

ANDY: Pienso que el abogado del diablo está bebiendo mi whisky.

JACOB: Veamos si realmente puede terminar esta oración sin morirse de la risa. Provóquenos, maestro *troll*.

JULIAN: Esas industrias que son productivas, que generan riqueza para toda la sociedad, usan parte de su dinero para no dejar de ser productivas, eliminando leyes. Y la mejor forma de hacer esto, de hecho, es comprando legisladores, usando el producto de su industria productiva para modificar la ley, para mantener la naturaleza productiva de la industria.

---

106 Los primeros trabajos de Lawrence Lessig sobre propiedad intelectual y cultura (por ejemplo en su libro *Free Culture* de 2004) han sido reemplazados en los últimos años por el interés en la corrupción estadounidense a través del *lobby* parlamentario. Véase The Lessig Wiki: <http://wiki.lessig.org>.

JACOB: Espera. Yo me encargo de esta. ¿Listo? ¿No?

JULIAN: ¿Por qué?

JACOB: Hay un par de motivos, pero, para empezar, hay un ciclo de retroalimentación que es extremadamente negativo. Por ejemplo, entiendo que uno de los mayores contribuyentes a la campaña electoral del estado de California es el sindicato de guardia-cárceles, y esto explica en parte por qué les gusta hacer *lobby* a favor de leyes más estrictas. No es porque les interese el Estado de derecho sino porque para ellos tienen un incentivo laboral.[107] Entonces si estas personas están presionando para la creación de más prisiones, para encarcelar a más personas, para que estas tengan sentencias más prolongadas, ¿qué es lo que están haciendo en realidad? Lo que están haciendo es usar beneficios que reciben del trabajo que da beneficios —lo que es discutible— para expandir el monopolio que el Estado les otorga.

JULIAN: Entonces solo lo están usando para la transferencia de riquezas de industrias realmente productivas a industrias que no son productivas.

JACOB: Podrías resumirlo de ese modo.

JULIAN: Pero tal vez ese es solo un pequeño componente. Cada sistema es abusado, tal vez estos oportunistas que están solamente involucrados en la transferencia de riquezas constituyen un pequeño elemento, y de hecho la mayoría del *lobby*, la mayoría de la influencia sobre el Congreso realmente proviene de las industrias productivas que se aseguran que las leyes sigan permitiendo que aquellas industrias sean productivas.

JACOB: Pero eso se puede medir muy fácilmente porque uno puede detenerse a observar qué personas quieren promover actividades rentables y si no hubieran restringido las libertades de otras personas no habrían podido llegar a estar donde están parados hoy. Cuando hacen ese tipo de cosas sabes que algo ha salido mal y ellos solo protegen lo que tienen, que esencialmente han creado mediante la explotación —usualmente por medio de una apelación a las emociones en la que dicen: «Dios, detengan a los terroristas, detengan la pornografía infantil,

---

107 The California Correctional Peace Officers Association es un influyente grupo de presión en California que con frecuencia dona sumas de siete cifras en elecciones estatales, si bien no es, año a año, el mayor contribuyente a una campaña. Véase «California reelin», *The Economist*, 17 de marzo de 2011: <http://www.economist.com/node/18359882>. Y «The Golden State's Iron Bars», Reason, julio de 2011: <http://reason.com/archives/2011/06/23/the-golden-states-iron-bars>. Véase además la sección de California Correctional Peace Officers Association en el sitio Web Follow The Money del Instituto Nacional del Dinero en Políticas de Estado: <http://www.followthemoney.org/database/topcontributor.phtml?u=3286&y=0> (todos los *links* fueron consultados el 22 de octubre de 2012).

detengan el lavado de dinero, libren una guerra contra las drogas»—. Tal vez esas cosas son todas totalmente razonables en el contexto en el que fueron originalmente presentadas, y usualmente lo son, porque en términos generales pensamos que son malas porque existe un componente negativo en cada una de ellas.

ANDY: Quisiera volver al derecho de propiedad intelectual y darte otro ejemplo: hubo serios problemas cuando aparecieron los autos. Aquellos que dirigían compañías de transporte de pasajeros a caballo temieron que esto acabase con su negocio, que fue lo que ocurrió, pero tal vez también tenía sentido. Me invitaron a hablar en la Asociación alemana de compañías cinematográficas y antes de mi discurso hubo un profesor de una universidad de Berlín quien habló súper educadamente sobre la evolución de la raza humana y el desarrollo de la cultura, diciendo que copiar ideas y profundizar su desarrollo era la clave, al igual que hacer películas se trata de tomar temas y expresarlos de forma dramática. Después de cuarenta minutos, el moderador lo interrumpió descaradamente y dijo: «Bueno, después de que dijeras que debemos legalizar el robo, veamos qué tiene para decirnos el tipo del Chaos Computer Club». Y yo pensaba: «Guau, ¿qué carajo le pasa? ¿Me dejarán salir con vida si digo lo que pienso?». Es decir que algunas industrias tienen modelos comerciales que simplemente no les están siendo útiles a la evolución. Esto es egoísta: conservar el impulso des-evolutivo, haciéndolo más monopólico aún. Cuando aparecieron los casetes, también se pensó que acabarían con la industria discográfica. Y ocurrió lo opuesto, la industria discográfica se disparó. La pregunta es cuál es la política a aplicar aquí. ¿Cómo podemos formular estas cosas de forma positiva?

JULIAN: Yo solo me pregunto si no pudiésemos, de hecho, estandarizar la práctica vigente en Estados Unidos, y formalizarla de modo que simplemente compres a senadores y votos en el Senado.

JÉRÉMIE: No, no, no, no.

ANDY: Asumamos que tenemos el dinero.

JULIAN: Sí, y que todo ocurre abiertamente y hay compradores y cada uno va a una subasta.

ANDY: Pero la industria armamentística seguirá teniendo más dinero.

JULIAN: No, no creo que sea el caso. Pienso que el complejo militar-industrial estaría relativamente aislado porque su capacidad está en operar a puertas cerradas en un sistema que no está abierto a las ofertas del mercado general.

JACOB: Hay una inequidad fundamental en el sistema.

JÉRÉMIE: Desde una perspectiva económica liberal, antimonopólica, cuando dices dejemos que los actores dominantes decidan cuál será la política, puedo responderte con la experiencia de internet en los últimos quince años: donde la innovación surgió de abajo hacia arriba, donde las nuevas prácticas aparecieron de la nada, donde un par de tipos en un garaje inventaron una tecnología que se diseminó.

JULIAN: Para casi todo, Apple, Google, YouTube, para todo.

JÉRÉMIE: Por todo. Todo lo que apareció en internet fue un *boom* surgido de algo desconocido apenas meses o años antes, entonces no se puede predecir cuál será el próximo gran avance, y el ritmo de la innovación es más rápido que el ritmo de elaboración de políticas. Cuando se hace una ley que repercute en el mercado tal como es hoy en día, en las relaciones de fuerza entre los actores, puede que se fortalezca a uno que ya es fuerte y esto impedir la entrada de uno nuevo que podría haber sido eficiente.

JULIAN: El mercado debe ser regulado para ser libre.

JÉRÉMIE: Por supuesto que debes luchar contra los monopolios y debes tener un poder superior al de esas compañías para poder castigar las malas conductas, pero mi punto es que la política debe adaptarse a la sociedad, y no al revés. Tenemos la impresión de que en las batallas con relación a la propiedad intelectual[108] los legisladores tratan de que toda la sociedad cambie para adaptarse a un marco regulatorio definido por Hollywood, por ejemplo: «Bueno, lo que están haciendo con su nueva práctica cultural está moralmente mal, entonces si no quieren dejar de hacerlo, diseñaremos herramientas legales para que dejen de hacer lo que piensan que es correcto». Esa no es la forma de hacer buenas políticas públicas. Una buena política pública observa el mundo y se adapta a él para poder corregir lo que está mal y posibilitar lo que está bien. Estoy convencido de que cuando permites que los actores industriales más poderosos decidan cuáles son las políticas que deben aplicarse, no estás yendo en ese camino.

ANDY: Solo estoy tratando de hacer que pensemos cuál sería una buena política. Lo que planteaste es, en mi opinión, un poco complicado en este momento. Estoy tratando de simplificarlo un poco. Está este tipo llamado Heinz von Foerster —el padrino de la cibernética— quien una vez formuló una serie de reglas y una de ellas era: «Siempre actúa de forma tal que incrementes las opciones».[109] De modo que en

---

108 Véase nota 77.

109 Heinz von Foerster (1911-2002) fue un científico y arquitecto en cibernética austríaco-estadounidense. Su denominado «imperativo ético» o lema común es: «Actúa siempre para incrementar el número de opciones», o en alemán, «*Handle stets so, daß die Anzahl der Wahlmöglichkeiten größer wird*».

materia de política, tecnología o lo que fuera, siempre haz lo que te dé más y no menos opciones.

JULIAN: Una estrategia de ajedrez también.

ANDY: Se mencionó que el incremento en la privacidad de las transacciones monetarias podría tener un efecto negativo, entonces debemos pensar: «El sistema monetario en este momento tiene una lógica propia y la pregunta es cómo hacemos para que no acapare otras áreas». Porque el sistema monetario tiene la capacidad —a diferencia del sector de las comunicaciones— de afectar y limitar totalmente las opciones de las personas en otras áreas. Si puedes contratar asesinos a sueldo para hacer cosas específicas, o si puedes comprar armas e ir a la guerra con otros países, entonces estás limitándole al prójimo la opción de vivir, de actuar. Si inviertes más dinero en comunicaciones entonces más personas tendrán más opciones. Si colocas más armas en el mercado...

JACOB: No cuanta más capacidad de vigilancia tengas, más control tendrás.

ANDY: Lo cual es otro buen argumento para restringir el mercado armamentista, incluyendo la tecnología de vigilancia de las telecomunicaciones.

JACOB: Seguro, quieres restringir mi capacidad de vender eso, ¿cómo lo harías? ¿Cómo restringes mi capacidad para transferir dinero? También mediante redes de comunicaciones. Una de las cosas más ofensivas sobre los rescates a los bancos en Estados Unidos —que fueron irritantes para muchas personas por toda una serie de motivos— fue que demostraron que la riqueza solo es una serie de bits en un sistema informático. Mendigando de forma muy efectiva algunas personas lograron darles un muy alto valor a muchos de los bits, y entonces ¿qué hay que preguntarse? ¿Existe valor en el sistema si puedes simplemente burlarlo para poner tus bits arriba de la lista? Y ni siquiera se reconoce al resto del mundo que lucha por sobrevivir como poseedores de bits que ni vale la pena intercambiar.[110]

ANDY: Entonces lo que dices es que necesitamos un sistema económico totalmente diferente porque el valor hoy en día no está ligado al valor económico.

JACOB: No. Digo que sí existe un valor económico.

ANDY: Puedes hacer cosas negativas y generar dinero con eso, y puedes hacer cosas positivas y no obtendrás un centavo.

JACOB: Bueno, no. Lo que estoy diciendo es que no se puede separar la economía de la comunicación. No estoy hablando de si necesitamos

110 Jacob le atribuye esta observación a John Gilmore.

un sistema económico diferente o no. No soy economista. Solo voy a decir que existe algún valor en los sistemas de comunicación y en la libertad de dichas comunicaciones, tal como hay valor en la libertad de trueque: tengo el derecho a darte algo a cambio de tu mano de obra, tal como tengo el derecho a explicarte una idea y tú tienes el derecho a decirme lo que piensas al respecto. No podemos decir que el sistema económico existe en una suerte de vacío. El sistema de comunicación está directamente ligado a esto, y esto es parte de la sociedad.

Si vamos a tener una noción reduccionista de la libertad, de las tres libertades que Julian mencionó, esto está obviamente ligado a la libertad de movimiento, ni siquiera puedes comprar un boleto de avión ahora sin usar una divisa rastreable, de otro modo quedas marcado. Si entras a un aeropuerto y tratas de comprar un boleto con efectivo para ese mismo día, quedas marcado. Eres registrado en exceso, no puedes volar sin identificación y si corrieras con la mala suerte de comprar tu boleto de avión con una tarjeta de crédito, ellos acceden a toda tu información —tu dirección IP, tu buscador de internet—. Yo obtuve por medio de la Ley de Libertad de Información los registros del Servicio de Inmigración y Control de Aduanas de mis movimientos hace unos años, porque pensé que algún día sería interesante cotejar las diferencias. Y con seguridad figura Roger Dingledine, quien me compró un boleto de avión para un trabajo, su tarjeta de crédito, la dirección donde estaba cuando lo compró, el buscador que usó y todo sobre el boleto de avión.

JULIAN: Y esa información terminó en manos del Gobierno estadounidense: no quedó en el procesador comercial.

JACOB: Exacto. Los datos comerciales fueron reunidos, enviados al Gobierno y ellos los enlazaron. Y lo que encuentro realmente desquiciado es que se trata esencialmente de la fusión de estas tres cosas de las que hablas. Fue mi derecho a viajar libremente, mi capacidad de comprar ese boleto de avión o que alguien compre ese boleto de avión en mi lugar, y mi libertad de expresión —yo estaba viajando para disertar en algún lado, y para hacer eso tuve que hacer sacrificios en las dos otras esferas—. Y en efecto esto repercute en mi capacidad de expresarme, esencialmente cuando más tarde descubro lo que han reunido y elaborado sobre mí.

CENSURA

JULIAN: Jake, ¿puedes hablar un poco sobre las detenciones que has sufrido en aeropuertos de Estados Unidos y por qué han ocurrido?

JACOB: Ellos afirmaron que «yo sabía» por qué ocurría.

JULIAN: Pero ¿ellos no te dijeron por qué?

ANDY: Puedo tratar de resumirlo, porque la seguridad técnica y la seguridad de asuntos gubernamentales son dos cosas totalmente inconexas. Puede que tengas un sistema técnico totalmente seguro pero el Gobierno piensa que no sirve, porque para ellos hay seguridad cuando ellos mismos pueden investigar, tener el control y violar la seguridad técnica. Esto no fue porque Jake trató de acercarse a los aviones, de matar a alguien, de secuestrar una aeronave o algo por el estilo. Esto se trató de su capacidad de afectar los asuntos gubernamentales viajando a otros países, hablando con la gente y divulgando ideas. Eso es lo más peligroso que les ocurre a los Gobiernos estos días —cuando las ideas de la gente son mejores que sus políticas—.

JACOB: Agradezco totalmente tu cumplido en esa afirmación, pero solo me gustaría señalar que fue mucho peor que eso, porque esa es la información que recaban sobre todos. Esto fue antes de que yo hiciera cualquier cosa interesante; fue el mero hecho de estar viajando y el mismo sistema, su arquitectura, generó esta búsqueda de información. Esto fue antes de ser detenido por cualquier cosa, antes de ser deportado del Líbano, antes de que el Gobierno estadounidense se interesara particularmente en mí.

ANDY: Tal vez lo previeron, tal vez lo supieron antes que tu.

JACOB: Por supuesto que lo previeron, en parte debido a la recolección de la información. Pero ellos siempre me dieron respuestas diferentes. Usualmente ellos dan una respuesta tipo: «Porque podemos hacerlo». Y yo digo: «Bueno, yo no pongo en duda su autoridad —bueno, sí pongo en duda su autoridad, pero no lo hago ahora— solo deseo saber por qué me está ocurriendo esto». Y me dicen todo el tiempo: «Bueno, ¿acaso no es obvio? Trabajas en Tor», o, «Estás muy cercano a Julian, ¿qué esperabas?». Me tiene asombrado que cada una de las personas que me detiene —usualmente de la Oficina de Aduanas y Protección Fronteriza y del Servicio de Inmigración y Control de Aduanas— me dice que es porque

tienen la autoridad para hacerlo más que cualquier otra razón. También me han dicho estupideces como: «Oh, ¿recuerdas el 11 de septiembre? Ese es el motivo» o «Porque queremos que respondas algunas preguntas y aquí es donde menos derechos tienes, o así es como lo hacemos».

Y en estas situaciones te niegan el derecho a un abogado, no te permiten ir al baño pero te dan agua, te dan cualquier cosa de beber, como un diurético, para convencerte de que cooperes de algún modo. Ellos hicieron esto para ejercer presión sobre mí, por razones políticas. Me preguntaron qué pensaba sobre la guerra en Irak, sobre la guerra en Afganistán. Básicamente, en todo el transcurso repitieron las tácticas del FBI durante COINTELPRO (el enorme Programa nacional de operaciones encubiertas que se llevó a cabo entre 1956 y 1971). Probablemente, trataron específicamente de ejercer su autoridad para cambiar mis convicciones políticas, y presionaron no solo para que las cambie, sino para que les diera acceso a lo que estaba ocurriendo en mi cabeza. Confiscaron mis bienes. No soy realmente libre de hablar sobre todas las cosas que me han ocurrido porque estoy en una zona muy gris y no sé si estoy realmente autorizado a hablar sobre ellas. Estoy seguro de que esto les ocurrió a otras personas pero nunca he escuchado hablar al respecto.

Una vez estaba en el aeropuerto Pearson de Toronto volviendo a casa de un evento familiar. Volvía a Seattle adonde estaba viviendo en aquel momento y me detuvieron, luego me sometieron a una segunda inspección, y luego a una tercera y finalmente me metieron en una celda. Me tuvieron ahí dentro durante tanto tiempo que cuando fui finalmente liberado perdí mi vuelo. Pero hay algo curioso: estas zonas de pre-detención en realidad, técnicamente, son suelo estadounidense en suelo canadiense, y por tanto en ellas rige una norma que dice que si pierdes tu vuelo o falta mucho para el próximo vuelo, debes irte. Entonces técnicamente fui expulsado de Estados Unidos por estar detenido demasiado tiempo y entrar a Canadá, atravesar el país volando, alquilar un auto y cruzar la frontera. Y cuando llegué del lado de los Estados Unidos me dijeron: «¿Cuánto tiempo ha estado en Canadá?» a lo que yo respondí: «Bueno, cinco horas más la detención que sufrí en Toronto», por lo tanto había estado en Canadá unas ocho horas, y me dijeron: «Bien, pase, vamos a detenerlo nuevamente». Entonces procedieron a desarmar mi auto, tomaron mi computadora, la inspeccionaron y luego me detuvieron. Me permitieron ir al baño al cabo de media hora, fueron muy misericordiosos se podría decir. Y esto es lo que denominan una excepción en la inspección de frontera. Este tipo de conductas se debe a que tienen la autoridad, según afirman, de hacerlo, y nadie los cuestiona al respecto.[111]

---

111 Para más información sobre el hostigamiento de Jacob y otras personas asociadas a WikiLeaks, véase «Nota sobre los varios intentos por reprimir a WikiLeaks y a las personas vinculadas al proyecto» más arriba.

JULIAN: En Occidente, cuando hablamos de China y de su gran *firewall*, lo hacemos en términos de censura: qué se está impidiendo que los ciudadanos lean, qué dicen sobre el Gobierno chino en Occidente, qué dicen los chinos disidentes, qué dice la disciplina Falun Gong, qué dice la BBC y, para ser justos, qué dice la verdadera propaganda sobre China. Pero a los chinos con lo que he hablado no parece inquietarles la censura.

Su preocupación radica en que para que exista censura en internet también debe haber vigilancia. Para poder verificar lo que una persona está viendo en internet, para determinar si está permitido o no —en tanto Estado de control— debes estar viéndolo, y por lo tanto si lo estás viendo puedes registrarlo todo. Y esto ha tenido un tremendo efecto intimidatorio sobre la población china —no por sufrir la censura sino porque todo lo que leen está siendo vigilado y registrado—. De hecho, eso nos ocurre a todos. Esto es algo que cambia a las personas una vez que toman conciencia de ello. Cambia sus conductas y se vuelven menos perseverantes en sus reclamos ante las autoridades.

JACOB: Pero esa es la respuesta errónea a ese tipo de presión. El hostigamiento que sufro en las fronteras, por ejemplo, no me ocurre solamente a mí, ya que todo estadounidense de origen árabe, desde el 11 de septiembre y antes, ha tenido que enfrentarse a esto. Y yo me resisto a desperdiciar el privilegio de tener piel blanca y pasaporte estadounidense, y no guardo silencio al respecto porque las cosas que están haciendo están mal, y están abusando del poder que tienen. Debemos hacerle frente a este tipo de violaciones. Hay personas valientes en China que se están levantando ante esto, como Isaac Mao por ejemplo,[112] quien viene trabajando muy decididamente contra este tipo de censura, porque la respuesta correcta es simplemente no ceder ante este tipo de presiones solo porque el Gobierno afirma tener la capacidad de hacerlo.

JÉRÉMIE: Pero nuevamente estamos hablando de política porque lo que dices es que, básicamente, la gente debe luchar por sus derechos, pero las personas deben comprender por qué hacerlo y poder comunicarse entre sí para hacerlo. Tuve la oportunidad de conversar con algunas personas en China —y no sé si tenían algún cargo en el Estado, o si fueron seleccionados para hablar conmigo— pero al hablar con ellos sobre la censura en internet a menudo recibí como respuesta: «Bueno, es por el bien del pueblo. Existe la censura, sí, porque si no existiera entonces habría conductas extremistas, habría cosas que a todos nos disgustarían, entonces el Gobierno está tomando estas medidas para asegurarse de que todo vaya bien».

---

112 Isaac Mao es un bloguero, diseñador de *software* y capitalista de riesgo chino. Es cofundador de CNBlog.org y miembro del directorio del Proyecto Tor.

JACOB: Ese es el mismo argumento para la extracción de órganos. ¡No permitamos que esos órganos se echen a la basura!

JÉRÉMIE: Si observas la forma en que la censura es llevada a cabo en China, ves que, desde el punto de vista técnico, se trata de uno de los sistemas más avanzados del mundo.

JACOB: Absolutamente.

JÉRÉMIE: Y he escuchado que en Weibo —el equivalente chino de Twitter— el Gobierno tiene la facultad de filtrar algunos de los *hashtags* para asegurarse de que no salgan de una determinada provincia.

JACOB: Es crucial recordar que cuando las personas hablan de censura en Asia prefieren hacerlo en términos del «otro» —como si solo afectara a la gente en la República de Masallá. Es muy importante saber que cuando efectúas una búsqueda en Google en Estados Unidos, dice que hay resultados de búsqueda omitidos debido a requerimientos legales. Hay una diferencia entre los dos tipos de censura —tanto en cómo son implementados y, por supuesto, la realidad social del cómo, el porqué e incluso el dónde— pero una gran parte de eso es en realidad la arquitectura. Por ejemplo, la red estadounidense está muy descentralizada, por lo que resulta muy difícil ejercer la censura al estilo chino.

JULIAN: Bueno, una gran parte de la censura tiene que ver con Google y se puede condenar esa acción de Google. Hay miles de páginas que mencionan a WikiLeaks que están censuradas por Google.

JACOB: Sí, sin duda. Y en realidad como el índice mismo es libre, es posible realizar un análisis diferencial.

JULIAN: Sí, en teoría.

JACOB: En teoría. Y en la práctica hay algunas personas que están trabajando en ese tipo de detección de la censura observando las distintas perspectivas en el mundo. Creo que es importante recordar que la censura y la vigilancia no son problemas de «otros lugares» —a la gente en Occidente le encanta hablar de cómo «los iraníes, los chinos y los norcoreanos necesitan el anonimato y la libertad, pero nosotros no los necesitamos aquí»—. Y por «aquí» usualmente se refieren a «Estados Unidos». Pero en realidad no solo se da en regímenes opresivos, porque si resulta que estás en los más altos estamentos de cualquier régimen, tú no serás la víctima de la opresión. No obstante consideramos al Reino Unido como un lugar maravilloso; la gente piensa por lo general que Suecia es un gran lugar y, sin embargo, puedes ver que cuando pierdes el apoyo de quienes están en el poder terminas quedando en una posición desfavorable. Pero Julian todavía está con vida, ¿no? Entonces eso claramente significa que se trata de un país libre, ¿es correcto?

JULIAN: Yo trabajé duro para sostener mi posición actual. Pero tal vez deberíamos hablar de la censura en internet en Occidente. Es muy interesante. Si nos retrotraemos a 1953 y observamos la gran enciclopedia soviética, que se distribuía por todos lados, esa enciclopedia a veces incluía enmiendas cuando se renovaban los cargos políticos en la Unión Soviética. En 1953, Beria, el jefe de la NKVD, la policía secreta soviética, murió y perdió el prestigio del que gozaba y la sección de la enciclopedia que lo describía elogiosamente fue eliminada y se distribuyó una enmienda que debía ser pegada en todas las enciclopedias. Fue algo extremadamente obvio. Traigo este ejemplo a colación porque fue tan obvio y tan notorio que mismo el intento pasó a formar parte de la historia. Mientras que en el Reino Unido tenemos *The Guardian* y los otros grandes periódicos que eliminan material de sus archivos de internet en secreto y sin constancia alguna. Si uno va a las páginas de esos diarios e intenta encontrar esas notas, por ejemplo artículos sobre el caso del fraude del billonario Nadhmi Auchi, uno encuentra, «Página no encontrada», material que también ha sido suprimido de los índices.

Permítanme contarles sobre mi participación en la historia de Nadhmi Auchi. En 1990, Irak invadió Kuwait y eso dio lugar a la primera guerra del Golfo. El Gobierno kuwaití en el exilio, y también a su regreso, estaba necesitado de dinero, por lo que empezó a liquidar varios de sus activos incluyendo varias refinerías petroleras que tenía fuera de Kuwait. Nadhmi Auchi, un empresario iraquí que había emigrado al Reino Unido a comienzos de los ochenta y quien tenía un rol importante en el régimen de Saddam Hussein, negoció dicho acuerdo y fue subsiguientemente acusado de estar involucrado en el desvío de 118 millones de dólares en comisiones ilegales. Fue la mayor investigación de corrupción en la historia europea de posguerra. Auchi fue condenado por fraude en 2003, lo que pasó a conocerse como el escándalo de Elf Aquitaine. Sin embargo, hoy en día, él tiene más de 200 compañías a nombre de su conglomerado de empresas en Luxemburgo, y otras a través de Panamá. Él participa de contratos con compañías de telefonía celular en el Irak de posguerra y en muchos otros emprendimientos alrededor del mundo.[113]

Tony Rezko, un recaudador de fondos para la campaña de Barack Obama a senador, era un viejo amigo de Auchi, quien había sido su financista. Asimismo, Auchi y Rezko se involucraron con el exgobernador de Illinois, Rod Blagojevich. Tanto Rezko como Blagojevich fueron condenados por corrupción, Rezko en 2008 y Blagojevich en 2010-2011 (después de que el FBI grabara una llamada telefónica en la que trataba

113 Véase la página sobre Nadhmi Auchi en WikiLeaks: <http://wikileaks.org/wiki/Nadhmi_Auchi> (consultado el 24 de octubre de 2012).

de vender la antigua banca de Obama en el Senado). En 2007-2008, cuando Obama se postulaba como candidato a presidente del Partido Demócrata, la prensa estadounidense empezó a investigar las conexiones de Obama. Investigaron a Rezko y divulgaron algunos nexos sobre la compra de la casa de Barack Obama. En 2008, poco antes de su juicio, Rezko recibió una transferencia de Auchi por 3,5 millones de dólares sobre la que no informó a la Corte, a pesar de que se le había requerido que lo hiciera —hecho por el cual fue enviado a prisión—. Entonces, la atención de la prensa estadounidense recayó sobre Auchi quien, en ese momento, instruyó a sus abogados británicos de Carter-Ruck para que libraran una agresiva campaña contra gran parte de los reportajes sobre el escándalo de Elf Aquitaine de 2003 y su condena en Francia. Esto tuvo mucho éxito. Auchi puso a la prensa británica en la mira, e incluso a algunos *blogs* estadounidenses, y logró la eliminación de cerca de doce artículos sobre los que tenemos conocimiento. La mayoría de estos, incluyendo algunos de los archivos de periódicos británicos, simplemente desaparecieron. Fue como si nunca hubiesen existido. No hubo un aviso del estilo: «La nota ha sido eliminada a raíz de una solicitud del Poder Judicial». También desaparecieron de los índices. WikiLeaks investigó y los republicó.[114]

JACOB: Están borrando la historia.

JULIAN: No solo se modifica la historia, sino que deja de haber existido. Es el dicho de Orwell: «Quien controla el pasado, controla el futuro y quien controla el presente, controla el pasado». Es la indetectable tachadura de la historia al estilo occidental, y esta es la censura pospublicación. La autocensura previo a la publicación es mucho más extrema pero a menudo es difícil de detectar. Hemos visto eso con el Cablegate ya que WikiLeaks trabaja con diferentes socios mediáticos en todo el mundo, de modo que podemos ver cuáles censuran nuestro material.[115]

Por ejemplo, el *The New York Times* redactó un cable que decía que se habían distribuido millones de dólares para influir de forma encubierta a libios con conexiones con el Gobierno de Gadaffi por medio de compañías petroleras que operaban en Libia. El cable ni siquiera mencionaba una compañía petrolera en particular —el *The New York Times* simplemente redactó la frase «compañías de servicios petroleros».[116] El

---

114 Las notas pueden encontrarse en WikiLeaks: <http://wikileaks.org/wiki/Eight_stories_on_Obama_linked_billionaire_Nadhmi_Auchi_censored_from_the_Guardian,_Observer,_Telegraph_and_New_Statesman> (consultado el 24 de octubre de 2012).

115 Como comentario general tanto <http://cables.mrkva.eu/> y <http://cablegatesearch.net> ofrecen excelentes formas de comparar las versiones redactadas de los cables y las versiones completas, para ver lo que redactaron los socios mediáticos de WikiLeaks.

116 «Qaddafi's Son Is Bisexual and Other Things the New York Times Doesn't Want You to Know», Gawker, 16 de septiembre de 2011: <http://gawker.com/5840809/qaddafis-son-is-bisexual-and-other-things-the-new-york-times-doesnt-want-you-to-know-about>.

caso más flagrante probablemente haya sido el uso de *The New York Times* de un cable de sesenta y dos páginas sobre el programa misilístico de Corea del Norte, y sobre si le había vendido misiles a Irán, del cual el matutino neoyorquino usó dos párrafos para sostener, en un artículo, que Irán tenía misiles que podían atacar Europa, mientras que en el resto del cable se sostenía exactamente lo opuesto.[117]

The Guardian redactó un cable sobre Yulia Tymoshenko, la exprimera ministro de Ucrania, que decía que ella podría estar ocultando su riqueza en Londres.[118] El periódico censuró las acusaciones de corrupción en la elite kazaja en general —no se nombraba siquiera a una persona— y la acusación de corrupción contra ENI, la compañía de energía italiana que operaba en Kazajistán, y British Gas.[119] Esencial-

---

El ejemplo específico citado se refiere al cable cuya identificación de referencia es 06TRIPOLI198, WikiLeaks: <https://wikileaks.org/cable/2006/05/06TRIPOLI198.html>.

Las redacciones pueden ser analizadas visualmente en el sitio Cablegatesearch que muestra la revisión de la historia, donde las redacciones aparecen sombreadas en rosa: <http://www.cablegatesearch.net/cable.php?id=06TRIPOLI198&version 1291757400> (todos los *links* fueron consultados el 22 de octubre de 2012).

117 Para ver el cable original consultar el cable cuya identificación de referencia es 10STATE17263, WikiLeaks: <http://wikileaks.org/cable/2010/02/10STATE17263.html>.

Para acceder a la nota de *The New York Times*, véase «Iran Fortifies Its Arsenal With the Aid of North Korea», *The New York Times*, 29 de noviembre de 2010: <http://www.nytimes.com/2010/11/29/world/middleeast/29missiles.html?_r=0>.

El mismo cable fue usado por David Leigh de *The Guardian* para su artículo, «WikiLeaks cables expose Pakistan nuclear fears», *The Guardian*, 30 de noviembre de 2010: <http://www.guardian.co.uk/world/2010/nov/30/wikileaks-cables-pakistan-nuclear-fears>. La versión redactada del cable publicado por *The Guardian*, sin número de identificación de referencia, reducido a solo dos párrafos con relación a Pakistán. «US embassy cables: XXXXXXXXXXXX», *The Guardian*, 30 de noviembre de 2010: <http://www.guardian.co.uk/world/us-embassy-cables-documents/250573>.

El alcance de la redacción puede observarse visualmente en el sitio Cablegatesearch que muestra la revisión de la historia, donde la redacción de casi todo el documento aparece sombreada en rosa: <http://www.cablegatesearch.net/cable.php?id=10STATE 17263&version=1291486260> (todos los *links* fueron consultados el 22 de octubre de 2012).

118 Para ver el cable original consultar el cable cuya identificación de referencia es 08KYIV2414, WikiLeaks: <http://wikileaks.org/cable/2008/12/08KYIV2414.html>.

Para acceder a la versión redactada por *The Guardian* véase, «US embassy cables: Gas supplies linked to Russian mafia», 1 de diciembre de 2010: <http://www.guardian.co.uk/world/us-embassy-cables- documents/182121?INTCMP=SRCH>.

La redacción puede observarse visualmente en el sitio Cablegatesearch que muestra la revisión de la historia, donde las redacciones aparecen sombreadas en rosa: <http://www.cablegatesearch.net/cable.php?id=08KYIV2414&version=1291255260> (todos los *links* fueron consultados el 22 de octubre de 2012).

119 Para ver el cable original consultar el cable cuya identificación de referencia es 10ASTANA72, WikiLeaks: <http://wikileaks.org/cable/2010/01/10ASTANA72.html>. Para acceder a la versión redactada por *The Guardian* véase, «US embassy cables: Kazakhstan - the big four», *The Guardian*, 29 de noviembre de 2010: <http://www.guardian.co.uk/world/us-embassy-cables-documents/245167?INTCMP=SRCH>. La redacción puede observarse visualmente en el sitio Cablegatesearch que muestra la revisión de la historia, donde las redacciones aparecen sombreadas en rosa: <http://www.cablegatesearch.net/cable.php?id=10ASTANA72&version=1291113360> (todos los *links* fueron consultados el 22 de octubre de 2012).

mente, *The Guardian* censuraba las instancias en las que una persona rica era acusada de algo en un cable, a menos que *The Guardian* tuviera intereses institucionales contra esa persona adinerada.[120] Entonces, por ejemplo, en un cable sobre el crimen organizado en Bulgaria aparecía un ruso y *The Guardian* hizo como que todo tenía que ver con él, pero él solo era una persona en una larga lista de organizaciones e individuos vinculados al crimen organizado en Bulgaria.[121] *Der Spiegel* censuró un párrafo sobre lo que Merkel estaba haciendo —no preocupados por los derechos humanos—, cuestiones solamente políticas sobre Merkel.[122] Hay muchos ejemplos por el estilo.[123]

ANDY: Lo que nosotros entendemos por libertad de información y por libre flujo de información es un concepto nuevo y muy radical en algún sentido si observas el planeta Tierra. Diría que no hay mucha diferencia entre Europa y los otros países. Bueno, hay países con un

---

120 Véase, por ejemplo el cable cuya identificación de referencia es 09TRIPOLI413 sobre compañías de energía occidentales que operan en Libia. La representación visual en el sitio Cablegatesearch, donde las redacciones de *The Guardian* aparecen sombreadas en rosa, muestra que el periódico eliminó todas las referencias a los nombres de las compañías y sus ejecutivos, excepto las referencias a la compañía rusa Gazprom. Aunque parte del contenido resulte en algún sentido favorable para las compañías occidentales, las redacciones son elaboradas, y la versión redactada ofrece una imagen bastante diferente:<http://www.cablegatesearch.net/cable.php?id=09TRIPOLI413&version 1296509820> (consultado el 22 de octubre de 2012).

121 En este ejemplo el cable original tenía 5226 palabras. La versión redactada por *The Guardian* solo tenía 1406 palabras.
Para ver el cable original consultar el cable cuya identificación de referencia es 05SOFIA1207, WikiLeaks: <http://wikileaks.org/cable/2005/07/05SOFIA1207.html>.
Para acceder a la versión redactada por *The Guardian* véase, «US embassy cables: Organised crime in Bulgaria», December 1, 2010: <http://www.guardian.co.uk/world/us-embassy-cables-documents/36013>.
Para leer el artículo de *The Guardian* basado en el cable véase, «WikiLeaks cables: Russian government "using mafia for its dirty work"», *The Guardian*, 1 de diciembre de 2010: <http://www.guardian.co.uk/world/2010/dec/01/wikileaks-cable-spain-russian-mafia>.
El alcance de la redacción puede observarse visualmente en el sitio Cablegatesearch que muestra la revisión de la historia, donde las redacciones del documento aparecen sombreadas en rosa:<http://www.cablegatesearch.net/cable.php?id=05SOFIA1207&version=1291757400>.
Este ejemplo sobre Bulgaria es tratado por el socio mediático de WikiLeaks en Bulgaria Bivol en, «Unedited cable from Sofia shows the total invasion of the state by organized crime (Update: Cable Comparison)», WL Central, 18 de marzo de 2011: <http://wlcentral.org/node/1480>. Para más información, véase «The Guardian: Redacting, censoring or lying?» WL Central, 19 de marzo de 2012: <http://wlcentral.org/node/1490>. Cabe destacar también el comentario del periodista de *The Guardian*, David Leigh, debajo de ambas notas de WL Central y las consiguientes respuestas (todos los *links* fueron consultados el 22 de octubre de 2012).

122 Esto se refiere al cable cuya identificación de referencia es 09BERLIN1108. La redacción puede observarse visualmente en el sitio Cablegatesearch que muestra la revisión de la historia, donde las redacciones aparecen sombreadas en rosa: <http://www.cablegatesearch.net/cable.php?id=09BERLIN1108&version=1291380660> (consultado el 22 de octubre de 2012).

123 Para más ejemplos, véase el sitio cabledrum: <www.cabledrum.net/pages/censorship.php>.

marco democrático, lo que significa que puedes leer, comprender y tal vez incluso resistirte legalmente a la infraestructura de censura, lo que no significa que no exista, mientras que te resultará muy difícil hacer eso mismo en países como Arabia Saudita o China.

JULIAN: Mi experiencia en Occidente es que es tanto más sofisticado debido al número de capas de indirección y oscurecimiento de lo que está realmente ocurriendo. Estas capas existen para quitar posibilidades de contrarrestar la censura vigente. Se puede pensar en la censura como una pirámide. Solo la punta de esta pirámide asoma por sobre la arena, y esto es intencional. La punta es la parte pública —demandas judiciales, asesinatos de periodistas, cámaras decomisadas por militares, etcétera— la censura declarada públicamente. Pero ese es el menor de los componentes. Bajo la punta, la próxima capa consta de todas esas personas que no quieren estar en la punta, quienes incurren en la autocensura para no terminar allí. Luego, la capa siguiente constituye todas las formas de incentivos económicos o mecenazgos entregados a personas para que escriban sobre una cosa u otra. La capa que sigue hacia abajo es la economía en crudo —lo que resulta económico escribir, aunque no se incluyan los factores económicos de los estamentos superiores de la pirámide—. La capa siguiente es el prejuicio de los lectores que solo tienen un determinado nivel de educación, quienes por ende son fáciles de manipular con información falsa y a quienes no les puedes decir que algo sofisticado sea cierto. La última capa es la distribución —por ejemplo, algunas personas simplemente no tienen acceso a la información en un determinado idioma—. Así que esa es la pirámide de la censura. Lo que *The Guardian* está haciendo con las redacciones del Cablegate calificaría como la segunda capa.

Ahora, tal censura es fácil de negar porque es realizada de forma encubierta, o porque no hay instrucción de censurar una afirmación determinada. Rara vez se les indica a los periodistas: «No escriban nada sobre determinado tema» o «no consignen determinado hecho». En cambio, ellos comprenden que eso es lo que se espera que hagan porque conocen los intereses de aquellos a quienes se quieren acercar o a quienes quieren complacer. Si te comportas bien serás recompensado y recibirás una palmada en la espalda, y si no te comportas bien, no. Es así de simple. A menudo me gusta dar este ejemplo: la evidente censura que ocurrió en la Unión Soviética, la censura sobre la que se hizo tanta propaganda en Occidente —matones que se llevan periodistas de sus casas en medio de la noche— solo ha sido atrasada doce horas. Ahora esperamos que sea de día para quitarles las casas a los periodistas. Cuando estos pierden el patrocinio y no pueden honrar sus deudas se los saca de sus casas mediante la confiscación de sus propiedades. Las sociedades occidentales se especializan en el lavado

de la censura y en facilitar los asuntos de los poderosos de modo tal que si trasciende algún resto de discurso público este no afecte las verdaderas relaciones de poder de una sociedad altamente controlada, porque tales relaciones están ocultas bajo capas y capas de complejidad y hermetismo.

ANDY: Jérémie mencionó a los nazis pedófilos.

JACOB: Volvemos a los nazis pedófilos.

JÉRÉMIE: Dos jinetes en uno.

ANDY: Los nazis pedófilos resumen bastante bien los argumentos alemanes, o tal vez parte de los argumentos europeos, de la censura. Alemania no quería que en internet hubiera ningún contenido semejante al discurso del odio debido a su historia y, por supuesto, si les dices a las personas que necesitas aplicar una restricción sobre la red debido a la pedofilia entonces podrás hacer cualquier cosa. Además, hay un documento interno de la Comisión Europea sobre la interceptación de las telecomunicaciones que sostiene algo así como: «Debemos hablar más sobre la pornografía infantil para que la gente esté a favor de la censura».[124]

JULIAN: ¿Puedes hablar un poco de esto? Si tuviéramos que censurar algo, digamos la pornografía infantil, entonces para poder impedir que la gente la mire necesitamos vigilar todo lo que toda la gente está viendo. Necesitamos desarrollar esa infraestructura. Necesitamos construir un sistema de espionaje y censura en masa para reprimir una sola actividad.

ANDY: Es un detalle del mecanismo —lo que en Alemania se llama el sistema de pre-censura te obliga a dar el nombre de la persona legalmente responsable por lo que sea que publiques—. Entonces, a grosso modo, si publicas algo, ya sea en papel o en internet, sin decir quién es legalmente responsable por el contenido, estarás violando la ley. Esto significa que la responsabilidad recae en alguien y si se viola la ley dis-

---

124 «Intercepción de las telecomunicaciones. La Presidencia brindó información sobre el estado de la cuestión... Recordó el impacto negativo que este tema generó en los medios... En este contexto, la Presidencia reconoció de este modo que el progreso en la materia es muy lento... Varias delegaciones expresaron cautela en cuanto a la elaboración de un comunicado de prensa, observando que esto podría provocar una reacción en cadena y más repercusiones negativas en la prensa. La Comisión, si bien aclara que su posición no ha cambiado, informó a las delegaciones que una posible forma de salir del punto muerto podría ser una estrategia similar a la puesta en práctica para abordar el problema de la pornografía infantil en internet. Aunque reconoce que se trata de un tema diferente, también comprende la intercepción en cierta dimensión», Comisión Europea, encuentro de grupo de trabajo de cooperación policial sobre intercepción de telecomunicaciones, 13-14 de octubre de 1999. El documento completo se encuentra en: <http://www.quintessenz.at/doqs/000100002292/1999_10_13,Police%20Cooperation%20Working%20Group%20mixed%20committee%20meeting.pdf> (consultado el 24 de octubre de 2012).

tribuyendo, digamos, pornografía infantil o propagando el odio, simplemente se puede decir: «Bien, veamos dónde está ubicada esta persona, daremos con él y retiraremos ese contenido de internet».

JULIAN: Eso es censurar al editor en lugar de censurar al lector.

ANDY: Sí. Y esto es con relación a ver determinadas cosas. Podría estar de acuerdo en que no todo debe estar disponible en todo momento porque hay sitios que propagan el odio y dan direcciones privadas y cuestiones personales que podrían dar lugar a situaciones con las que no estoy de acuerdo.

JULIAN: Andy eso es algo tan alemán. Para hacer eso, para determinar qué es lo que será aceptable y lo que no, debes contar con un comité, debe haber nombramientos para conformar dicho comité, debes llevar adelante un proceso de selección de los integrantes a nombrar...

ANDY: Sí, tenemos toda esa estupidez. Las matanzas por parte de alemanes en la segunda guerra mundial —todo lo que los nazis hicieron, por cada propiedad que robaron dieron un recibo, para todo hicieron una lista. Todas eran acciones burocráticas. Se puede decir que los alemanes asesinaron injustificadamente a muchas muchísimas personas —lo cual es cierto— pero lo hicieron de forma burocrática. Así es Alemania.

JULIAN: Si hay alguien encargado de decidir qué debe ser censurado y qué no, entonces tienes que contar con dos cosas: primero que nada, debes desarrollar una estructura técnica para llevar a cabo la censura. Debes construir una máquina de censura nacional que lo haga eficazmente. Y, en segundo término, debes contar con un comité y una burocracia para ejercer dicha censura. Y ese comité debe ser inherentemente secreto porque sería completamente inútil si no fuera secreto y por lo tanto tendrás una justicia secreta.

ANDY: Y ¿sabes qué? Tenemos un buen principio en Alemania.

JACOB: ¿Solo uno?

ANDY: El principio es que si la aplicación de una ley no es realista, esta no debería existir. Si una ley no tiene sentido, como si prohibieses los molinos de viento, decimos: «Eh, vamos, olvídalo». Nosotros aquí nos inspiramos en internet tal como la hemos conocido cuando estaba creciendo, en el libre flujo de información, en el sentido de libre en tanto ilimitado, no bloqueado, no censurado, sin filtros. Entonces si aplicamos nuestra forma de ver el libre flujo de información en el planeta Tierra —y ha sido aplicada, en términos generales, a todo el planeta— vemos, por supuesto, que los Gobiernos se han visto afectados por esta y vemos la forma en que han aplicado el poder y manera en que la censura ha sido llevada a cabo, ya sea que se trate de precen-

sura, poscensura o el tipo que sea. Todos nosotros hemos aprendido sobre estos complicados conflictos que surgen. La pregunta es cuál es nuestro concepto de Gobierno o del futuro de una Organización Pos-Gubernamental (OPG) —tal vez WikiLeaks sea la primera o una de las primeras OPG— porque no estoy seguro de que los Gobiernos sean la respuesta correcta a todos los problemas en este planeta, como los problemas ambientales.

JULIAN: Los Gobiernos tampoco tienen la certeza de dónde está el límite que divide lo que es gobierno y lo que no. Dicho límite se ha desdibujado. Los Gobiernos ocupan el espacio, pero WikiLeaks ocupa parte del espacio de internet. El espacio que ocupa internet está integrado al espacio real, pero el grado de complejidad entre la integración y el objeto integrado hace que a la primera no le resulte fácil decirle al segundo que siquiera es parte de él. Este es el motivo por el cual tenemos esta sensación de ciberespacio —que en realidad es algún otro reino que existe en algún sitio— debido al grado de su indirección, complejidad y universalidad. Cuando lees un documento en internet desde una determinada ubicación, es lo mismo a leerlo desde otra ubicación o en el futuro: esa es la universalidad de la red. Entonces en ese sentido, en tanto una organización que ocupa el ciberespacio y que es hábil para mover su información por estratos subyacentes, tal vez seamos una organización posestatal debido a la falta de control geográfico.

No quiero llevar esta analogía demasiado lejos, porque estoy bajo arresto domiciliario. La fuerza coercitiva de los Estados obviamente se aplica a todos nosotros, sea donde sea que nos encontremos. Pero al resto de la prensa le gusta decir que somos una organización mediática apátrida y tienen bastante razón en cuanto a la importancia de la ausencia de Estado. Siempre solía decir: «Bueno, ¿qué crees que es Newscorp? Es una gran multinacional». Pero no obstante, Newscorp está estructurada de manera tal que uno pueda acceder a sus componentes centrales, y ese es el motivo por el cual ha tenido tantos problemas aquí en el Reino Unido con el escándalo de las escuchas telefónicas, y por el que está tratando tan arduamente de quedar bien con el *establishment* estadounidense. Pero si los activos de una organización son principalmente su información, entonces WikiLeaks puede tratarse de una organización transnacional en tanto que es bastante difícil de detener por medio de la criptografía. No es por nada que se montó un bloqueo financiero en contra nuestro: nuestras otras facetas organizacionales son más difíciles de eliminar.[125]

125 Véase «Nota sobre los varios intentos por reprimir a WikiLeaks y a las personas vinculadas al proyecto» más arriba.

JACOB: Si hablamos al respecto en términos utópicos, debemos retrotraernos a cuando me preguntaste sobre el hostigamiento que sufrí, me preguntaste sobre la censura en Occidente y yo me referí antes al programa de asesinatos selectivos de Obama, que dicen que es legal porque existe un proceso y por lo tanto cuenta como debido proceso.

JULIAN: Bueno, un proceso secreto.

JACOB: También podemos ligar esto a John Gilmore. Uno de los procesos que tuvo por su capacidad de viajar de forma anónima dentro de Estados Unidos terminó con una resolución de la Corte que decía: «Mire, vamos a consultar con la ley, que es secreta. La leeremos y averiguaremos cuando leamos esta ley secreta si usted puede hacer o no lo que tiene permitido hacer». Y luego de leer la ley secreta encontraron, en efecto, que tenía permitido hacerlo, porque lo que la ley secreta decía no se lo impedía. Él nunca supo qué decía la ley secreta y luego de ganar la demanda cambiaron las *políticas* de la Administración de Seguridad del Transporte y del Departamento de Seguridad Interior, porque resultó que la ley secreta no era lo suficientemente restrictiva en este sentido.[126]

JULIAN: ¿Y pasó a ser más restrictiva?

JACOB: Efectivamente, posibilitando leyes de la burocracia. Pero es importante observar que el programa de asesinatos selectivos, el hostigamiento que la gente sufre en las fronteras, la censura que encontramos en internet, la censura que las corporaciones llevan a cabo por orden de una entidad pública o privada, todas estas cosas están vinculadas. Y todo se reduce a que el Estado tiene demasiado poder en cada una de las áreas donde vemos aflorar estos hechos. Esto se debe a que el poder se ha concentrado en estos sectores y ha atraído a personas que abusan de dicho poder, o que pugnan por su utilización. Y aunque a veces haya casos legítimos, lo que vemos es que el mundo estaría mejor si no existiera dicha centralización, si no existiera la tendencia hacia el autoritarismo.

Occidente no es la excepción a la regla, porque resulta que si tienes al zar de la seguridad cibernética, bueno, no es muy diferente al zar

126 Jacob se refiere a Gilmore *vs.* Gonzales, 435 F.3d 1125 (9° Circuito, 2006). John Gilmore, un criptopunk de la primera época, llevó su caso hasta la Corte Suprema de Estados Unidos para revelar los contenidos de una ley secreta —una Directiva de Seguridad— que restringía el derecho de los ciudadanos a viajar en avión sin identificación. Además de afirmar que dicha cláusula era inconstitucional, Gilmore objetaba el hecho de que la cláusula misma era secreta y no podía ser revelada, aunque tuviera efectos vinculantes para los ciudadanos estadounidenses. La Corte consultó la Directiva de Seguridad a puertas cerradas y falló contra Gilmore en cuanto a la constitucionalidad de la Directiva. Sin embargo, los contenidos de la ley nunca fueron revelados durante el curso del proceso. Véase Gilmore *vs.* Gonzales en PapersPlease.org: <http://papersplease.org/gilmore/facts.html> (consultado el 22 de octubre de 2012).

que estaba en las fuerzas de seguridad de otra nación hace cincuenta años. Estamos construyendo el mismo tipo de estructuras autoritarias de control, que atraerán personas que abusarán de dichas estructuras, y eso es algo que en Occidente hacemos de cuenta que es distinto. No es diferente en Occidente porque hay una variedad de gobiernos que va del autoritarismo al liberalismo. No estoy hablando de los partidos políticos estadounidenses, sino que en esa variedad Estados Unidos está muy lejos de la Unión Soviética en muchos aspectos, pero está mucho más cerca de la Unión Soviética que de Cristiania, el barrio autónomo que se encuentra en el corazón de Copenhague, Dinamarca.[127] Y me parece que está incluso más lejos de un posible mundo utópico si alguna vez establecemos una colonia en Marte. Seguro que vamos a querer que lo que hagamos en Marte esté tan lejos del totalitarismo y el autoritarismo como podamos. Estos son defectos cuando no tenemos eso.

JÉRÉMIE: Una vez más, todos estos temas están imbricados. Cuando hablamos de concentrar poder hablamos nuevamente de arquitectura. Y cuando hablamos de censura en internet, nos referimos a centralizar el poder para determinar lo que la gente puede o no puede ver, y a si la censura oficial o privada constituye un poder indebido. Tenemos este ejemplo: nuestro sitio laquadrature.net estuvo censurado en el Reino Unido por Orange UK durante varias semanas. El sitio figuraba en una lista de sitios a los que Orange les negaba el acceso a menores de dieciocho años. Tal vez mencionamos el término pornografía infantil cuando nos opusimos a ese tipo de legislación, o tal vez no les caímos bien porque nos oponemos a sus políticas contra la neutralidad en la red, dado que nosotros propugnamos por una ley para impedirles que discriminen las comunicaciones de sus usuarios.[128] Nunca lo sabremos. Pero aquí tenemos un actor privado que, como servicio, estaba impidiendo que la gente accediera a cierta información en internet. Veo un gran riesgo en esto más allá del poder que le damos a Orange o al Gobierno de China o del país que sea.

JACOB: Aclaremos algo —cuando dices privado en el Reino Unido, ¿quieres decir que ellos realmente son propietarios de cada línea, de cada conexión de fibra óptica y todo o ellos usan algún tipo de recurso estatal? ¿Cómo fueron adjudicadas las ondas? ¿No hay participación del Estado en absoluto? ¿Hubo negligencia?

---

127 Cristiania es una zona autoproclamada independiente en Copenhague, Dinamarca. Unas viejas barracas del ejército fueron ocupadas en los setenta por una comunidad anarquista. Ha forjado un singular estatus legal en Dinamarca.

128 El principio de «neutralidad en la red» requiere que a los ISP se les impida (por ley, según se sostiene usualmente) restringir el acceso de sus usuarios a redes de internet, incluyendo la restricción de contenidos. Véase la página de la Fundación Electronic Frontier sobre la neutralidad en la red: <https://www.eff.org/issues/net-neutrality> (consultado el 24 de octubre de 2012).

JÉRÉMIE: Hubo adjudicación. Ya sea el Gobierno o las compañías están transformando la arquitectura de una internet universal a una balcanización de pequeñas subredes. Pero lo que estamos debatiendo desde el comienzo son todos asuntos globales, ya sea que hablemos de que el sistema financiero está fuera de cauce, de la corrupción, de geopolítica, de energía o de medio ambiente. Todos estos son problemas globales a los que la humanidad está enfrentándose hoy en día y todavía tenemos una herramienta global en nuestras manos que permite una mejor comunicación, una mejor divulgación del conocimiento, una mejor participación en los procesos políticos y democráticos. Lo que sospecho es que una red global y universal es la única herramienta que tenemos para atender esos problemas globales y ese es el motivo por el cual esta lucha por una internet libre es la lucha central que todos nosotros tenemos el deber de librar.

ANDY: Estoy totalmente de acuerdo en que internet debe ser entendida como una red universal con libre flujo de información; que no solo necesitamos definir eso muy bien, sino que también debemos nombrar a aquellas compañías y a aquellos proveedores de servicios que ofrecen algo que llaman internet y que en realidad es algo totalmente diferente. Pero creo que no hemos respondido la pregunta clave más allá de este asunto del filtro. Quisiera darte un ejemplo de lo que creo que debemos responder. Hace unos años, hace unos diez años, protestamos porque Siemens ofrecía lo que denominaba *software* de filtros inteligentes. Siemens es una de las mayores empresas de telecomunicaciones en Alemania y un proveedor de *software* de inteligencia. Y Siemens les vendió estos sistemas de filtros a compañías para que, por ejemplo, sus empleados no pudiesen consultar el sitio de los sindicatos para informarse sobre sus derechos laborales, etcétera. Pero Siemens también bloqueó el sitio del Chaos Computer Club lo cual nos hizo enfadar. Ellos lo tildaron de «contenido criminal» o algo así, por lo cual iniciamos acciones legales. Pero en una exposición decidimos organizar una enorme protesta y rodear los estands de Siemens e impedir que la gente entrara o saliera. Lo gracioso fue que nosotros la anunciamos en nuestro sitio para atraer a tanta gente como fuera posible, y la gente en el estand de Siemens no tenía la menor idea porque ellos también estaban usando el sistema de filtros lo que les impidió leer las advertencias sobre lo que estaba sucediendo.

JULIAN: El Pentágono creó sistemas de filtros para que cualquier correo electrónico enviado al Pentágono con la palabra WikiLeaks sea filtrado. Y entonces, durante el caso de Bradley Manning, la fiscalía, al intentar llevar adelante el caso, por supuesto que envió correos electrónicos a civiles sobre WikiLeaks, pero nunca recibieron respuesta al-

guna porque contenía esa palabra.[129] El estado de seguridad nacional puede devorarse a sí mismo.

ANDY: Lo que nos lleva nuevamente a la pregunta realmente básica: ¿existe tal cosa como la información con efecto negativo? Y desde el punto de vista de la sociedad, ¿queremos una internet censurada porque es mejor para la sociedad o no? Y aunque hablemos incluso de pornografía infantil, uno podría sostener: «Aguarda un momento, la pornografía infantil pone de relieve un problema, que es el abuso infantil, y para solucionar el problema necesitamos conocer dicho problema».

JACOB: Porque produce evidencias de un delito.

JULIAN: Bueno, no, produce un *lobby*.

ANDY: Esa sería la postura más radical, pero si hablamos de los nazis o lo que fuera tendrás que decir qué es aquello de lo que estamos hablando. Las personas con hijos se preguntarán: «Bueno, ¿no es mejor que la sociedad filtre lo malo para aferrarse a lo bueno? o ¿no está limitando eso nuestra capacidad para dar cuenta de problemas, de atenderlos, resolverlos y controlarlos?».

JÉRÉMIE: Pienso que la censura nunca es la solución. Cuando hablamos de pornografía infantil no deberíamos usar el término pornografía, se trata de representaciones de escenas de abuso infantil. Una de las cosas que hay que hacer es ir a los servidores, inhabilitar los servidores, identificar a las personas que subieron el contenido para poder identificar a quiénes lo produjeron, quiénes abusaron de niños en primer lugar. Y siempre que haya una red, una red comercial, hay que arrestar a las personas involucradas. Y cuando aprobamos leyes —y en Francia tenemos una ley que confiere a una autoridad administrativa dependiente del Ministerio de Interior el poder de decidir qué sitios serán bloqueados— eliminamos el incentivo para que fuerzas de seguridad aprehendan a las personas que cometen delitos diciendo: «Si ya se eliminó el acceso al material», como si tapar los ojos a quien estuviera mirando resolviera el problema. Desde ese punto de vista, pienso que basta con describirlo de esta manera, en la que todos acordamos que deberíamos eliminar dicho material de internet.

JACOB: Perdón, me descompongo. Es tan frustrante escuchar el argumento que estás diciendo. Quiero vomitar por lo que acabas de decir: «Quiero usar mi posición de poder para ejercer mi autoridad sobre otras personas, quiero borrar la historia». Tal vez soy un extremista en este tema —y en muchos temas, estoy seguro— pero me la voy a

---

129 «Blocking WikiLeaks emails trips up Bradley Manning prosecution», *Politico*, 15 de marzo de 2012: <http://www.politico.com/blogs/under-the-radar/2012/03/blocking-wikileaks-emails-trips-up-bradley-manning-117573.html> (consultado el 21 de 2012).

jugar. Este es un claro ejemplo en el que borrar la historia resulta perjudicial. Resulta que con internet nos enteramos de la epidemia de abuso infantil que hay en la sociedad. Con la pornografía infantil —creo que es mejor llamarlo explotación infantil— vimos evidencia de esto. Taparla, borrarla, me parece que sería una aberración porque, de hecho, uno puede aprender mucho sobre la sociedad en su conjunto. Por ejemplo —y obviamente nunca voy a tener una carrera política después de terminar esta oración, pero para dejarlo bien en claro— uno puede enterarse de quién está produciendo el material y de quiénes son las víctimas de dicho proceso. Es imposible ignorar este problema. Pero significa que debes empezar a indagar en las causas que lo hacen posible, que son quienes explotan a los niños. Irónicamente, para esto podría ser útil una tecnología de vigilancia de reconocimiento facial y de análisis de los metadatos en las imágenes. Borrar eso, asegurarnos de que vivimos en un mundo en el que es posible borrar algunas cosas y no otras, crear organismos administrativos de censura y control, es un precedente peligroso, una senda resbalosa que, como hemos visto, lleva directamente al tema de derechos intelectuales y a muchos otros.

Tal vez no debamos tomar el camino más corto solo porque es una causa noble. De hecho tal vez debamos tratar de resolver los crímenes, ayudar a las víctimas, aunque esa ayuda tiene un costo. Tal vez en lugar de ignorar el problema, debamos enfrentarnos al hecho de que la sociedad en su conjunto tiene este gran problema que se manifiesta en internet de un modo particular.

Es como, por ejemplo, cuando Polaroid construyó la cámara Swinger (la cámara instantánea) la gente empezó a tomar fotografías de abusos con esas cámaras. Pero la respuesta no es destruir el medio o controlar dicho medio. Lo es cuando haya evidencias para investigar los crímenes que el medio ha documentado. La respuesta no es debilitar el medio, no se trata de penalizar a la sociedad en su conjunto por esto. Ya que estamos hablando de pornografía infantil. Hablemos de la Policía. La Policía abusa de personas regularmente en muchos países. Posiblemente haya más policías abusivos que abusadores de niños en internet.

JULIAN: Casi sin duda hay más.

JACOB: Sabemos que existe un número «n» de policías en el mundo y sabemos que existe un número «x» de dichos policías que han cometido violaciones a la ética: usualmente hechos violentos. Si observamos en el movimiento Ocupar Wall Street, vemos ejemplos de esto. ¿Acaso debemos censurar internet porque sabemos que algunos policías son malvados? ¿Acaso debemos impedir que la Policía realice un buen trabajo de control?

JULIAN: Bueno, está la cuestión de la revictimización, cuando el niño más adelante, o de adulto, o su círculo social, ven las imágenes del abuso.

JACOB: En la medida en que esos policías estén en línea, me siento revictimizado.

JULIAN: Uno podría decir que ver una imagen de uno siendo golpeado por policías es un ejemplo de revictimización. Diría que es más importante la protección de los documentos en los que consta realmente lo que ocurrió en nuestro mundo; esa revictimización ocurre, pero, sin embargo, crear un régimen censor que sea capaz de eliminar porciones de historia significa que no podemos atender el problema porque no podemos ver cuál es el problema. En los noventa me desempeñé como asesor de la Policía Federal Australiana en asuntos de pedofilia en internet, la Unidad Victoriana de Explotación Infantil. Esos policías no estaban conformes con los sistemas de filtros, porque cuando la gente no puede ver que hay pornografía infantil en internet, desaparece el *lobby* que garantiza que los policías cuenten con los fondos para ponerle fin al abuso infantil.

JÉRÉMIE: El punto en el que estamos de acuerdo —pienso que es el punto más importante— es que al final está la responsabilidad individual de quienes realizan el contenido, material de abuso infantil u otro por el estilo, eso es lo que cuenta y sobre lo que la Policía debería actuar.

JACOB: No estoy de acuerdo. Eso no es lo que dije.

JULIAN: No; Jérémie está hablando de hacer, no de divulgar, hay una diferencia.

JACOB: La producción del contenido no es el problema, en realidad. Una pequeña aclaración: por ejemplo, si has abusado de un niño y Andy tomó una fotografía del hecho como prueba, no creo que Andy deba ser imputado de delito alguno.

JÉRÉMIE: No; debe imputarse a las personas que cometen el abuso. Vamos, es auxiliar e incitar.

ANDY: Pero algunas personas abusan de niños para producir las imágenes, ¿correcto?

JACOB: Por supuesto que sí.

ANDY: También podría haber un aspecto económico en juego aquí.

JACOB: Estoy de acuerdo en un cien por ciento. Solo estoy estableciendo una distinción, si el contenido mismo es un registro histórico que constituye la prueba de un delito, la evidencia de un crimen muy serio por cierto, nunca debemos perder de vista la revictimización,

pero la victimización original existe y ese es en realidad el problema central, haya o no imágenes del hecho.

JÉRÉMIE: Por supuesto. Eso es lo que quiero decir.

JACOB: Que haya imágenes o no es casi irrelevante. Cuando hay imágenes, es muy importante recordar que debes mantener la vista en el propósito, y que el objetivo es en realidad ponerle fin al daño, detener el abuso. Para alcanzar este objetivo es importante asegurarse de que exista evidencia y que existan alicientes para las personas con las herramientas adecuadas para resolver estos crímenes. Eso, me parece, es increíblemente importante, y la gente tiende a perder eso de vista porque el camino fácil es hacer de cuenta que no existe, censurarlo y decir eso le puso fin al abuso. Y no fue así.

ANDY: Y el problema en este momento es que mucha gente favorecerá la solución fácil obviamente porque resulta muy incómodo mirar lo que realmente ocurre en la sociedad. Pienso que tienes chances de manejar un problema político si no tratas de generar una política que lo ignore o lo haga invisible. Esta puede ser la ciberpolítica en cierta forma, pero también es la forma en que la sociedad maneja los problemas. Y tengo mis serias dudas de que haya algo como información que cause daño de manera directa. Tiene que ver con la capacidad de filtrar, por supuesto, y también con que uno no quiere ver todas las imágenes que están disponibles en internet. Hay algunas que realmente desagradan y distraen, pero lo mismo ocurre con las tiendas de video que exhiben películas de ficción y feas. Entonces, la pregunta es ¿acaso tengo la capacidad de manejar lo que estoy viendo, procesando y leyendo? Y ese es el enfoque del filtro. En realidad, Wau Holland, el fundador del Chaos Computer Club, dijo algo gracioso: «Saben, el filtro debería operar en el consumidor final, y en el dispositivo final del consumidor final».[130]

JULIAN: De modo que los filtros deberían ser ejecutados por parte de las personas que reciben la información.

ANDY: Deberían ser ejecutados aquí. ¡Aquí! [*Apuntando a su cabeza*].

JULIAN: En el cerebro.

ANDY: En el dispositivo final del usuario final, es lo que tienes entre los oídos. Allí es donde uno debería filtrar y no debería hacerlo el Gobierno en nombre de las personas. Si las personas no quieren ver cosas, bueno, no tienen que hacerlo, y de cualquier modo hoy en día uno tiene la necesidad de filtrar muchas cosas.

---

130 Para más información sobre Wau Holland véase el sitio de la fundación Wau Holland: <http://www.wauland.de>.

PRIVACIDAD PARA EL DÉBIL, TRANSPARENCIA PARA EL PODEROSO

JULIAN: Andy, recientemente hablé con el presidente de Túnez y le pregunté por lo que estaba por ocurrir con los archivos de inteligencia del Gobierno del dictador Ben Ali —el equivalente de los archivos de la Stasi— y él dijo que si bien estos eran muy interesantes, las agencias de inteligencia eran un problema, son peligrosas y tendría que acabar con ellas una por una. Pero con respecto a esos archivos, él me dijo que lo mejor para la unión de la sociedad tunecina es que permanecieran en secreto para que no hubiera un juego de inculpaciones. Tú eras joven durante la caída de la Stasi en Alemania Oriental, ¿puedes hablar un poco sobre los archivos de la Stasi, y sobre lo que piensas de la apertura de dichos archivos?

ANDY: Alemania probablemente cuente con la agencia de inteligencia mejor documentada del planeta, o una de ellas. Todos los archivos de la Staatssicherheit de Alemania Oriental —todos los manuales, actas, documentos de entrenamientos, estudios internos— son prácticamente públicos. Prácticamente significa que no todos ellos son de fácil acceso, pero muchos de ellos sí lo son, y el Gobierno ha creado una agencia para cuidar de los archivos de modo que los ciudadanos alemanes también tengan el derecho de consultar sus propios archivos de la Stasi.

JULIAN: El Gobierno alemán creó el BstU (Bundesbeauftragtefür die Stasi-Unterlagen), el gran distribuidor de archivos de la Stasi.

ANDY: Sí, y los periodistas pueden realizar las denominadas consultas de investigación, lo que tal vez se asemeja a las solicitudes de libertad de información de los Estados Unidos, que les permitan estudiar distintos temas. También hay muchos libros, cuadernos de estudio de comportamiento estratégico de cómo la Stasi aplicó esto y aquello. En realidad, pienso que esto es algo muy bueno de lo que aprender. Puedo entender que parezca excesivo esperar que los tunecinos publiquen todos los archivos personales que la ex agencia de inteligencia creó porque el presidente —el presidente actual— tendrá que juzgar qué hacer sobre sus propios archivos, los de sus aliados, etcétera. Estas agencias de inteligencia no respetan la privacidad por lo que tendrás archivos personales de tus asuntos sexuales, tus telecomunicaciones, tus trans-

ferencias monetarias, de todo lo que hayas hecho, lo que tal vez no quieras que salga a la luz.

JULIAN: ¿Seguiste la situación de la Amn El Dawla, la seguridad estatal de Egipto? Miles de personas irrumpieron en sus oficinas y saquearon los archivos mientras los agentes de Amn El Dawla trataban de quemarlos, destruirlos y tirarlos a la basura, y mucho material se divulgó y tomó estado público. Se podía comprar un archivo por dos dólares en un mercado local para subirlo a internet. Esto no ha destruido a la sociedad egipcia.

ANDY: No, solo estoy diciendo que en alguna medida me consta que la gente no quiere que se divulguen sus registros personales. Puedo entender eso, porque vivo en un país en el que se mantiene un archivo de inteligencia sobre mí desde hace cuarenta años y queda registro de cada vez que voy al baño.

JULIAN: Pero alguien hace un análisis costo-beneficio, ¿no? Desde mi punto de vista, basta espiar una vez para ser espía.

ANDY: Correcto, pero el argumento de la ética *hacker*, en pocas palabras, es usar la información pública y proteger la información privada, y pienso que si abogamos por la privacidad —y tenemos muy buenos motivos para hacerlo— no deberíamos decir que hay mucho equilibrio. Se puede establecer distinciones. Tampoco es que haya que poner todo a disposición del público.

JACOB: Pero esa confidencialidad tiene un beneficio asimétrico. Vayamos un paso atrás. Tú partes de un punto de vista equivocado, que es esta noción de que la información es privada cuando está restringida, y eso simplemente no es verdad. Por ejemplo en mi país, si se da permiso de acceso a un millón de personas a esos datos privados...

JULIAN: 4,3 millones...

JACOB: ¿Cómo puedes decir que esos datos son privados? El problema es que esos datos no son cien por ciento secretos para todas las personas del planeta.

JULIAN: Son secretos para quien carece del poder y para quien lo ejerce.

ANDY: Sí, tienes razón. Pero si queremos abrir los archivos en su totalidad...

JULIAN: Ha ocurrido en algunos países europeos.

ANDY: No. No conozco un solo país que haya abierto todos sus archivos.

JULIAN: Con un alcance mayor que Alemania, por ejemplo, en Polonia se abrieron los archivos.

ANDY: Eso puede ser. Lo que ha ocurrido en realidad, el lado negativo de este acuerdo que ha hecho Alemania, es que usaron a ex agentes de la Seguridad Estatal de Alemania Oriental para que administrara no solo los archivos de la Stasi sino también parte de los de la denominada «Nueva Alemania», la antigua parte oriental unificada. Hay una historia muy interesante sobre una compañía que ganó una licitación pública para limpiar el edificio donde se conservaban los archivos. Esa compañía ganó la licitación solo porque hicieron la oferta más baja. Después de seis años, la organización que mantenía los registros halló que había contratado a una compañía formada por miembros de la antigua inteligencia oriental para limpiar sus propios archivos.

JÉRÉMIE: Hubo un informe sobre eso en WikiLeaks. Lo leí. Estaba muy bien.[131]

ANDY: WikiLeaks publicó el informe sobre eso exactamente, y estás en lo cierto en cuanto a que una vez que estos archivos se crean y quedan en manos de personas malignas es difícil declarar su confidencialidad.

JULIAN: De todos modos podríamos pasar a un tema más amplio. Internet ha producido una explosión en la cantidad de información disponible para el público; es simplemente extraordinario. La función educativa es extraordinaria. Por otro lado, la gente habla sobre WikiLeaks y dice: «Mira, toda la información confidencial del Gobierno ahora es pública, el Gobierno no puede mantener nada en secreto». Yo digo que esto es una tontería. Yo digo que WikiLeaks es una sombra de una sombra. De hecho, que nosotros hayamos producido más de un millón de palabras en información y las hayamos publicado es una consecuencia de la enorme explosión de material secreto que existe. Y, de hecho, los grupos de poder ahora tienen tal cantidad de material confidencial que hace que la cantidad de material público parezca pequeña, y las operaciones de WikiLeaks no representan más que una fracción de este material secreto. Cuando observas este balance entre, de un lado los poderosos que conocen cada transacción con tarjeta de crédito en el mundo y del otro las personas capaces de buscar los blogs del mundo y los comentarios de la gente, ¿cómo ves este balance?

ANDY: Yo podría sostener que es algo positivo si todos estos archivos tomaran estado público porque las personas entenderían que si usan sus tarjetas de crédito dejan una huella. Algunas personas, si se lo explicas, encuentran esto muy abstracto y difícil de entender. Cuando lean sus propios archivos lo comprenderán.

---

131 «Stasi still in charge of Stasi files», WikiLeaks, 4 de octubre de 2007: <http://www.wikileaks.org/wiki/Stasi_still_in_charge_of_Stasi_files> (consultado el 22 de octubre de 2012).

JULIAN: Si obtuvieras tus registros de Facebook, que tienen 800 MB de información tuya.

ANDY: Sé que tras la caída del bloque oriental, el canciller alemán Helmut Kohl quiso unificar Alemania y los estadounidenses pusieron una condición en el denominado Tratado Dos más Cuatro. Ellos dijeron que querían seguir manteniendo las telecomunicaciones alemanas bajo su órbita de control, y Kohl pensó que no era importante porque no entendía lo que significaba la vigilancia de las telecomunicaciones. Conocí a alguien de su oficina que me dijo que estaban realmente molestos por esto y finalmente consiguieron la transcripción de 8000 páginas de sus llamadas telefónicas que la Stasi había interceptado y las colocaron en su oficina en dos pequeñas latas. Y él dijo: «¿Qué carajo es esto?». A lo que le respondieron: «Son sus llamadas telefónicas de los últimos diez años, incluyendo las de sus novias, su esposa, su secretaria, etcétera». Y así fue cómo le hicieron entender lo que era la interceptación de telecomunicaciones. Y en efecto, estos registros de inteligencia ayudan a que la gente entienda lo que la inteligencia está haciendo. De modo que podríamos favorecer la apertura total y si sometiésemos eso a una votación, no estoy seguro de que me opondría.

JULIAN: No quisiera hablar tanto sobre eso, ya que obviamente hay casos en los que si estás investigando a la mafia por ejemplo, durante el período de investigación debes mantener los archivos en secreto. Hay circunstancias en las que esto podría verse como legítimo. No estoy diciendo que es legítimo como política; estoy diciendo que es políticamente inevitable. Hay demandas tan políticamente convincentes para esto —como, «estos tipos han cometido asesinatos, están tramando otro asesinato»— que sin importar si piensas que la interceptación debería ser posible o no, es algo que va a ocurrir. No se puede ganar esa batalla política. Pero este tipo de vigilancia táctica cuenta con el beneficio de que puede estar regulado en parte y el daño puede circunscribirse a un número mínimo de personas. Cuando la interceptación táctica es usada para la aplicación de la ley (y no para inteligencia) con frecuencia forma parte de la recolección de evidencias. Las evidencias terminan en la Justicia, y por lo tanto terminan tomando estado público. De modo que uno puede tener cierta supervisión, al menos durante una parte del tiempo, de lo que está sucediendo. Y uno puede interrogar a personas en el banquillo sobre cómo se reunió dicha información y por qué deberíamos asumir que fue un procedimiento válido. Uno puede supervisarlo. Pero la regulación de la interceptación estratégica es completamente absurda. Por definición, se trata de interceptar a todos, entonces, ¿qué legislación vamos a aplicar si tu premisa es interceptar a todos?

JÉRÉMIE: El debate sobre la apertura total me hace pensar en el grupo conocido como LulzSec, que publicó 70 millones de archivos de Sony —los datos de todos los usuarios de Sony— y uno podía ver todas las direcciones, las direcciones de correo electrónico y contraseñas. Creo que incluso estaban los detalles de las tarjetas de crédito de 70 millones de usuarios. Como activista por los derechos fundamentales, pensé: «Oh, hay algo mal aquí si revelas los datos personales de las personas para demostrar algo o para divertirte». Me incomodó mucho ver las direcciones de correo electrónico de las personas en el archivo. En un sentido, pensé que esas personas se estaban divirtiendo con la seguridad informática, y lo que estaban dejando en claro es que una compañía tan reconocida y poderosa como Sony no era capaz de mantener los secretos de sus usuarios a resguardo, y hacer que esos 70 millones de usuarios buscaran sus direcciones de correo electrónico o sus nombres en un buscador para encontrar este archivo los llevaría a preguntarse: «Guau, ¿qué hice al darle esta información a Sony? ¿Qué significa darle datos personales a una compañía?»

JACOB: Entonces matan al mensajero.

RATAS EN LA ÓPERA

JULIAN: Ya hemos examinado todas estas situaciones negativas, y ahora quisiera que analicemos un escenario utópico potencial. Tenemos la radicalización de la juventud de internet, y ahora internet está por abarcar a casi toda la juventud. Por otro lado, tenemos algunos intentos desesperados por conseguir el anonimato y la libertad de publicación, libre de censuras —contamos con una amplia gama de interacciones entre el Estado y el sector privado que están luchando contra esto— pero asumamos que tomamos el camino más positivo. ¿A qué se parece dicho escenario?

JACOB: Pienso que necesitamos el derecho a leer y el derecho a expresarnos libremente sin excepción para cada persona, sin excluir a nadie, sin excepciones de ningún tipo, parafraseando a Bill Hicks.[132] Él se refirió a esto con respecto a la educación, la vestimenta y el alimento, pero eso es a lo que se reduce realmente: todo el mundo tiene derecho a leer y a expresarse libremente. Esto incluye el derecho a expresarse de forma anónima, la capacidad de poder pagarles a las personas sin interferencia de terceros, de desplazarse libremente, de corregir la información sobre uno que aparece en los sistemas. Para que haya transparencia y control en todo sistema que se constituya como medio.

ANDY: Yo añadiría la idea que debido al incremento de los sistemas de procesamiento de información y su funcionamiento en red, más la disponibilidad de herramientas como Tor y la codificación, la cantidad de datos que puede eliminarse es bastante baja, lo que significa que los Gobiernos necesitan hacer solo eso y lo saben. Ellos saben que actuar en secreto estos días solo significa actuar en secreto durante un lapso de tiempo, tomará estado público tarde o temprano, y esto es algo positivo. Esto cambia la forma en la que los Gobiernos se manejan. Esto significa que saben que llegado el momento tendrán

132 «Aquí tienes lo que puedes hacer para convertir el mundo, ahora mismo, en un lugar mejor. Tomemos todo el dinero que gastamos en armas y mecanismos de defensa al año, y gastémoslo en cambio en alimento, vestimenta y educación para los pobres del mundo, para lo que alcanzaría reiteradas veces, sin excluir a un solo ser humano, y podríamos explorar el espacio, juntos, tanto el espacio exterior como el interior, en paz». Bill Hicks. Para ver un video con esta cita véase. «Bill Hicks —Positive Drugs Story»: <http://youtu.be/vX1CvW38cHA> (consultado el 24 de octubre de 2012).

que rendir cuentas. Esto también significa que los Gobiernos promueven procesos internos de denuncia, como la Ley Sarbanes-Oxley que les requiere a las compañías que cotizan en las bolsas de Estados Unidos que cuenten con una infraestructura de denuncia, para que las personas que necesitan denunciar conductas criminales o de otro tipo sobre sus superiores tengan una forma de hacerlo sin verse afectadas directamente por aquellos a quienes están denunciando.[133] Entonces, esto es algo positivo y traerá procesos más sustentables a largo plazo.

JÉRÉMIE: Además de lo que acaba de decir Jake, pienso que debemos dejarles en claro a todos que una internet libre, abierta y universal probablemente sea la herramienta más importante que tenemos para solucionar los problemas globales que están en juego, que protegerla es una de las tareas más esenciales que nuestra generación tiene entre manos, y que cuando alguien, en algún lugar —ya sea un Gobierno o una compañía— le impide a alguien acceder a una internet universal, es la red toda la que se ve afectada. Es la humanidad toda la que se ve restringida. A medida que nos damos cuenta de que colectivamente podemos incrementar el costo político de tomar esa decisión, todos los ciudadanos que accedan a una internet libre podrán impedir esa conducta. Estamos empezando a ver que en tanto ciudadanos de la red tenemos el poder en la toma de decisiones políticas y que podemos hacer que nuestros representantes electos y gobiernos rindan cuentas por lo que hacen cuando toman malas decisiones que afectan nuestras libertades fundamentales y que afectan una internet libre y universal.

Pienso que deberíamos poner eso en práctica. Deberíamos seguir compartiendo el conocimiento sobre cómo hacerlo. Deberíamos seguir mejorando nuestras formas de acción, las formas en que intercambiamos tácticas sobre cómo acudir al Parlamento, sobre cómo poner de manifiesto lo que los políticos están haciendo, sobre cómo exponer la influencia de los *lobbies* de la industria en el proceso de toma de decisiones. Deberíamos seguir desarrollando herramientas para hacer que los ciudadanos puedan construir mejores infraestructuras descentralizadas de codificación, para ser propietarios de sus propias infraestructuras de comunicación. Debemos promover estas ideas para que la sociedad en su conjunto pueda construir un mundo mejor y estamos empezando a hacerlo; no debemos bajar los brazos.

---

133 La Ley Sarbanes-Oxley de 2002 es una ley estadounidense aprobada en respuesta a los escándalos corporativos y contables de Enron, Tyco International, Adelphia, Peregrine Systems y WorldCom. La ley apuntaba a eliminar las mismas prácticas que habían dado lugar a estas crisis. La sección 1107 de la ley, llamada en código USC 1513(e), establece que las represalias contra denunciantes ahora constituyen ofensas criminales.

JULIAN: Jack, si tomamos la descripción que personas como Evgeny Morozov hacen de los problemas en internet, esos temas fueron previstos hace tiempo por los criptopunks.[134] No opinábamos que uno debía simplemente quejarse por el estado de control en aumento, sino que podemos y de hecho debemos construir las herramientas de una nueva democracia. En realidad podemos construirlas con nuestras mentes, transmitírselas a otras personas y participar de colectivos de defensa. La tecnología y la ciencia no son neutrales. Existen formas particulares de tecnología que pueden darnos estos derechos y libertades fundamentales a los que muchas personas han aspirado durante tanto tiempo.

JACOB: Absolutamente. Lo más importante que la gente debe captar, me parece —especialmente si hay personas de dieciséis o dieciocho años que desean hacer del mundo un lugar mejor— es que ninguno de los que estamos sentados aquí y nadie en todo el mundo nació con los logros que luego estarán grabados en sus lápidas. Todos construimos alternativas. Todos los aquí presentes construimos alternativas y todo el mundo, especialmente con relación a internet, tiene el poder de hacer eso en el contexto en el que existen. Y no es que tienen el deber de hacerlo, sino que si lo desean, pueden hacerlo. Si hacen eso, causarán impacto sobre muchas personas, especialmente con respecto a internet. Construir dichas alternativas produce una amplificación, un engrandecimiento.

JULIAN: Entonces, si construyes algo puedes dárselo a mil millones de personas para que lo usen.

JACOB: O, si participas de la construcción de una red anónima —como la red Tor por ejemplo— estás ayudando a construir una alternativa de comunicación anónima allí donde previamente no existía.

JÉRÉMIE: Se trata de compartir ese conocimiento libremente y habilitar los canales de comunicación para que ese conocimiento fluya libremente, esto es lo que estás haciendo. Tor es un *software* libre, hoy en día es usado ampliamente porque incorporamos esa noción de libertad en la forma en que construimos alternativas, tecnologías y modelos.

JACOB: Necesitamos *software* libre para un mundo libre, y necesitamos *hardware* libre y abierto.

JULIAN: Pero ¿por libre te refieres a irrestricto, o sea que la gente puede jugar con los subcomponentes?, ¿acaso pueden ver cómo funciona?

---

134 Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (Public Affairs, 2011).

JACOB: Absolutamente. Necesitamos un *software* que sea tan libre como la ley en democracia, que uno puede estudiarla para cambiarla, para poder comprenderla y asegurarse de que haga lo que se desea que haga. *Software* libre, *hardware* libre y abierto.[135]

JULIAN: Ellos tenían esta noción de los criptopunks, «el código es ley».

JÉRÉMIE: Eso es de Larry Lessig.

JULIAN: En internet, lo que puedes hacer está determinado por los programas que existen, qué programas funcionan, y por lo tanto el código es ley.

JACOB: Absolutamente, y lo que eso significa es que uno puede generar alternativas, especialmente en términos de programación pero incluso en términos de impresiones 3D o cosas sociales que existen como los *hacker spaces*.[136] Uno puede ayudar a construir alternativas y la clave es enmarcarlo en un proceso de normalización, proceso en el que la gente se acostumbre mucho a poder construir sus propios objetos tridimensionales, poder modificar su propio *software*, y en el que tome conciencia de que si alguien les impide hacer eso entonces quien sea que esté implementando el bloqueo no está ofreciendo acceso a internet, sino acceso a *filternet* o a *censornet* y, en efecto, están incurriendo en negligencia.

Eso es lo que cada uno de nosotros ha hecho con su propia vida y la gente debería saber que tiene la capacidad de hacerlo para las generaciones futuras, y para la generación actual. Por eso estoy aquí —porque si no apoyo a Julian ahora, en las situaciones que está atravesando, ¿qué tipo de mundo estoy construyendo? ¿Qué mensaje transmito cuando dejo que un grupo de policías me hostigue? No hay forma, nunca. Debemos progresar y cambiar eso. Como dijo Gandhi: «Debes ser el cambio que quieres ver en el mundo», pero también debes encarnar ser el problema.[137] Esa es una cita de *A Softer World*, no

---

135 Sobre *software* libre véase, «The Free Software Definition», del sitio del Sistema Operativo GNU: <https://www.gnu.org/philosophy/free-sw.html>. *Hardware* libre significa que no está obstruido por patentes, que está construido en base a estándares abiertos, donde no hay leyes contra el rediseño o la manipulación (sin leyes anti-elusión), y donde los principios de diseño, instrucciones y planos están abiertamente disponibles para que cualquiera que acceda a estos últimos y a los recursos necesarios pueda construir una réplica. Para más información sobre hardware libre, véase «Exceptionally Hard and Soft Meeting: exploring the frontiers of open source and DIY», EHSM: <http://ehsm.eu>. Véase también, «Open-source *hardware*» en Wikipedia: <https://en.wikipedia.org/wiki/Open-source_hardware> (todos los *links* fueron consultados el 24 de octubre de 2012).

136 Para más información sobre impresiones 3D que usan *hardware* libre y abierto véase un video introductorio a la impresora RepRap 3D: <http://vimeo.com/5202148> (consultado el 24 de octubre de 2012).

137 «Encarnar el problema que quieres ver en el mundo», está tomado de *A Softer World*, un *webcomic* fotográfico: <http://www.asofterworld.com/index.php?id=189> (consultado el 24 de octubre de 2012).

es igual a la cita de Gandhi, pero creo que la gente necesita saber que no puede quedarse de brazos cruzados, necesita entrar en acción y espero que así sea.[138]

ANDY: Creo que hay probabilidades de que la gente avance respecto de donde estamos, y las alternativas surgen de la gente que no está conforme con la situación en la que se encuentra o con las opciones que tiene.

JULIAN: ¿Puedes hablar un poco sobre el Chaos Computer Club en este contexto?

ANDY: Siempre, CCC... fnord.[139]

JULIAN: Es algo único en el mundo en realidad.

ANDY: El CCC es una organización galáctica de *hackers* que promueve la libertad de información, la transparencia tecnológica y cuida la relación entre el desarrollo humano y el tecnológico, es decir la sociedad y el desarrollo interactuando entre sí.

JULIAN: Esto se ha tornado una cuestión realmente política.

ANDY: El CCC se ha convertido en un foro de la escena *hacker* con unos cuantos miles de miembros radicados en alguna medida en Alemania —pero no nos consideramos como habitantes de Alemania, consideramos que vivimos en internet, que es tal vez una gran parte de nuestra autopercepción que además atrae. Estamos muy bien interconectados con otros grupos de *hackers* de Francia, Estados Unidos y otros lugares.

JULIAN: ¿Y por qué crees que surgió en Alemania? El corazón está en Alemania, pero se ha expandido al resto del mundo.

ANDY: Alemania siempre trata de estructurar todo.

JÉRÉMIE: La ingeniería alemana es mejor.

JULIAN: Pienso que no es solo eso. Es que esto es Berlín y la caída del Este.

ANDY: Tiene que ver con diferentes cosas. Alemania ha hecho lo peor que un país le puede hacer a otro, entonces tal vez es algo inmune a hacer lo mismo de nuevo, como empezar una guerra contra otros países. Lo hemos hecho todo, lo hemos atravesado, hemos sido casti-

---

138 Para seguir cualquiera de los temas planteados en el debate, Jacob recomienda los siguientes recursos bibliográficos: *The Anonymity Bibliography, Selected Papers in Anonymity*, compilado por Roger Dingledine y Nick Mathewson: <http://freehaven.net/anonbib>.
The Censorship Bibliography, Selected Papers in Censorship, seleccionado por Philipp Winter: <www.cs.kau.se/philwint/censorbib> (ambos *links* fueron consultados el 24 de octubre de 2012).

139 Nota dejada intencionalmente en blanco.

gados tan duramente y tuvimos que aprender la lección, y en realidad este pensamiento descentralizado y esta conducta antifascista, como evitar el Estado totalitario, todavía se enseñan en las escuelas alemanas porque nosotros pasamos por eso en su peor expresión. Entonces pienso que eso es parte de entender el CCC, que es una suerte de fenómeno alemán. Wau Holland, el creador que fundó el CCC, también tuvo una postura fuertemente política respecto a esto. Yo vi a su padre en el entierro de Wau, él murió delante de su padre, y su padre no decía cosas agradables. Decía: «... y que nunca vuelva a haber actividad totalitaria y no pacífica alguna en suelo alemán». Ese fue el comentario de su padre al enterrar a su hijo, y para mí eso explicó mucho de por qué Wau estaba tan abocado a influir y a cuidar de las personas, comportándose pacíficamente con el prójimo, divulgando ideas sin limitarlas, y sin comportarse agresivamente pero de forma cooperativa.

Y la idea de generar cosas de forma cooperativa —como los movimientos de *software* de fuente abierta— efectivamente ha estado contagiando y sumándose a ideas de los criptopunks estadounidenses y Julian Assange/WikiLeaks, etcétera. Es un fenómeno global en curso, que tiene actitudes culturales muy diferentes y descentralizadas de *hackers* suizos, alemanes, italianos, y eso es algo positivo. Los *hackers* italianos se comportan totalmente diferente a los *hackers* alemanes —donde sea que estén—, necesitan preparar buena comida; los *hackers* alemanes necesitan tener todo bien estructurado. No estoy diciendo que unos son mejores que los otros, solo estoy diciendo que cada una de estas culturas descentralizadas tiene costados muy hermosos. En la conferencia italiana de *hackers* uno puede ir a la cocina y verá un lugar hermoso; en el encuentro alemán de *hackers* uno verá una internet hermosa, pero mejor no entres a la cocina. De cualquier modo, el centro de la cuestión es que estamos creando. Y pienso que nos encontramos en alguna suerte de conciencia común que está totalmente alejada de nuestra identidad nacional —de ser alemanes, italianos, estadounidenses o lo que fuera— solo vemos que queremos resolver problemas, queremos trabajar juntos. Vemos la censura en internet, esta lucha de los Gobiernos contra las nuevas tecnologías, como una forma de situación evolutiva que debemos superar.

Estamos en camino a identificar soluciones y no solo problemas, y eso es algo positivo. Probablemente tengamos que luchar contra muchas estupideces durante los próximos no sé cuántos años, pero finalmente vemos una generación de políticos que no ven a internet como un enemigo sino que entienden que es parte de la solución, y no parte del problema. Aún tenemos un mundo construido sobre armas, sobre el poder de la confidencialidad, sobre todo un esquema económico, pero eso está cambiando y creo que somos muy importantes en el actual desarrollo de políticas. Podemos hablar de los problemas de manera

polémica —y eso es algo que el CCC ha logrado hacer durante mucho tiempo, en realidad. No somos un grupo homogéneo, tenemos opiniones muy diferentes. Encuentro positivo que podamos sentarnos aquí todos juntos y no vengamos con las mejores respuestas de inmediato, solo planteamos interrogantes, y contrastamos nuestras diferentes ideas y vemos cuál es el balance. Ese es el proceso que debe continuar, y ese es el motivo por el cual necesitamos una internet libre.

JULIAN: Pregunté cómo sería la trayectoria más positiva para el futuro. Autoconocimiento, diversidad y redes de autodeterminación. Una población global altamente educada —no digo educación formal, sino altamente educada en su comprensión de cómo funciona la civilización humana a nivel político, industrial, científico y psicológico— como resultado del libre intercambio de comunicaciones, estimulando asimismo nuevas culturas y la diversificación máxima del pensamiento individual, una mayor auto-determinación regional y la autodeterminación de grupos de interés capaces de interactuar e intercambiar valor rápidamente a través de fronteras geográficas. Y tal vez eso quedó expresado en la Primavera Árabe y en el activismo pan-árabe que se vio potenciado por internet. Cuando trabajamos junto a Nawaat.org, quienes crearon Tunileaks, sorteando la censura del régimen para publicar los cables del Departamento de Estado en los albores de la revolución tunecina, vimos de primera mano el formidable poder de la red para llevar información hacia donde es necesaria, y fue tremendamente gratificante estar en la posición, debido a nuestros esfuerzos, de contribuir a lo que estaba empezando a ocurrir allí.[140] No veo que esa lucha por la autodeterminación sea muy diferente a la nuestra.

Esta trayectoria positiva implicaría el autoconocimiento de la civilización humana ya que el pasado no puede ser destruido. Significaría que en la práctica no podrían surgir Estados neototalitarios debido al libre movimiento de información, a la capacidad de las personas de comunicarse entre sí de forma privada, a conspirar contra tales tendencias y a la posibilidad de transferir microcapitales libremente hacia lugares amigables.

Con esos fundamentos, uno puede construir una amplia variedad de sistemas políticos. La utopía sería una situación distópica si existiese solo una utopía. Creo que los ideales utópicos significan la diver-

---

140 Nawaat.org es un colectivo de blogueros independientes creado en Túnez en 2004: <http://nawaat.org/portail>.
Tunileaks fue lanzado por Nawaat en noviembre de 2010, con la publicación de cables de WikiLeaks vinculados a Túnez: <https://tunileaks.appspot.com>.
Para más información sobre Tunileaks y las iniciativas de censura del Gobierno de Ben-Ali véase, «Tunisia: Censorship Continues as Wikileaks Cables Make the Rounds», Global Voices Advocacy, 7 de diciembre de 2010: <http://advocacy.globalvoicesonline.org/2010/12/07/tunisia-censorship-continues-as-wikileaks-cables-make-the-rounds> (todos los *links* fueron consultados el 24 de octubre de 2012).

sidad de sistemas y modelos de interacción. Si observamos el agitado desarrollo de nuevos productos culturales, la evolución lingüística y las subculturas cuyos mecanismos de interacción se vieron potenciados por internet, entonces sí puedo ver que eso marque un posible rumbo positivo.

Pero pienso en todas las probabilidades de una tendencia hacia la homogeneización, la universalidad, hacia una civilización humana devenida en un mercado, lo que significa factores mercantiles normales como un líder del mercado, un segundo, un tercero, y luego los rezagados que no hacen diferencia alguna. Pienso que tal vez implique una masiva homogenización lingüística, una enorme homogenización cultural, una enorme estandarización para poder hacer que estos rápidos intercambios sean eficientes. Entonces pienso que el escenario pesimista también es bastante probable, y que el estado de vigilancia transnacional y las interminables guerras con aviones no tripulados están casi a la vuelta de la esquina.

Esto me hace acordar a una vez que entré sin boleto a la Ópera de Sydney a ver *Fausto*. La Ópera de Sydney es muy hermosa de noche, con sus imponentes interiores y luces brillando sobre el agua. Luego salí y escuché a tres mujeres conversando, apoyadas sobre la baranda que da a la bahía a oscuras. La mayor de las tres, quien hablaba sobre sus problemas en el trabajo, resultó ser agente de la CIA y les contaba a las otras dos sobre cómo se había quejado ante el Comité Selecto de Inteligencia del Senado. Esto lo decía en voz baja a su sobrina y otra mujer. Y yo pensé, «Entonces, es cierto. ¡Los agentes de la CIA sí vienen a la Ópera de Sydney!». Y luego miré hacia adentro de la Ópera a través de los enormes paneles de vidrio del frente, y allí, en todo este refinamiento palaciego vi una rata, que se movía de un lado al otro a toda velocidad, comiéndose los alimentos servidos sobre finos manteles, yendo de arriba para abajo, saltando desde una mesa hasta el mostrador con todos los boletos, pasándola realmente bien. Y, en realidad, pienso que ese es el escenario más probable para el futuro: una estructura totalitaria, transnacional y posmoderna; extremadamente restringida y homogeneizada con una increíble complejidad, ridiculeces y degradaciones, y dentro de esa increíble complejidad, un espacio al que solo las ratas inteligentes pueden acceder.

Esta es una mirada desde un ángulo positivo de la trayectoria negativa, siendo esta el estado de vigilancia transnacional, infestado de aviones no tripulados, el neofeudalismo de la elite internacional en red —no en un sentido clásico, sino en una compleja interacción de múltiples participantes surgidos como resultado del ascenso y posterior fusión de varias elites de diferentes países—. Todas las comunicaciones serán vigiladas, rastreadas y registradas de forma permanente; cada individuo en todas sus interacciones será identificado para este

nuevo *establishment* como ese individuo, desde su nacimiento hasta la muerte. Esto constituye un cambio importante respecto de hace diez años y prácticamente ya están dadas las condiciones para que ocurra. Pienso que eso solo puede producir un clima muy asfixiante. Si toda la información fuese pública, entonces se podría equilibrar la dinámica de poder y nosotros, en tanto civilización global, podríamos dar forma a nuestro propio destino. Pero sin un cambio dramático no sucederá. El control masivo recae desproporcionadamente sobre la gran mayoría de nosotros, transfiriéndoles poder a personas del sistema quienes, me parece, tampoco disfrutarían de ese mundo feliz. Este sistema coincidirá con la carrera armamentista no tripulada que eliminará las fronteras bien definidas como las conocemos, ya que dichas fronteras son resultado de la impugnación de líneas físicas, llevando a un estado de guerra perpetuo en el que las redes de influencia ganadoras empiecen a sonsacarle concesiones al mundo. Y cuando esto ocurra, la gente quedará enterrada bajo la imposible complejidad de la burocracia.

¿Cómo puede una persona normal ser libre en ese sistema? Simplemente no puede, es imposible. Nadie puede ser completamente libre sea el sistema que sea, pero las libertades que nos han hecho evolucionar biológicamente, las libertades a las que nos hemos acostumbrado culturalmente, quedarán casi totalmente eliminadas. Entonces pienso que las únicas personas que podrán conservar la libertad que teníamos, digamos hace veinte años —porque el estado de control ya ha eliminado gran parte de eso, solo que aún no nos dimos cuenta— son aquellas personas altamente educadas con un profundo conocimiento interno del sistema. Entonces solo una elite tecnológica rebelde será libre, como esas ingeniosas ratas que corretean por la Ópera.

Impreso y Encuadernado en
mastergraf srl
Gral. Pagola 1823 - CP 11800 - Tel.: 2203 4760*
Montevideo - Uruguay
E-mail: mastergraf@mastergraf.com.uy

Depósito Legal 361.748 - Comisión del Papel
Edición Amparada al Decreto 218/96

CRIPTOPUNKS
LA LIBERTAD Y EL FUTURO DE INTERNET

La infraestructura de internet dirige gran parte del tráfico desde y hacia América Latina a través de cables de fibra óptica que físicamente atraviesan las fronteras de Estados Unidos. El Gobierno de Estados Unidos no ha mostrado escrúpulos en transgredir su propia ley al interceptar estas líneas para espiar a sus propios ciudadanos. Y no existen las leyes que impidan espiar a ciudadanos extranjeros. Cada día, cientos de millones de mensajes de toda América Latina son devorados por las agencias de espionaje de Estados Unidos y almacenados para siempre en depósitos del tamaño de ciudades.

El mundo debe ser consciente del riesgo que la vigilancia —para controlar y reprimir— significa para América Latina y para el antiguo Tercer Mundo. No solo es un problema para la democracia o para la gobernabilidad, sino que es un problema geopolítico. El control de toda una población por parte de poderes internacionales naturalmente amenaza la soberanía.
Internet, nuestro mayor instrumento de emancipación, ha sido transformado en la más peligrosa herramienta del totalitarismo que hayamos visto.

Julian Assange, *Prefacio para América Latina*

JULIAN ASSANGE es periodista, editor en jefe de WikiLeaks. Su trabajo se orienta por el lema criptopunk: «privacidad para los pobres, transparencia para los poderosos». En 2010, WikiLeaks reveló el sistemático abuso del secreto por los militares y el gobierno estadounidense. Estas publicaciones —*Asesinato colateral*, los *Diarios de la guerra de Afganistán* y *Cablegate*— tuvieron como respuesta una campaña para destruir WikiLeaks. En Estados Unidos hay un proceso en curso donde penden acusaciones de espionaje y terrorismo. Assange se encuentra desde junio de 2012 asilado en la embajada de Ecuador en Londres esperando un salvoconducto que le permita evitar ser extraditado a los Estados Unidos. De adolescente, fue uno de los primeros investigadores en materia de seguridad informática y de redes; es autor de numerosos proyectos de *software* como el sistema Rubberhose de cifrado y el código original de WikiLeaks. Es coautor, junto a Sulette Dreyfus, de *Underground*, la historia del movimiento *hacker* internacional.

TRILCE
LOM EDICIONES
MAREA EDITORIAL
9 789974 32617