Serie Bianca Feltrinelli

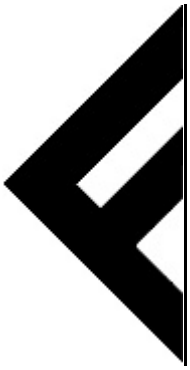
JULIAN ASSANGE
INTERNET È IL NEMICO

CONVERSAZIONE CON JACOB APPELBAUM,
ANDY MÜLLER-MAGUHN E JÉRÉMIE ZIMMERMANN

Serie Bianca Feltrinelli

JULIAN ASSANGE
INTERNET È IL NEMICO

CONVERSAZIONE CON JACOB APPELBAUM,
ANDY MÜLLER-MAGUHN E JÉRÉMIE ZIMMERMANN



Feltrinelli

Julian Assange

INTERNET È IL NEMICO

Conversazione con Jacob Appelbaum, Andy Müller-Maguhn e Jérémie Zimmermann

Traduzione di Giancarlo Carlotti

Prima edizione nella collana “Serie Bianca” giugno 2013

ISBN edizione cartacea: 9788807172588

Introduzione

Una chiamata alle armi crittografica

Questo libro non è un manifesto. Non c'è tempo per cose del genere. Questo libro è un segnale d'allarme.

Il mondo non sta scivolando, sta letteralmente galoppando verso una nuova distopia transnazionale. Questa evoluzione è passata quasi inosservata al di fuori delle cerchie deputate alla sicurezza nazionale. È stata occultata dal segreto, dalla complessità e dalle dimensioni. Internet, il nostro massimo strumento di emancipazione, è stata trasformata nel più pericoloso contributo al totalitarismo che si sia mai visto. Internet è una minaccia per la civiltà.

Queste trasformazioni sono avvenute in silenzio perché chi sa che cosa sta succedendo lavora nel settore della sorveglianza globale e non ha il minimo interesse a parlarne. Se abbandonata alla propria inerzia, la civiltà globale diventerà nel giro di pochi anni una postmoderna distopia della sorveglianza, dalla quale nessuno potrà fuggire, a parte gli individui più abili. Anzi, forse ci siamo già.

Tanti autori si sono interrogati su quello che significa Internet per la civiltà globale, ma si sbagliano. Si sbagliano perché non hanno la giusta prospettiva frutto dell'esperienza diretta. Si sbagliano perché non hanno mai conosciuto il nemico.

Nessuna descrizione del mondo sopravvive al primo contatto con il nemico.

Noi abbiamo conosciuto il nemico.

Negli ultimi sei anni WikiLeaks ha dovuto combattere con quasi tutte le potenze. Noi conosciamo il nuovo stato della

sorveglianza dal di dentro perché abbiamo svelato i suoi segreti. Lo conosciamo dal punto di vista del combattente perché siamo stati costretti a proteggere la nostra gente, le nostre finanze e le nostre fonti. Lo conosciamo dal punto di vista globale perché abbiamo persone, strutture e informazioni in quasi tutti i paesi. Lo conosciamo dal punto di vista cronologico perché combattiamo questo fenomeno da anni e l'abbiamo visto raddoppiare e allargarsi più e più volte. È un parassita invasivo che ingrassa sulle società che si fondono con Internet. Sta dilagando nel pianeta, infettando tutti gli stati e tutti i popoli.

Che fare?

C'erano una volta, in un posto che non era lì o qui, i costruttori e cittadini della giovane Internet, noi, e discutevamo sul futuro del nostro nuovo mondo.

Capivamo che i rapporti fra tutte le persone sarebbero stati mediati dal nostro nuovo mondo, e che sarebbe cambiata anche la natura degli stati, i quali sono delineati dal modo in cui la gente scambia informazioni, valori economici e forza.

Capivamo che l'intreccio fra le strutture statali esistenti e Internet favoriva un'apertura al cambiamento nella natura degli stati.

Per prima cosa, ricordate che gli stati sono sistemi nelle cui vene scorre la forza coercitiva. Le fazioni all'interno di uno stato possono combattersi per il consenso, portando a fenomeni democratici di superficie, ma le basi degli stati sono l'utilizzo sistematico della violenza e la sua eventuale sospensione. La proprietà terriera e fondiaria, le rendite, i dividendi, le tasse, le sanzioni dei tribunali, la censura, i diritti d'autore e i marchi commerciali vengono fatti tutti rispettare con la minaccia dell'utilizzo della violenza statuale.

Di solito non ci accorgiamo nemmeno di quanto siamo vicini alla violenza perché tutti facciamo concessioni per evitarla. Come marinai che annusano il vento, è raro che ci soffermiamo a pensare fino a che punto il nostro mondo di superficie è sorretto dalle tenebre.

Nel nuovo spazio di Internet quale sarà il mediatore della forza coercitiva?

Ha senso anche solo porre questa domanda? In questo spazio ultraterreno, in questo regno apparentemente platonico di idee e flusso di informazioni, potrebbe esistere il concetto di forza coercitiva? Una forza capace di modificare i dati storici, intercettare i telefoni, separare le persone, trasformare la complessità in un cumulo di macerie ed erigere muri come un esercito d'occupazione?

La natura platonica di Internet, fatta di idee e flusso di informazioni, è svilita dalle sue origini fisiche. Le sue basi sono i cavi di fibre ottiche che si snodano sul fondo degli oceani, i satelliti che ruotano sulla nostra testa, i server ospitati nei palazzi di città che vanno da New York a Nairobi. Come il soldato che ammazzò Archimede con una banale spada, altrettanto oggi una falange armata potrebbe assumere il controllo dell'evoluzione di punta della civiltà occidentale, del nostro regno platonico.

Il nuovo mondo di Internet, astratto dal vecchio mondo dei bruti atomi, agognava l'indipendenza. Però poi gli stati e i loro amici si sono attivati per mettere sotto sorveglianza il nostro nuovo mondo, controllando le sue basi fisiche. Lo stato, come un esercito schierato attorno a un pozzo di petrolio o un doganiere che pretende mazzette al confine, avrebbe presto imparato ad approfittare del proprio controllo dello spazio fisico per assumere la gestione del nostro regno platonico. Avrebbe impedito l'indipendenza che sognavamo e poi, appostato sulle fibre ottiche e attorno alle stazioni satellitari al suolo, sarebbe passato a intercettare in blocco il flusso di informazioni del nostro nuovo mondo, la sua vera essenza, proprio mentre ogni rapporto umano, economico e politico lo adottava. Lo stato sarebbe filtrato nelle vene e arterie delle nostre nuove società, divorando qualsiasi relazione espressa o comunicata, ogni pagina web letta, ogni messaggio inviato e ogni pensiero googlato, per poi immagazzinare questo sapere, miliardi di intercettazioni al giorno, un potere inaudito, dentro immensi depositi top secret, per sempre. Potrebbe scavare all'infinito in questo tesoro, la produzione intellettuale privata collettiva dell'umanità, utilizzando sempre più sofisticati algoritmi di

ricerca e rilevamento pattern, arricchendo il tesoro e massimizzando lo squilibrio di potere tra gli intercettatori e il mondo degli intercettati. Dopodiché lo stato rimanderebbe quanto ha appreso verso il mondo fisico per scatenare guerre, indirizzare droni, manipolare commissioni Onu e accordi commerciali e fare regalie alla sua immensa rete interconnessa di industrie, insider e compari.

Però abbiamo scoperto una cosetta. L'unica nostra speranza contro il dominio totale. Una speranza che con coraggio, intuito e solidarietà potremmo sfruttare per resistere. Una strana proprietà dell'universo fisico in cui viviamo.

L'universo crede nella cifratura.

È più facile cifrare le informazioni che decifrarle.

Abbiamo visto che potremmo usare questa strana proprietà per creare le leggi di un nuovo mondo. Per astrarre il nostro nuovo regno platonico dalla sua base fatta di satelliti, cavi sottomarini e relativi controllori. Per consolidare il nostro spazio sotto un velo crittografico. Per creare nuovi territori proibiti a coloro che controllano la realtà fisica perché seguirci sin lì richiederebbe risorse infinite.

E in questo modo dichiarare la nostra indipendenza.

Gli scienziati del Manhattan Project scoprirono che l'universo consentiva la costruzione di un ordigno nucleare. Non era una conclusione scontata. Forse le armi nucleari non potevano esistere entro le leggi della fisica. Invece l'universo crede nelle bombe atomiche e nei reattori nucleari. Sono un fenomeno che l'universo benedice, come il sale, il mare o le stelle.

Allo stesso modo l'universo, il nostro universo fisico, possiede la proprietà di rendere possibile a un individuo o gruppo di individui codificare qualcosa in modo affidabile, automatico, persino inconsapevole, così che tutte le risorse e tutta la volontà politica della più forte superpotenza sulla terra non siano in grado di decodificarla. E i sentieri della cifratura tra persone possono incrociarsi in modo da creare zone libere dalla forza coercitiva dello stato là fuori. Libere dall'intercettazione di massa. Libere dal controllo statale.

In questo modo la gente può contrapporre la sua volontà a

quella di una superpotenza totalmente mobilitata contro di lei, e vincere. La cifratura è un'incarnazione delle leggi della fisica e non dà ascolto alle vuote minacce degli stati, persino a quelle delle distopie transnazionali della sorveglianza.

Non è scontato che il mondo debba funzionare in questo modo. Però in qualche maniera l'universo sorride alla cifratura.

La crittografia è l'estrema forma di azione diretta non violenta.

Anche se gli stati provvisti di testate nucleari possono esercitare una violenza illimitata su addirittura milioni di individui, la crittografia forte porta con sé che uno stato, persino se esercita una violenza illimitata, non può violare l'intenzione del singolo di tenergli segreto qualcosa.

La crittografia forte è in grado di resistere al ricorso illimitato alla violenza. Nessuna dose di coercizione sarà mai capace di risolvere un problema matematico.

Potremmo prendere questa bizzarria del mondo e farla diventare un basilare architrave dell'emancipazione per ottenere l'indipendenza dell'umanità nel regno platonico di Internet? E questa libertà, ora che le società si fondono con Internet, potrebbe riflettersi nella realtà fisica in modo da ridefinire lo stato?

Gli stati, non dimentichiamolo, sono i sistemi che determinano dove e come la forza coercitiva si applica in modo consistente.

Il problema di quanta coercizione può filtrare nel regno platonico di Internet dal mondo fisico trova una risposta nella crittografia e negli ideali dei cypherpunk.

Ora che gli stati si fondono con Internet e il futuro della nostra civiltà diventa il futuro di Internet, noi dobbiamo reimpostare i rapporti di forza.

Altrimenti l'universalità di Internet trasformerà l'umanità globale in un unico gigantesco reticolo di sorveglianza di massa e controllo di massa.

Dobbiamo lanciare un allarme. Questo libro è il grido della sentinella.

Il 20 marzo 2012, mentre ero agli arresti domiciliari nel

Regno Unito in attesa di essere estradato, ho incontrato tre amici e colleghi sentinelle, ritenendo che forse le nostre voci in coro potevano svegliare la città. Dobbiamo comunicare quanto abbiamo imparato finché c'è ancora la possibilità che tu, lettore, capisca e reagisca a quanto sta accadendo.

È venuto il momento di imbracciare le armi del nostro nuovo mondo, di combattere per noi stessi e per coloro che amiamo.

Il compito che ci prefiggiamo è quello di garantire l'autodeterminazione dove possiamo, respingere la distopia ventura dove ciò sarà impossibile e, se proprio va male tutto il resto, accelerare la sua autodistruzione.

Julian Assange
Londra, ottobre 2012

Nota del curatore

Per rendere il libro più accessibile al lettore comune, ciascuno dei partecipanti alla discussione ha avuto la possibilità di ampliare sostanzialmente le sue affermazioni, chiarirle e aggiungere note. L'ordine del manoscritto editato coincide nel complesso con la dinamica della discussione originaria.

Che cos'è un cypherpunk?

I cypherpunk sostengono l'uso della crittografia e di tecniche affini per arrivare a un cambiamento sociale e politico.[1] Il movimento, fondato all'inizio degli anni novanta, è stato in prima linea nelle "crittoguerre" dello stesso decennio e dopo la primavera Internet del 2011. Il sostantivo *cypherpunk*, che deriva dalla fusione di *cypher* (nel senso di cifrario) e *punk*, è entrato nell'Oxford English Dictionary nel 2006.[2]

Julian Assange è il caporedattore e la mente visionaria che sta dietro a WikiLeaks.[1] Dopo essere stato uno dei primi collaboratori della mailing list Cypherpunk, Julian è oggi uno dei più importanti esponenti al mondo della filosofia cypherpunk. Il suo lavoro con WikiLeaks ha dato una valenza politica al tradizionale binomio cypherpunk: “privacy per i deboli, trasparenza per i potenti”. Anche se il suo contributo più visibile risiede nel robusto esercizio della libertà di espressione per costringere le istituzioni più potenti alla trasparenza e a rendere conto del proprio operato, Julian è pure un accanito critico dello stato e dell’intromissione delle aziende nella privacy dei singoli. Julian è autore di numerosi progetti informatici in linea con la filosofia cypherpunk, come strobe.c, il primo port scanner TCP/IP, il sistema di crittografia negabile Rubberhose e il codice originale di WikiLeaks.[2] Durante l’adolescenza Julian è stato uno dei primi analisti della sicurezza dei computer e delle reti quando ancora i codici non definivano reato certi tipi di hacking. Diventato poi attivista e provider Internet in Australia negli anni novanta, Julian ha scritto in collaborazione con Suelette Dreyfus una storia del movimento hacker internazionale, *Underground*, su cui è liberamente basato il film *Underground: The Julian Assange Story*.[3]

Jacob Appelbaum è uno dei fondatori di Noisebridge di San Francisco, membro del berlinese Chaos Computer Club e sviluppatore.[4] Jacob è fautore e ricercatore del Tor Project, un sistema di anonimato online per tutti, per difendersi dalla sorveglianza e aggirare la censura in Internet.[5] Il suo principale impegno nell’ultimo decennio è stato l’appoggio ai

militanti ambientalisti e per i diritti umani. A questo fine ha pubblicato originali ricerche su vari argomenti, dalla legislazione informatica alla marijuana a scopo terapeutico. Jacob è convinto che tutti abbiano il diritto di leggere senza limitazioni e il diritto di parlare liberamente senza eccezioni. Nel 2010, quando Julian Assange non ha potuto parlare a New York, è stato Jacob a intervenire al posto suo. Da quel giorno lui, i suoi amici e i suoi familiari sono perseguitati dal governo degli Stati Uniti: fermati per essere interrogati negli aeroporti, sottoposti a perquisizioni invasive mentre vengono minacciati di automatico rischio di stupro in galera da parte dei secondini, privati dei loro macchinari con la confisca, mentre i loro servizi di rete subiscono ordinanze segrete. Jacob non si fa intimidire da queste misure, continua a combattere in varie cause giudiziarie e rimane un loquace paladino della libertà di espressione oltre a essere un chiassoso sostenitore di WikiLeaks.

Andy Müller-Maguhn è da anni membro del Chaos Computer Club in Germania, di cui è stato consigliere e portavoce.[6] È stato uno dei fondatori di EDRI, European Digital Rights, una ong per la tutela dei diritti umani nell'era digitale.[7] Dal 2000 al 2003 è stato eletto dagli utenti europei di Internet direttore europeo dell'ICANN, Internet Corporation for Assigned Names and Numbers, l'ente responsabile per le politiche mondiali sulla gestione dei "nomi e numeri" in Internet.[8] È specialista di telecomunicazioni e di altre forme di sorveglianza e lavora in una struttura giornalistica che analizza il settore della sorveglianza con il suo progetto wiki, buggedplanet.info.[9] Andy, che sta lavorando sulle comunicazioni cifrate, ha creato con altri un'azienda chiamata Cryptophone che vende ai privati strumenti sicuri di comunicazione vocale e fornisce consulenza strategica nel contesto dell'architettura della rete.[10]

Jérémie Zimmermann è cofondatore e portavoce di La Quadrature du Net, un gruppo di tutela legale dei cittadini, la più importante organizzazione europea per la difesa del

diritto all’anonimato online e per favorire la consapevolezza degli attacchi tesi a controllare la libertà online.[11] Jérémie si batte per costruire strumenti che la gente possa utilizzare per prendere parte al dibattito pubblico e per tentare di cambiare le cose. È principalmente impegnato nelle battaglie sul copyright, nel dibattito attorno alla neutralità della rete e in altri problemi della regolamentazione cruciali per il futuro di un’Internet libera. Di recente il suo gruppo La Quadrature du Net ha ottenuto un successo storico nell’arena politica europea conducendo un’efficace campagna pubblica per sconfiggere l’ACTA (Accordo anticontraffazione e sui traffici) al parlamento europeo. Poco dopo avere partecipato alla discussione che costituisce la base di questo libro, Jérémie è stato fermato da due agenti dell’FBI mentre usciva dagli Stati Uniti ed è stato interrogato a proposito di WikiLeaks.

Nota sui vari tentativi di molestare WikiLeaks e le persone a essa associate

In parecchi punti della discussione che segue si fa riferimento ai fatti recenti della storia di WikiLeaks e al suo impegno nella diffusione di notizie. Dato che potrebbero risultare oscuri ai lettori che non conoscono bene la vicenda di WikiLeaks, li riassumiamo qui all'inizio.

La missione di WikiLeaks è quella di ricevere informazioni dai "whistleblowers", coloro che scoprono gli altarini e fanno le soffiate, renderle pubbliche e poi difendersi dagli inevitabili attacchi politici e giudiziari. È ormai procedura usuale che gli stati e le organizzazioni più potenti tentino di mettere a tacere le rivelazioni di WikiLeaks, e trattandosi dell'editore di ultima istanza è una delle avversità per reggere la quale WikiLeaks è stata costruita.

Nel 2010 WikiLeaks ha avviato la sua a tutt'oggi più ambiziosa campagna di rivelazioni, svelando gli abusi sistematici del segreto di stato nell'esercito e nel governo degli Stati Uniti, pubblicazioni note come Collateral Murder, War Logs e Cablegate.[1] La risposta è stata lo sforzo concertato e incessante del governo Usa e dei suoi alleati per distruggere WikiLeaks.

Il gran giurì di WikiLeaks

Come diretta conseguenza delle pubblicazioni di WikiLeaks il governo Usa ha avviato un'indagine criminale che vede il contributo di diverse agenzie su Julian Assange e sul personale, sui sostenitori e sui presunti associati di WikiLeaks. Ad Alexandria, in Virginia, è stato costituito un

gran giurì con il contributo del ministero della Giustizia e dell'FBI per studiare la possibilità di incriminare Julian Assange e altri, anche per complotto in base allo Espionage Act del 1917. Alcuni pubblici ufficiali Usa hanno definito queste indagini di "dimensioni e natura senza precedenti". Durante i lavori del gran giurì non possono essere presenti giudici o avvocati difensori. Nelle successive udienze della commissione del Congresso, vari parlamentari hanno ventilato che lo Espionage Act potrebbe essere usato come strumento per colpire i giornalisti che "consapevolmente pubblicano informazioni riservate fatte trapelare", indicando che poco per volta questa politica si sta introducendo e normalizzando nel sistema giudiziario americano.[2]

Mentre andiamo in stampa le indagini su WikiLeaks continuano.[3] Parecchie persone sono state costrette dalla giustizia a fornire prove. Gli atti del processo a Bradley Manning, il soldato accusato di avere passato informazioni a WikiLeaks, rivelano l'esistenza di un dossier dell'FBI sulle indagini su WikiLeaks che supera le 42.100 pagine, di cui 8000 riguardano Manning. Bradley Manning è stato in carcere senza processo per oltre 880 giorni. Juan Mendez, il relatore speciale delle Nazioni Unite sulla tortura, ha valutato ufficialmente che Bradley Manning è stato trattato in modo crudele e disumano, che poteva corrispondere a tortura.[4]

L'esortazione all'assassinio di Julian Assange e l'ammissione dell'esistenza di più task force contro WikiLeaks

Le indagini del gran giurì non sono l'unica strada per aggredire WikiLeaks. Nel dicembre 2010, all'indomani di Cablegate, parecchi politici Usa hanno invocato l'assassinio extragiudiziale di Julian Assange, anche usando i droni. Alcuni senatori degli Stati Uniti hanno definito WikiLeaks un'"organizzazione terrorista" e Assange un "terrorista hi-tech" e "nemico combattente" impegnato nella "ciberguerra".[5]

Ancor prima della diffusione di Cablegate o dei War Logs sull'Iraq, è stata formata una squadra del Pentagono forte di

centoventi persone chiamata WikiLeaks Task Force, o WTF, per “intraprendere azioni” contro WikiLeaks. Sono tuttora operative simili task force ufficialmente ammesse anche all’interno di FBI, CIA e Dipartimento di stato.[6]

Censura diretta

Esercitando una censura senza precedenti su una pubblicazione giornalistica, il governo Usa ha fatto pressione sui provider di Internet perché sospendessero i servizi a WikiLeaks.org. Il primo dicembre 2010 Amazon ha rimosso WikiLeaks dai suoi server di storage, e il 2 è stato interrotto il servizio DNS che puntava al domain WikiLeaks.org. In questo periodo WikiLeaks è rimasta online solo grazie a una campagna di “mass-mirroring”: migliaia di sostenitori di WikiLeaks hanno copiato il sito web e ospitato la loro versione, diffondendo gli indirizzi IP attraverso i social network.[7]

L’amministrazione Obama ha avvertito i dipendenti federali che i materiali diffusi da WikiLeaks rimanevano segretati anche se pubblicati da alcune delle principali strutture giornalistiche al mondo, compresi “New York Times” e “Guardian”, e che accedere a quel materiale, che fosse su WikiLeaks o sul “New York Times”, sarebbe equivalso a una violazione della sicurezza.[8] Organismi pubblici come la Biblioteca del Congresso, il ministero del Commercio e l’esercito hanno bloccato l’accesso ai materiali di WikiLeaks nelle loro reti. Il divieto non era limitato al settore pubblico. Alcuni funzionari hanno avvertito le istituzioni accademiche che gli studenti che speravano di avviare una carriera nel settore pubblico dovevano rimanere alla larga dai materiali diffusi da WikiLeaks nelle loro ricerche e nelle attività online.

Censura finanziaria: il blocco bancario

WikiLeaks è finanziata dalle donazioni dei sostenitori. Nel dicembre 2010 i principali istituti bancari e di credito, tra cui Visa, MasterCard, PayPal e Bank of America, si sono piegati alle pressioni ufficiose degli Stati Uniti e hanno iniziato a

negare i servizi finanziari a WikiLeaks. Hanno bloccato i bonifici e tutte le donazioni effettuate con le principali carte di credito. Anche se sono tutti istituti americani, la loro ubiquità nella finanza mondiale significava che ai donatori volontari in America e all'estero veniva preclusa la possibilità di inviare soldi a WikiLeaks per sostenere le sue attività di pubblicazione.

Il "blocco bancario", com'è diventato noto, è portato avanti fuori da qualsiasi norma giudiziaria o amministrativa e rimane in vigore mentre andiamo in stampa. WikiLeaks ha intentato importanti cause in diverse giurisdizioni in tutto il mondo per spezzare questo embargo, con qualche vittoria preliminare. I processi sono ancora in corso. Nel frattempo è stata privata dei proventi, ha costi elevati e da quasi due anni è rimasta attiva attingendo alle riserve.

Il blocco bancario è la dimostrazione del potere di controllare le transazioni finanziarie fra terzi e compromette direttamente le libertà economiche dei singoli. Ma anche lasciando perdere questo risvolto, l'attentato alla sopravvivenza di WikiLeaks è il perfetto esempio di una nuova e preoccupante forma di censura economica globale.[9]

Alcuni presunti associati a WikiLeaks, assieme ai sostenitori e al personale stesso di WikiLeaks, hanno avuto misteriosi problemi con il proprio conto corrente, dall'estratto conto sino alla chiusura completa.

La persecuzione di Jacob Appelbaum e Jérémie Zimmermann

Il 17 luglio 2010 Julian Assange era prenotato per parlare all'HOPE, il convegno hacker di New York. Avendo dovuto cancellare la sua presenza, in sua vece s'è presentato Jacob Appelbaum. Da quel giorno le forze dell'ordine hanno avviato una campagna contro Appelbaum e le persone a lui vicine. Appelbaum viene continuamente fermato, perquisito, privato della presenza di un legale e interrogato alla frontiera ogni volta che esce dagli Stati Uniti o rientra. I suoi macchinari sono stati sequestrati e i diritti violati, e in queste occasioni gli sono state rivolte minacce di ulteriori violazioni dei suoi

diritti. La sua persecuzione ha coinvolto decine di strutture federali, dal ministero della Sicurezza interna, Immigrazione e Dogane fino all'esercito. I fermi hanno contemplato persino il rifiuto dell'accesso ai bagni come metodo per piegarlo. Nonostante ciò, Appelbaum non è mai stato incriminato né il governo gli ha spiegato come mai lo perseguita.[10]

A metà giugno 2011, mentre si apprestava a salire a bordo di un aereo all'aeroporto Dulles di Washington, Jérémie Zimmermann è stato bloccato da due persone che si sono identificate come agenti federali. I due l'hanno interrogato su WikiLeaks minacciandolo di arresto e successivo soggiorno in prigione.

Appelbaum e Zimmermann appartengono alla lunga lista di amici, sostenitori o presunti associati di Julian Assange che sono stati sottoposti a persecuzioni e sorveglianza da parte delle agenzie Usa, un elenco che comprende avvocati e giornalisti nello svolgimento della loro professione.

Il sequestro senza mandato dei dati elettronici e il "caso della citazione a Twitter"

Il 14 dicembre 2010 Twitter ha ricevuto dal ministero della Giustizia Usa una "citazione amministrativa" che le ordinava di cedere le informazioni che potessero essere pertinenti a un'indagine su WikiLeaks. Quel mandato era una cosiddetta "ordinanza 2703(d)", in riferimento a una sezione dello Stored Communications Act. Con questa legge il governo Usa si arroga l'autorità di costringere a rivelare i dati delle comunicazioni elettroniche private senza bisogno che ci sia un giudice a firmare un mandato di perquisizione, aggirando così le tutele del Quarto emendamento contro le perquisizioni e i sequestri arbitrari.

La citazione richiedeva gli username, i dati sulla corrispondenza, gli indirizzi, i numeri di telefono, i dettagli dei conti correnti e i numeri di carta di credito di account e persone presunti associati con WikiLeaks, compresi Jacob Appelbaum, la parlamentare islandese Birgitta Jonsdottir, l'uomo d'affari olandese pioniere di Internet Rop Gonggrijp e

la stessa WikiLeaks. Stando al mandato, a Twitter era perfino impedito di rivelare a costoro l'esistenza dell'ordinanza. Tuttavia Twitter si è appellata con successo contro questa clausola bavaglio e si è aggiudicata il diritto di informare gli indagati del fatto che i loro dati erano stati richiesti.

Saputo da Twitter del mandato, il 26 gennaio 2011 Appelbaum, Jonsdottir e Gonggrijp, rappresentati da Kecker e Van Nest, dalla American Civil Liberties Union e dalla Electronic Frountier Foundation, hanno fatto presentare dagli avvocati una mozione di annullamento dell'ordinanza. La vicenda è diventata nota come il "caso della citazione a Twitter".[11] Un'ulteriore mozione è stata presentata dall'avvocato di Appelbaum per richiedere la desegretazione degli atti giudiziari ancora riservati relativi ai tentativi del governo di ottenere dati privati da Twitter e da qualsiasi altra azienda. Entrambe le mozioni sono state respinte da un magistrato Usa l'11 marzo 2011. I querelanti si sono appellati.

Il 9 ottobre 2011 il "Wall Street Journal" ha rivelato che anche il provider californiano Sonic.net aveva ricevuto un mandato che richiedeva i dati di Jacob Appelbaum. La Sonic si era opposta senza successo ma aveva ottenuto il permesso di rivelare di essere stata costretta a cedere le informazioni su Appelbaum. Il "Wall Street Journal" ha inoltre riferito che anche Google aveva ricevuto un mandato simile, senza però specificare se l'azienda si era opposta.[12]

Il 10 novembre 2011 un giudice federale ha emesso una sentenza a sfavore di Appelbaum, Jonsdottir e Gonggrijp, decidendo che Twitter doveva cedere le loro informazioni al ministero della Giustizia.[13] Il 20 gennaio 2012 i querelanti si sono di nuovo appellati per contestare il rifiuto di rivelare le ordinanze eventualmente inviate ad altre aziende oltre a Twitter.[14] Mentre andiamo in stampa la causa è ancora in corso.

Aumento delle comunicazioni contro aumento della sorveglianza

JULIAN: Se torniamo ai primi anni novanta, alla nascita del movimento cypherpunk come reazione ai limiti imposti dagli stati alla crittografia, vediamo che c'era un sacco di gente interessata alla potenzialità di Internet di fornire comunicazioni libere e senza censura rispetto ai media classici. Però i cypherpunk capivano anche che nella realtà assieme a questo c'era anche la possibilità di sorvegliare tutte le comunicazioni in corso. Oggi ci ritroviamo con un aumento delle comunicazioni contro un aumento della sorveglianza. Aumento delle comunicazioni significa che hai una maggiore libertà nei confronti di quelli che cercano di controllare le idee e di manipolare il consenso, mentre aumento della sorveglianza significa l'esatto contrario.

La sorveglianza è assai più evidente oggi che non ai tempi in cui il grosso era portato avanti solo da americani, britannici, russi e qualche altro governo come quello svizzero e quello francese. Adesso è praticata da tutti e da quasi tutti gli stati a causa della messa in commercio della sorveglianza di massa. E oggi è totalizzante perché la gente sbatte in rete le sue simpatie politiche, le comunicazioni familiari e le amicizie. Perciò non è che abbiamo una maggiore sorveglianza delle comunicazioni, questa c'era anche prima. È che ci sono molte più comunicazioni. E non c'è solo un aumento del volume delle comunicazioni, c'è un aumento delle forme di comunicazione. Tutte queste nuove forme di comunicazione, che in precedenza sarebbero state riservate, oggi vengono intercettate in massa.

C'è una battaglia in corso tra il potere di queste

informazioni raccolte dall'interno, da questi stati ombra dell'informazione che stanno nascendo, scambiandosi materiale, sviluppando collegamenti l'uno con l'altro e con il settore privato, e l'aumento dei beni comuni, con Internet come strumento comune perché l'umanità si possa parlare.

Vorrei che riflettessimo su come presentare le nostre idee. Il grosso problema che ho avuto, in quanto persona intimamente coinvolta nella sorveglianza statale e che sa quanto il settore della sicurezza transnazionale s'è sviluppato nell'ultimo ventennio, è che lo conosco sin troppo bene e pertanto non riesco più a vederlo in un'ottica comune. Solo che adesso il nostro mondo è il mondo di tutti perché ciascuno ha sbattuto in Internet il nucleo segreto della sua vita. Dobbiamo comunicare in qualche maniera quello che sappiamo finché possiamo.

Andy: Propongo di ragionarci su non dal punto di vista del cittadino ma dal punto di vista di chi ha il potere. L'altro giorno ho partecipato a un curioso convegno a Washington in cui ho incrociato certi tizi con il tesserino dell'ambasciata tedesca. Mi sono avvicinato e ho detto: "Oh, siete dell'ambasciata tedesca" e loro: "Ehm, non esattamente dell'ambasciata, siamo di un posto vicino a Monaco". S'è poi scoperto che erano dei servizi di informazione per l'estero. Durante il rinfresco serale gli ho domandato qual è la vera ragion d'essere dei servizi segreti e loro hanno risposto: "Be', sta tutto nel rallentare i processi per poterli controllare meglio". È il senso di questo tipo di lavoro di intelligence, rallentare un processo sottraendo alla gente la capacità di capirlo. Dichiarare segrete le cose significa che limiti la quantità di persone che detengono il sapere e pertanto la capacità di influenzare quel processo.

Se guardi Internet nell'ottica di chi detiene il potere, gli ultimi vent'anni devono essere stati spaventosi. Quella gente considera Internet una malattia che compromette la loro possibilità di influenzare la realtà, di definire quello che succede, possibilità che è poi usata per decidere quello che la gente può sapere che sta succedendo e la sua capacità di

interagirci. Se guardi, che so, l'Arabia Saudita, dove per un accidente della storia i capi religiosi e quelli che possiedono la maggior parte del paese sono le stesse persone, il loro interesse al cambiamento è circa zero. Forse sotto zero. Considerano Internet una malattia e chiedono ai loro consulenti: "Avete qualche medicina contro quella roba là? Dobbiamo farci trovare immuni se colpisce il nostro paese, se arriva quella roba di Internet". E la risposta è la sorveglianza di massa, è "dobbiamo controllare in toto, dobbiamo filtrare, dobbiamo sapere tutto quello che fanno". È esattamente quanto è successo negli ultimi vent'anni. Ci sono stati massicci investimenti nella sorveglianza perché la gente al potere temeva che Internet influenzasse il modo in cui governano.

JULIAN: Eppure, nonostante questa sorveglianza di massa, le comunicazioni di massa hanno permesso a milioni di persone di arrivare a un consenso rapido. Se puoi passare molto velocemente da una posizione normale a una nuova posizione di consenso di massa, allora lo stato può anche accorgersi che sta nascendo ma non ha il tempo di impostare una risposta efficace.

Detto questo, c'è stata al Cairo nel 2008 una manifestazione di protesta organizzata su Facebook. Ha colto di sorpresa il governo di Mubarak, ma il risultato è che quella gente è stata rintracciata proprio usando Facebook.[1] Nel 2011, la prima pagina di un manuale che è stato uno dei più importanti documenti utilizzati nella rivoluzione egiziana affermava "non usate Twitter o Facebook" per diffonderlo, e l'ultima pagina ripeteva di "non usare Twitter o Facebook" per distribuire il manuale.[2] Ugualmente un sacco di egiziani ha usato Twitter e Facebook, ma sono riusciti a sfangarla perché la rivoluzione ha vinto. Se non avesse avuto successo allora quella gente se la sarebbe passata brutta, molto brutta. E non dimentichiamo che quasi subito il presidente Mubarak ha oscurato Internet in Egitto. In realtà è tutto da discutere se il black-out di Internet ha facilitato la rivoluzione o l'ha danneggiata. Alcuni pensano che l'abbia facilitata perché la

gente era costretta a scendere in strada per avere notizie di quello che stava succedendo, e una volta che sei sceso in strada sei sceso in strada. E poi la popolazione s'è sentita colpita direttamente perché il cellulare e Internet non funzionavano più.

Perciò, se un'azione vuole avere successo, deve raggiungere una massa critica, deve essere fulminea e deve vincere perché se non vince la medesima infrastruttura che permette di arrivare a una veloce unanimità sarà usata per rintracciare ed emarginare tutte le persone coinvolte nella diffusione del consenso.

Era l'Egitto, che era un alleato Usa, certo, ma non fa parte dell'alleanza spionistica anglofona Stati Uniti, Regno Unito, Australia, Nuova Zelanda e Canada. Adesso proviamo invece a immaginare la rivoluzione egiziana che scoppia negli Stati Uniti. Che succederebbe a Twitter e Facebook? Sarebbero sequestrate dallo stato. E se la rivoluzione fallisse sarebbero setacciate, come adesso, da CIA e FBI in cerca di dati sui suoi protagonisti.

JÉRÉMIE: È difficile scindere la sorveglianza dal controllo. Dobbiamo affrontare entrambi i temi. A me interessa più questo, il controllo di Internet, che sia portato avanti dal governo o dalle multinazionali.

JACOB: Credo sia abbastanza chiaro che la censura è un sottoprodotto della sorveglianza in genere, che sia un'autocensura o vera censura in senso tecnico, e credo che un modo importante per farlo capire alla gente normale sia spiegarlo a livelli poco tecnici. Per esempio, se avessimo costruito le strade come abbiamo costruito Internet, ciascuna avrebbe dovuto avere le telecamere di sorveglianza e i microfoni a cui può accedere solo la polizia, o qualcuno che s'è fatto passare per poliziotto.

JULIAN: Jake, in Gran Bretagna ci stanno arrivando.

JACOB: Quando costruisci una strada non è necessario che ogni millimetro sia monitorato con una sorveglianza totale a

cui può accedere solo un gruppo riservato di persone. Spiegare all'uomo della strada che è così che stiamo costruendo le strade di Internet e poi richiediamo alla gente di usarle, be', ecco una cosa che l'uomo della strada può afferrare appena capisce che i costruttori della strada non saranno sempre quelli che la controllano.

ANDY: Però certa gente non ha nemmeno costruito strade. Ha piazzato lì un giardino invitando tutti a starci nudi. Siamo arrivati a Facebook! Fa soldi facendo sentire la gente a suo agio quando rivela i propri dati.

JACOB: Esatto. Una volta la gente veniva ricompensata perché lavorava nella Stasi, la vecchia polizia politica della Germania Est, mentre oggi viene ricompensata perché è su Facebook. Solo che in Facebook viene ricompensata con crediti sociali, tipo scopare con il vicino, invece di essere pagata direttamente. Ed è importante metterlo in relazione con l'aspetto umano, perché non riguarda la tecnologia, riguarda il controllo attraverso la sorveglianza. Sotto certi aspetti è il perfetto Panopticon.[3]

JULIAN: A me interessa la filosofia della tecnica. Tecnica non è soltanto un pezzo di tecnologia ma, che so, il consenso della maggioranza di un consiglio di amministrazione o la struttura di un parlamento, è l'interazione sistematizzata. Per esempio, se non sbaglio i sistemi feudali sono nati dalla tecnica dei mulini. Una volta che avevi i mulini centralizzati, che richiedevano enormi investimenti ed era facile sottoporre a un controllo fisico, era abbastanza naturale avere come esito i rapporti feudali. Nel tempo sembra che abbiamo messo a punto tecniche sempre più sofisticate. Alcune possono essere rese più democratiche, allargate a tutti, ma la maggior parte, a causa della loro complessità, sono tecniche che sfociano in organizzazioni fortemente interconnesse come la Intel Corporation. Forse la tendenza implicita della tecnica è attraversare questi periodi di scoperta, centralizzazione, democratizzazione tecnologica, quando il sapere come si fa tracima nella successiva generazione istruita. Però credo che

la tendenza generale della tecnica sia quella di centralizzare il controllo nelle persone che controllano le risorse fisiche delle tecniche.

Il perfetto esempio, secondo me, è il produttore di semiconduttori quando ti serve talmente tanto ordine che l'aria stessa deve essere incontaminata, quando ti serve uno stabilimento con migliaia di dipendenti che devono tenere la retina in testa per isolare ogni granello di forfora e ogni capello dal processo di manifattura dei semiconduttori, che è una procedura a più stadi estremamente complicata. E vedi letteralmente milioni di ore di sapere nato dalla ricerca in mano all'organizzazione che fabbrica i semiconduttori. Se queste cose sono popolari, e lo sono, e sono le fondamenta di Internet, allora dentro la liberazione di Internet è codificata la produzione dei semiconduttori. E dentro la produzione dei semiconduttori è codificata la possibilità per chiunque detenga il controllo fisico del fabbricante di semiconduttori di ricavare enormi agevolazioni.

Perciò alla base della rivoluzione delle comunicazioni hi-tech, e della libertà che ne abbiamo ricavato, c'è l'intera economia moderna di mercato, neoliberale, transnazionale e globalizzata. In realtà ne è il vertice. È il massimo, in termini di risultato tecnologico, che la moderna economia neoliberale globalizzata può produrre. Internet è sorretta da interazioni commerciali estremamente complesse tra produttori di fibre ottiche, fabbricanti di semiconduttori, compagnie minerarie che estraggono tutta questa roba e i vari lubrificanti finanziari che permettono i commerci, i tribunali per far rispettare le leggi sulla proprietà e così via. Così diventa il vertice della piramide dell'intero sistema neoliberale.

Andy: Per quanto riguarda la tecnica: quando Johannes Gutenberg inventò la stampa, venne proibita in certe parti della Germania, ed è proprio per questo che s'è diffusa in tutto il paese, perché appena era proibita in una regione si spostava in un'altra giurisdizione.[4] Non ho studiato tutti i particolari, ma so che si sono dovuti scontrare con la chiesa cattolica perché stavano spezzando il monopolio dei libri

scritti, e così appena avevano problemi legali si spostavano in un posto in cui non era proibita. In un certo senso ne ha aiutato la diffusione.

Internet, secondo me, è stata lievemente diversa perché qui hai delle macchine che possono essere usate come mezzo di produzione, com'era persino il Commodore 64, a modo suo, dato che tanta gente lo usava per altri scopi...

JULIAN: Ogni macchinetta che avevi poteva far girare il tuo programma.

ANDY: Sì. E potevi anche usarlo per diffondere idee. Ma dall'altro lato, in senso filosofico, come disse John Gilmore, uno dei fondatori della statunitense Electronic Frontier Foundation, all'inizio degli anni novanta, quando Internet arrivò a una diffusione globale: "La rete interpreta la censura come un danno e la aggira".[5] Come ormai sappiamo, era un misto di interpretazione tecnica combinata con un'ottica ottimista sui suoi effetti, una specie di pio desiderio e anche una specie di profezia che si autorealizza.

JULIAN: Però valeva anche per Usenet, un sistema di posta elettronica da molti a molti, per così dire, nato circa trent'anni fa. Per spiegarlo in parole semplici, immaginate che non ci sia alcuna differenza tra persone e server e che ogni persona faccia funzionare il proprio server Usenet. Scrivi qualcosa, poi lo passi a una o due persone. Loro (in automatico) controllano se ce l'hanno già. Se non ce l'hanno già lo prendono e lo passano a tutti coloro con cui sono collegati. E così via. Alla fine il messaggio scorre attraverso tutti, e tutti ne ottengono una copia. Se una persona è disposta a censurare allora viene semplicemente ignorata, non cambia nulla. Il messaggio continua a passare tra le persone che non censurano. Gilmore stava parlando di Usenet, non di Internet. E non parlava nemmeno di pagine web.

ANDY: Anche se è tecnicamente corretto, l'interpretazione delle parole di Gilmore e il loro impatto a lungo termine

hanno generato tante persone che si immedesimavano con Internet. La gente diceva: “Bene, c’è la censura, e noi l’aggireremo”, mentre i politici che non capivano un accidente di cose tecniche pensavano: “Oh, merda, c’è una nuova tecnologia che limita il nostro controllo della sfera dell’informazione”. Insomma, penso che Gilmore, che è stato uno dei precursori del cypherpunk, abbia fatto un gran lavoro nello spingere le cose in questa direzione, un lavoro che ha ispirato tutto il modo cryptoanarchico a cercare una propria forma di comunicazione anonima, senza alcun timore di essere monitorati.

Jérémie: Noto una differenza con la diffusione della tecnologia di cui abbiamo parlato perché nel caso del mulino e del torchio da stampa bastava guardarne uno per capire come funzionava, mentre oggi stiamo inserendo sempre di più il controllo dentro la tecnologia. Il controllo è insito. Se guardi un computer moderno, in tanti casi non puoi nemmeno aprirlo per identificare tutte le componenti. E tutte le componenti stanno dentro delle scatoline, e comunque non puoi capire che cosa fanno.

Andy: A causa della complessità?

Jérémie: A causa della complessità e perché la tecnologia stessa non è pensata per essere compresa. Come nel caso della tecnologia proprietaria.[6] Cory Doctorow ne parla nel suo *The War on General-Purpose Computing*.[7] Se il computer è una macchina generica, general-purpose, puoi farci di tutto. Puoi elaborare qualsiasi informazione come input, trasformarla in qualsiasi cosa come output. E sempre più spesso costruiamo macchinari che sono simili ai computer generici ma sono limitati al GPS o alle telefonate o a riprodurre MP3. Costruiamo sempre più macchine che hanno inserito un controllo interno per impedire all’utente di fare certe cose.

Julian: È un controllo interno per impedire alla gente di capirle e modificarle rispetto allo scopo che si prefiggeva il fabbricante, però oggi abbiamo anche di peggio perché sono

connesse alla rete.

Jérémie: Sì, così possono contenere la funzione di monitorare l'utente e i suoi dati. È per questo che il software libero è tanto importante per una società libera.

Andy: Sono assolutamente d'accordo sul fatto che ci serve una macchina generica, però stamattina mentre tentavo di venire qui da Berlino l'aereo non riusciva a partire. È la prima volta che mi succede. L'apparecchio s'è spostato dalla pista e il pilota ha detto: "Signore e signori, abbiamo avuto un problema al sistema elettrico, perciò abbiamo deciso di fermarci per riavviare i sistemi". Io intanto pensavo: "Oh, merda, mi ricorda il riavvio di Windows, Control Alt Delete. Forse funziona!". Perciò non sarei poi tanto contrario ad avere una macchina con un solo scopo su un aereo che fa solo quello e lo fa bene. Se sto seduto su un oggetto volante non voglio che i piloti siano distratti perché giocano a Tetris o sono stati infettati da Stuxnet o quant'altro.[8]

Jérémie: L'aereo di per sé non elabora i tuoi dati personali, non controlla la tua vita.

Andy: Be', per un po' una macchina volante ha controllato la mia.

Jacob: Secondo me, potremmo spiegare la tesi di Cory dicendo anche che non ci sono più auto, non ci sono più aerei, non ci sono più apparecchi acustici, ci sono invece computer a quattro ruote, computer con le ali e computer che ti aiutano a udire. E il problema, almeno in parte, non è se sono computer creati per un solo scopo o no, è se possiamo verificare o no che facciano la cosa che dicono di fare e se capiamo quanto bene la fanno. Spesso quelli là sostengono di avere il diritto di metterlo sotto chiave e mantenerlo segreto, e fanno i computer complessi oppure difficili da capire. In realtà è pericoloso per la società perché sappiamo che la gente non agisce sempre nell'interesse di tutti, e sappiamo pure che commette errori, anche se non è armata di cattive

intenzioni, e pertanto mettere sotto chiave queste cose è molto pericoloso a tanti livelli, non ultimo il fatto che siamo tutti imperfetti. È così. La possibilità di accedere ai progetti di lavorazione dei sistemi che sono alla base delle nostre vite è uno dei motivi per cui è importante il software libero, ma per cui è importante anche l'hardware libero. Migliora la nostra capacità di fare investimenti sostenibili in maniera libera, di migliorare i sistemi che usiamo e di decidere se questi sistemi funzionano come previsto.

Però, indipendentemente dalla libertà, è anche il motivo per cui è importante comprendere questi sistemi perché quando non li capiamo c'è una tendenza generale a deferire all'autorità, alla gente che li capisce o può reclamarne il controllo, anche se non coglie l'essenza intrinseca della cosa. È per questo che vediamo tutto questo battage sulla ciberguerra, perché certa gente che sembra autorevole in campo bellico attacca a parlare di tecnologia come se la capisse. Spesso questa gente parla di ciberguerra e nessuno, non uno di loro, parla di ciberpace o alcunché che abbia a che vedere con il peace-building. Stanno sempre a parlare di guerra perché è il loro business e perché stanno cercando di controllare i processi tecnologici e giudiziari come mezzo per favorire i propri interessi. Perciò se non abbiamo il minimo controllo della nostra tecnologia quella gente spera di usarla per i propri scopi, nello specifico per la guerra. È la ricetta giusta per creare roba piuttosto spaventosa, ed è così, secondo me, che siamo finiti con Stuxnet, e persone per il resto ragionevoli suggeriscono che, in un periodo in cui gli Stati Uniti scatenano guerre, queste trovate in qualche maniera impediranno le guerre. Forse sarebbe un discorso ragionevole per un paese che non sta invadendo direttamente altre nazioni, ma è poco credibile nel contesto di una nazione coinvolta contemporaneamente in più invasioni ancora in corso.

JULIAN: Noto una certa militarizzazione del ciberspazio, nel senso di occupazione militare. Quando comunichi via Internet, quando comunichi con la telefonia mobile, che è ormai intrecciata con Internet, le tue comunicazioni vengono intercettate dai servizi d'informazione militari. È come avere un carro armato in camera da letto, un soldato fra te e tua moglie mentre mandate sms. Viviamo tutti sotto legge marziale per quanto riguarda le nostre comunicazioni, non vediamo i carri armati ma ci sono. In questo senso Internet, che doveva essere uno spazio civile, è diventata uno spazio militarizzato. Però è il nostro spazio perché la usiamo tutti quanti per comunicare con gli altri e con i membri della nostra famiglia. Le comunicazioni al cuore della nostra vita privata oggi passano in Internet, perciò nella pratica la nostra vita privata è entrata in zona militarizzata. È come avere un soldato sotto il letto. È una militarizzazione della vita civile.

JACOB: Poco prima di venire qui mi hanno chiesto se volevo fare l'allenatore della squadra del Laboratorio di ricerca sulla sicurezza e la privacy nel torneo Pacific Rim Collegiate Cyber Defense. Mi hanno chiesto all'ultimo minuto di fare il consulente. Abbiamo passato un tot di tempo impegnati in una ciberguerra in cui SPAWAR, una branca civile della marina militare Usa che prevede anche servizi di penetration test, che fa hacking difensivo quanto offensivo, era quella che si chiama di solito la Squadra rossa.[1] Attacca tutti gli altri partecipanti, e il compito delle altre squadre consiste nella difesa dei propri sistemi informatici, che gli sono stati

assegnati all'inizio del torneo senza che ne sapessero nulla in anticipo. Non sai quale sistema dovrai difendere e all'inizio non è nemmeno chiaro come segni i punti, perciò puoi fare solo del tuo meglio e sperare in bene.

JULIAN: Sei sicuro che sia davvero un gioco? Forse non è un gioco!

JACOB: No, ti danno solo un gruppo di computer che devi proteggere mentre gli altri penetrano e prendono possesso del sistema. È una specie di rubabandiera in versione hacker o qualcosa del genere, ed è interessante perché quelli là hanno un sacco di strumenti, hanno scritto dei programmi.[2]

JULIAN: Ma a che serve, dal punto di vista della marina militare Usa?

JACOB: Be', per quanto riguarda loro lo stanno solo sponsorizzando perché vogliono formare i ciberguerrieri di domani, e infatti, per mostrarvi un esempio tangibile, vi ho portato una nota della CIA, che stava reclutando. Un certo Charlie, Charlie della CIA, spiegava che se sei disposto a entrare nell'agenzia hai la grande occasione di lavorare nel mondo reale. E c'erano quelli di SPAWAR, e anche la Microsoft stava reclutando. Pensavano di addestrare tutta quella gente, tutte le squadre, per partecipare al campionato nazionale "difesa della patria" e vincerlo, poi anche proseguire facendo hack offensivi come ciberguerrieri, non solo ciberdifensori. Abbiamo segnato qualcosa come 4000 punti in questo torneo, la somma totale dei punteggi delle squadre arrivate seconda, terza e quarta. In realtà eravamo ancora più su di tutte loro messe insieme.

JULIAN: Ehilà.

JACOB: Non è stato grazie a me, il mio slogan per motivarli era: "Ehi, fa sempre più scuro prima che diventi buio pesto". Non credo di essere un allenatore particolarmente in gamba, sono stati bravi i ragazzi. Però è stato interessante perché

tutta la faccenda era inquadrata in termini bellici, tipo che dicevano: “Ehi, vogliamo sentire il vostro grido di battaglia”. E noi: “Prego?”. Era per esempio quello che dicevano a pranzo, quando ci concedevamo una pausa dalla difesa dei nostri sistemi. Inquadravano tutto in termini di attaccare sistemi e guerra e ciberguerra e quanto è fantastico questo modo di pensare. Dettaglio abbastanza interessante, a parte la squadra con cui stavo lavorando, m’è parso che ci fosse tanta gente a disagio perché non gli stavano insegnando l’Arte della guerra, era più una Coppa amministratori di sistema, di difensori dei sistemi. Che schifo.[3] Era strano forte perché c’era tutta questa gente con un retroterra guerresco, gente con una mentalità marziale, ma non insegnavano strategia, erano concentrati sulla retorica della difesa di questi sistemi o dell’attacco a questi altri sistemi, e c’era parecchia guerra nell’aria quando tentavano di montare la gente in una sorta di fervore patriottico. Non favorivano il pensiero creativo o un’impostazione per svolgere un’analisi indipendente, stavano inculcando la mentalità da rotellina dell’ingranaggio di chi esegue gli ordini per il bene della nazione. Non m’era mai capitato prima. Avevo la nausea e quasi tutta la mia squadra ha avuto problemi a mandarla giù o anche solo a prenderla sul serio.

Julian: Credi che sia un classico addestramento della marina Usa e che adesso stiano solo tentando di applicarlo in un altro ambito? È una decisione dall’alto del cibercomando Usa, una decisione strategica internazionale degli Stati Uniti?

Andy: Ricorda più i campi giovanili nazisti in cui addestravano i bambini.

Jacob: *Sie können das sagen weil du bist Deutsche*. Lo puoi dire perché sei tedesco. No, non è così. Il coinvolgimento della marina Usa c’è solo perché è il governo Usa che finanzia tutta questa roba. M’hanno chiesto di fare l’allenatore perché avevano bisogno di qualcuno e io ho accettato perché mi piacevano i ragazzi coinvolti, gli studenti. Però in pratica il governo Usa sta sul serio cercando di

spingere la gente a questo genere di cose, e in un'ottica nazionalista. È un evento molto, molto strano perché da un lato è bello poter sapere come proteggere il proprio sistema e capire tutta l'infrastruttura a cui affidiamo le nostre vite, ma dall'altro non stavano cercando di convincere la gente a capirlo, cercavano di montarli in una specie di fervore perché fossero felici di fare questo tipo di lavoro.

ANDY: Purtroppo l'interesse degli Stati Uniti per i sistemi sicuri è estremamente limitato perché loro preferiscono che siano vulnerabili per poterne assumere il controllo. La politica del controllo della crittografia a livello mondiale non è arrivata fino al livello verso cui spingevano in origine gli Stati Uniti attorno al 1998, quando il sottosegretario Usa del Commercio internazionale David Aarons partì per un tour mondiale in cui sosteneva l'accesso del governo alle password crittografiche di tutti quanti.[4] Però la crittografia è ancora trattata come una cosiddetta tecnologia duale e la sua esportazione sotto forma di prodotti end-user in tanti paesi è limitata per legge, un provvedimento accettato in tutto il mondo in base al cosiddetto accordo di Wassenaar.[5] Potrebbe suonare ragionevole nel momento in cui si definiscono "canaglia" certi paesi e le loro attività, però evidenzia le dimensioni del doppio binario, dato che finora la tecnologia della sorveglianza delle telecomunicazioni non è limitata dal controllo delle esportazioni.[6]

JULIAN: Andy, tu progetti da anni telefoni cifrati. Che razza di sorveglianza di massa abbiamo nelle telecomunicazioni? Spiegami lo stato dell'arte per quanto riguarda il settore raccolta informazioni e sorveglianza di massa da parte del governo.

ANDY: Storage di massa, intendo la conservazione di tutte le telecomunicazioni, tutte le chiamate, tutti i dati sul traffico, i vari modi in cui i gruppi utilizzano lo Short Message Service (SMS), ma anche connessioni Internet, almeno in certe situazioni limitate alle e-mail. Se raffronti il bilancio militare e il costo dei ciberguerrieri, capisci subito che il classico

sistema degli armamenti costa una montagna di soldi. I ciberguerrieri o la sorveglianza di massa sono supereconomici rispetto anche a un solo aereo. Un apparecchio militare ti costa tra…

JULIAN: Circa cento milioni.

ANDY: E la conservazione dei dati costa sempre di meno ogni anno che passa. Anzi, noi del Chaos Computer Club abbiamo fatto qualche calcolo: puoi avere storage di qualità vocale di tutte le telefonate tedesche di un anno per circa 30 milioni di euro compresi i costi di gestione, e lo stoccaggio puro viene circa 8 milioni.[7]

JULIAN: E ci sono persino aziende come la VASTech in Sudafrica che vendono questi sistemi per 10 milioni di dollari all'anno.[8] "Noi intercetteremo tutte le vostre chiamate, e conserveremo in blocco tutte le vostre chiamate intercettate." Però c'è stato uno spostamento negli ultimi anni dall'intercettazione di tutto quello che viaggia da un paese all'altro, pizzicando solo le persone specifiche che vuoi spiare e assegnandole a esseri umani. Oggi intercetti tutti e conservi tutto per sempre.

ANDY: Per spiegarlo a grandi linee dal punto di vista storico, un tempo uno diventava un obiettivo per la sua posizione diplomatica o perché lavorava per un'azienda, perché era sospettato di qualcosa oppure era in contatto con persone che facevano qualcosa, e tu gli imponevi misure di sorveglianza. Oggigiorno è ritenuto molto più efficace dire: "Prendiamo tutto e selezioniamo dopo". Così abbiamo lo stoccaggio a lungo termine e i termini più usati per descrivere i due capisaldi del settore sono approccio "tattico" e approccio "strategico". Tattico significa "in questo momento, in questa riunione, dobbiamo piazzare delle cimici sul posto, dobbiamo inserire qualcuno con un microfono o con un giubbotto con i fili, oppure installare su un'auto sistemi di sorveglianza GSM (Global System for Mobile communications) in grado di intercettare al volo quel che

dice la gente senza bisogno di interagire con l'operatore di rete, di ottenere un mandato o roba del genere, senza procedure legali, basta farlo". L'approccio strategico è farlo di default, registrare tutto e poi setacciare usando sistemi analitici.

JULIAN: Perciò l'intercettazione strategica è prendere tutto quello che rimbalza da un satellite delle telecomunicazioni o

ANDY: Perché non sai mai quando uno è sospettato.

JACOB: C'è una vicenda negli Stati Uniti chiamata causa NSA AT&T, o meglio, la seconda causa, Hepting contro AT&T. A Folsom, in California, Mark Klein, un ex tecnico del gigante delle telecomunicazioni AT&T, ha rivelato che la NSA, la statunitense National Security Agency, stava trattenendo tutti i dati che convinceva la AT&T a passarle. Prendevano tutto in blocco, anche le chiamate vocali, così ogni volta che ho sollevato la cornetta o mi collegavo a Internet a San Francisco nel periodo di cui parlava Mark Klein la NSA stava captando tutto quanto passasse su suolo Usa contro i cittadini Usa.[9] Sono abbastanza sicuro che abbiano usato quei dati intercettati nelle indagini su certe persone negli Stati Uniti, e questo solleva tutta una serie di interessanti quesiti costituzionali, perché li conservano per sempre.

JÉRÉMIE: Abbiamo anche l'esempio di Eagle, il sistema commercializzato dalla francese Amesys che è stato venduto alla Libia di Gheddafi, e sulla bolla di accompagnamento c'era scritto "meccanismo di intercettazione su scala nazionale". È una grossa scatola che piazzi in un posto e ti permette di ascoltare tutte le comunicazioni del tuo popolo.[10]

JULIAN: Dieci anni fa era considerata una favola, una storia a cui potevano credere soltanto i paranoici, però oggi i costi dell'intercettazione di massa sono scesi al punto che persino un paese come la Libia dalle risorse relativamente scarse la stava attuando usando tecnologia francese. In realtà molti paesi sono già pronti in termini di vere intercettazioni. Il

prossimo grande balzo in avanti sarà l’efficienza nel capire e nel reagire a quanto viene intercettato e immagazzinato. Oggi tanti paesi hanno l’intercettazione strategica di tutto il traffico da e per la nazione, però innescare le azioni successive, come il blocco automatico dei conti correnti, o l’uso della polizia o la marginalizzazione di gruppi specifici oppure l’elevazione di altri è ancora una cosa in cui noi siamo imbattibili. Siemens vende una piattaforma per le agenzie di raccolta informazioni che produce vere azioni automatizzate. Così quando l’obiettivo A si trova a un certo numero di metri dall’obiettivo B secondo le loro intercettazioni mobili, riceve una e-mail con una parola d’ordine o simili, poi si innesca l’azione. Ci siamo quasi arrivati.

Jérémie: Insomma, ormai è un fatto assodato che la tecnologia consente la sorveglianza totale di qualsiasi comunicazione. Ma c’è l’altra faccia della medaglia, cioè che cosa ci facciamo. Possiamo anche ammettere che ci siano alcuni utilizzi legittimi per quella che chiamano sorveglianza tattica, i poliziotti che indagano i cattivi e le loro reti eccetera possono avere bisogno di usare questi strumenti sotto la supervisione della magistratura, però il problema è dove tracciare la linea di demarcazione, dove finisce il controllo che possono avere i cittadini sull’uso di queste tecnologie. È un problema politico. Quando arriviamo a questi problemi troviamo uomini politici ai quali chiedono soltanto di firmare qualcosa e che non capiscono la tecnologia implicata, e secondo me noi come cittadini abbiamo un ruolo da svolgere, non solo spiegare come funziona la tecnologia in genere, pure agli uomini politici, ma anche buttarci nei dibattiti politici attorno all’uso di queste tecnologie. So che in Germania c’è stato un enorme movimento contro la conservazione generalizzata dei dati che ha portato alla cancellazione della legge relativa da parte della Corte costituzionale.[1] Ed è aperto un dibattito nell’Unione europea sulla revisione della direttiva sulla conservazione dei dati.[2]

Andy: Stai descrivendo la teoria dello stato democratico che naturalmente deve isolare qualche cattivo qua e là e ascoltare le sue telefonate in seguito a una decisione del tribunale per essere indicativamente sicuri che sia fatto nel modo giusto. Il problema è che le autorità devono agire in

conformità con le leggi. Se non fanno questo allora a che servono? In particolar modo con questo approccio strategico, gli stati democratici europei comprano pletore di macchinari che gli permettono di agire esattamente al di fuori della legge con le intercettazioni perché non hanno bisogno di un'ordinanza del tribunale, basta premere il pulsante e farlo, ed è una tecnologia che non può essere controllata.

JULIAN: Però ci sono due modi di affrontare la sorveglianza statale di massa: con le leggi della fisica e con le leggi dell'uomo. Il primo significa sfruttare le leggi della fisica costruendo materialmente congegni che impediscono le intercettazioni. L'altro è introdurre controlli democratici attraverso la legge per verificare che quelli debbano avere dei mandati e compagnia bella e cercare di ottenere una qualche trasparenza. Però le intercettazioni strategiche non possono farne parte, non possono essere limitate in maniera significativa dai regolamenti. L'intercettazione strategica significa intercettare *tutti*, che siano innocenti o colpevoli. Non dobbiamo dimenticare che è il centro del potere a svolgere questa sorveglianza. Ci sarà sempre una scarsa volontà politica di far uscire allo scoperto lo spionaggio di stato. E la tecnologia è intrinsecamente tanto complessa e il suo uso pratico tanto segreto che non potrà mai esserci una significativa supervisione.

ANDY: Oppure spii il tuo stesso parlamento.

JULIAN: Ma sono soltanto scuse, la mafia e le spie straniere, sono solo scuse perché la gente accetti un sistema del genere.

JACOB: I Quattro Cavalieri dell'Infocalisse: pornografia infantile, terrorismo, riciclaggio e la Guerra a Certe Droghe.

JULIAN: Una volta che hai messo in campo questa sorveglianza, dato che è complessa, dato che è progettata per operare in segreto, non è forse vero che non può essere regolamentata dalla politica? Io penso che, a parte

piccolissime nazioni come l'Islanda, a meno che non ci siano condizioni rivoluzionarie, semplicemente non è possibile controllare l'intercettazione di massa con le leggi e la politica. Non succederà mai. È troppo a buon mercato ed è troppo facile aggirare la trasparenza politica e attuare intercettazioni. Gli svedesi hanno approvato nel 2008 una legge sulle intercettazioni, nota come FRA-lagen. Comportava che la FRA, l'agenzia di controspionaggio svedese, potesse intercettare legalmente tutte le comunicazioni che viaggiano in massa nel paese e spedirle negli Stati Uniti, con qualche caveat.[3] Bene, come puoi far rispettare queste diffide una volta che hai messo insieme il sistema di intercettazioni e che l'organizzazione che le attua è un'agenzia di spie e agenti segreti? È impossibile. E infatti si sono visti casi che dimostrano che la FRA aveva in varie occasioni infranto la legge. Molti paesi lo fanno semplicemente fuori dalla legge, senza la minima copertura legislativa. Siamo già fortunati se, come nel caso svedese, hanno deciso che per tutelarsi dalle accuse vogliono rimanere sul legale cambiando la legge. Ed è il caso di quasi tutti i paesi, fanno intercettazioni di massa, e quando c'è una proposta di legge serve solo a parare il culo di chi le attua.

Questa tecnologia è molto complessa. Per esempio, nel dibattito in corso in Australia e nel Regno Unito sulla proposta di una legge per intercettare tutti i metadati, tanta gente non capisce il valore dei metadati o persino la parola stessa.[4] Intercettare tutti i metadati significa che devi costruire un sistema che intercetta fisicamente tutti i dati e poi butta via tutto quanto a parte i metadati. Però non ti puoi fidare di un sistema del genere. Non è possibile capire se intercetta e conserva tutti i dati se non hai dei tecnici esperti autorizzati ad andare a controllare che cosa succede esattamente, e non c'è la minima volontà politica di consentire questo accesso. Il problema si sta aggravando perché la complessità e la segretezza sono una miscela tossica. Nascosto dalla complessità. Nascosto dalla segretezza. La mancanza di trasparenza è intrinseca. È un suo aspetto. È pericoloso già per come è progettato.

Jérémie: Non sto dicendo che la strategia politica potrebbe funzionare, solo che è così che funzionerebbe in teoria un sistema democratico, e infatti persino in questa ipotesi teorica hai i servizi segreti a cui è permesso andare oltre le regole vigenti per le forze di polizia classiche e per i classici investigatori. Perciò, anche se inquadriamo correttamente il comportamento degli investigatori normali, ci sarebbero comunque altre persone che potrebbero utilizzare quelle tecnologie. Poi c'è il vero problema: se dobbiamo regolamentare l'acquisto e il possesso di quelle tecnologie oppure regolamentare il loro utilizzo.

Julian: Stiamo parlando dei kit per l'intercettazione di massa che possono intercettare mezzo paese o una città intera.

Jérémie: Sì. È come con le bombe atomiche: non puoi vendere facilmente un'arma nucleare. Qualche paese vorrebbe costruirne una ma ha dei problemi a farlo. Con gli armamenti, è la tecnologia che viene regolamentata, non l'uso che ne fai. Credo che il dibattito potrebbe vertere sul fatto che queste tecnologie debbano essere equiparate alle armi o no.

Jacob: Dipende. Quando sono armi, e non c'è alcun dubbio che le apparecchiature di sorveglianza diventino armi in posti come la Siria o la Libia, le usano specificamente per colpire direttamente le persone. L'azienda francese Amesys ha colpito certe persone nel Regno Unito usando apparecchiature francesi che sarebbe illegale utilizzare in Francia, e le hanno vendute scientemente.[5]

Andy: E non lo ammettono mai, vero?

Jacob: Mah, la Amesys è stata beccata in flagrante con i suoi documenti interni negli Spy Files.[6] Se vogliamo continuare a parlarne in termini di armamenti, dobbiamo ricordare che non è come vendere un camion a un paese. È come vendere a un paese un camion, un meccanico e una squadra che viaggia sul mezzo, seleziona le persone e poi gli spara.

JULIAN: È come vendere un intero esercito di camion.

ANDY: È interessante che la crittografia sia regolamentata. L'accordo di Wassenaar è valido a livello internazionale, che significa che non puoi esportare ai paesi dichiarati canaglia o, per qualsiasi motivo, problematici la tecnologia crittografica che aiuti a proteggersi contro la tecnologia della sorveglianza. Invece se tratti apparecchiature di sorveglianza *puoi* vendere la tecnologia a livello internazionale. Non ci sono limiti alla sua esportazione. Il motivo, credo, è semplicemente che persino i governi democratici hanno un certo interesse a controllare. E anche se tratti con governi canaglia a cui porti apparecchiature di sorveglianza per fare cose brutte ne trarrai qualche vantaggio perché imparerai che cosa stanno ascoltando, di cosa hanno paura, quali sono le persone più importanti del paese che si oppongono al governo, organizzano iniziative politiche eccetera. Così sarai in grado di prevedere gli eventi futuri, sponsorizzare azioni e così via. Stiamo parlando del gioco sporchissimo di cosa succede tra i paesi, ed è il vero motivo per cui i sistemi di sorveglianza non sono regolamentati.

JULIAN: Vorrei approfondire questa analogia tra sorveglianza di massa e armi di distruzione di massa. Era un dato di fatto della fisica che fosse possibile ottenere una bomba atomica, e quando è stata creata la bomba atomica la geopolitica è cambiata, ed è cambiata la vita per tante persone, in tante maniere diverse, alcune forse positive, altre al limite dell'apocalisse totale. Un movimento per la regolamentazione ha attuato dei controlli e finora questi controlli ci hanno salvato dal conflitto nucleare, a parte il Giappone. Però è facile capire quando armi di questo genere sono usate o meno.

Con l'aumento della sofisticazione e la riduzione del costo della sorveglianza di massa avvenuti negli ultimi dieci anni, siamo ora a uno stadio in cui la popolazione umana raddoppia ogni venticinque anni circa, ma la capacità di sorveglianza raddoppia ogni diciotto mesi. La curva della sorveglianza sta

stracciando la curva della popolazione. Non c'è una via diretta di fuga. Siamo giunti al punto in cui con dieci milioni di dollari ti compri un'unità che può stoccare in permanenza le intercettazioni di massa in un paese di medie dimensioni. Perciò mi domando se ci serve una reazione equivalente. È sul serio una grande minaccia alla democrazia e alla libertà in tutto il mondo, e dobbiamo reagire, proprio come quando la minaccia della guerra atomica necessitava di una reazione di massa, per cercare di controllarla finché ancora possiamo.

ANDY: In Libia ho visto che il movimento democratico ha fatto irruzione nelle stazioni di sorveglianza, ha sequestrato i registri, ha fornito le prove dell'appoggio delle imprese occidentali alla dittatura di Gheddafi nella repressione delle attività politiche, poi il nuovo governo ha preso possesso delle medesime strutture che ora sono tornate a operare di nuovo a pieno regime.[7] Così, anche se sono d'accordo sul fatto che sarebbe una buona idea controllare questa tecnologia, sono un tantino scettico sugli interessi dei cittadini contro gli interessi di chi ha il potere. Non lo chiamerei nemmeno per forza governo, perché chiunque sia in grado di ascoltare tutte le telefonate è in grado di fare certe cose. Riguarda anche le quotazioni di borsa, puoi trarre parecchi vantaggi economici se sai che aria tira.

JULIAN: Dove le nazioni hanno leggi specifiche sui teorici obiettivi delle principali agenzie di spionaggio elettronico, strutture come la NSA negli Stati Uniti, GCHQ (Government Communications Headquarters) nel Regno Unito, DSD (Defense Signals Directorate) in Australia, hanno cambiato le leggi in modo da inserire la raccolta delle informazioni economiche. Per esempio, se Australia e Stati Uniti stessero competendo per un contratto sul grano, spierebbero tutte le persone coinvolte nell'accordo. Succede da un bel po' di tempo, almeno da dieci anni è risaputo, però è automatico perché la gente lo fa comunque. È iniziato con i contratti sulle armi, in cui vedi aziende come Lockheed Martin, Raytheon e Northrup che strappano contratti per gli

armamenti e poi sono coinvolte nell'installazione dei sistemi di intercettazione di massa perché questi gruppi sono vicini alle cerchie clientelari. Ottengono favori dai loro amici e coprono le intercettazioni sui contratti per le armi con i dettami della sicurezza nazionale. Ma adesso vale per tutto ciò che potrebbe portare un vantaggio economico alla nazione, cioè quasi tutto.

JACOB: Un buon paragone evocato da certuni al Chaos Communication Congress nel dicembre 2011 è l'idea di equiparare le tecnologie della sorveglianza, in particolare la sorveglianza tattica ma anche quella strategica, alle mine antiuomo.[8] Credo che sia una cosa molto efficace. Solo perché è possibile non significa che è inevitabile proseguire lungo questa rotta, e non significa che dovremo andare sino in fondo, sino al punto in cui tutti sono monitorati.

Purtroppo ci scontriamo con ben precisi incentivi economici. Per esempio, qualcuno mi ha spiegato che il sistema telefonico norvegese aveva un contatore che poteva andare più veloce o più adagio a seconda di quanto lontano chiamavi. Però non era legale che l'azienda telefonica norvegese tenesse un registro dei metadati della chiamata che avevi fatto, come il numero composto, nello specifico per via di preoccupazioni sulla privacy risalenti alla seconda guerra mondiale. Perciò è possibile installare la medesima tecnologia in modo che sia rispettosa della privacy ma consenta ancora un approccio di mercato, che permetta ancora un guadagno economico. Comunque con le tecnologie GSM (telefonia mobile) non possiamo vincere. Al momento questi sistemi sono pensati, non solo in termini di fatturazione ma anche di architettura, in modo da non garantire una privacy della posizione e dei contenuti.

JULIAN: Un cellulare è un congegno di rintracciamento che fa anche telefonate.

JACOB: Esatto. Per esempio, se diciamo che tutti nel Terzo mondo sono spiati, che cosa significa realmente? Significa che i loro sistemi telefonici, che poi sono il loro contatto con il

resto del mondo, diventano strumenti spionistici quando qualcuno sceglie di usare i dati ottenuti in quel modo.

Andy: Ho visto che i paesi africani ricevono in regalo dai cinesi un’intera infrastruttura Internet, compresi cavi in fibre ottiche e backbone switch.

Jacob: Regalini della zte o qualcosa del genere?[9]

Andy: Sì, e ovviamente i cinesi sono interessati ai dati, perciò non hanno bisogno di essere ripagati in soldi, loro accettano i dati, la nuova moneta.

Jérémie: La sorveglianza finanziata dallo stato è davvero un grosso problema che mette alla prova la struttura stessa di tutte le democrazie e il loro funzionamento, ma abbiamo anche una sorveglianza privata e una potenziale raccolta di massa di dati privata. Basta guardare Google. Se sei un tipico utente, Google sa con chi stai comunicando, chi conosci, che cosa cerchi, in potenza il tuo orientamento sessuale e le tue credenze religiose e idee politiche.

Andy: Sa su di te più di quanto sappia tu stesso.

Jérémie: Più di tua madre e forse persino più di te. Google sa quando sei online o no.

Andy: Tu lo sai che cosa hai cercato due anni, tre giorni e quattro ore fa? Tu non lo sai, Google lo sa.

Jérémie: Io cerco di non usare più Google proprio per questo motivo.

Jacob: È una specie di Kill the Television del Duemila.[1] Una protesta efficace, a meno che l'effetto rete non impedisca alla tua protesta di funzionare.[2] Fai fuori il tuo televisore, amico.

Jérémie: Mah, non è una forma di protesta, è più la mia visione personale delle cose.

Andy: Ho visto fantastici filmati di persone che scagliavano il televisore dalla loro villetta a tre piani.

Jérémie: Non è solo la sorveglianza finanziata dallo stato, è il problema della privacy, come i dati sono gestiti da terzi e sapere che cosa ci fanno con i dati. Io non uso Facebook, perciò non ne so molto, ma ora con Facebook vedi come si comportano gli utenti, felicissimi di rilasciare ogni genere di dato personale. Puoi criticare la gente se non sa dov'è il limite tra privato e pubblico? Qualche anno fa, prima delle tecnologie digitali, quelli che avevano una vita in pubblico li trovavi nel mondo dello spettacolo, nella politica o nel giornalismo, invece adesso tutti possono avere una vita pubblica cliccando il pulsante "publish". "Publish" significa rendere pubblico qualcosa, significa concedere l'accesso a questi dati al resto del mondo, e naturalmente quando vedi adolescenti che inviano le proprie foto da sbronzi o simili forse non capiscono che significa inviarle a tutto il resto del pianeta potenzialmente per tanti, tanti anni. Facebook guadagna confondendo la separazione tra privato, amici e pubblico. E conserva i dati perfino quando sei convinto che siano intesi solo per i tuoi amici e quelli che ami. Così, quale che sia il livello di pubblicità a cui vuoi sottoporre i tuoi dati, quando clicchi publish su Facebook prima li dai a Facebook e soltanto dopo quelli consentiranno l'accesso a qualche altro utente Facebook.

Julian: Persino la separazione tra governo e impresa è poco chiara. Se guardiamo l'espansione del settore degli appalti militari in Occidente negli ultimi dieci anni, all'inizio la NSA, la più grande agenzia di spionaggio al mondo, aveva dieci fornitori principali nei propri registri. Due anni fa ne aveva oltre mille. Perciò il confine tra governo e settore privato si sta sfrangiando.

Jérémie: E possiamo aggiungere che le agenzie di spionaggio Usa hanno accesso a tutti i dati conservati da Google.

Julian: Lo fanno.

Jérémie: E a tutti i dati di Facebook, perciò Facebook e Google potrebbero essere estensioni di queste agenzie.

Julian: Jake, hai un'ordinanza di Google? È stata inviata un'ordinanza a Google perché cedesse informazioni relative al tuo account Google? WikiLeaks ha ricevuto ordinanze per la nostra società di registrazione del nome di dominio in California, dynadot, dove è stato registrato wikileaks.org. Provenivano dalle indagini segrete del gran giurì in corso su WikiLeaks e chiedevano i bilanci, i registri dei login eccetera, e gli sono stati dati.[3]

Jacob: Il "Wall Street Journal" ha segnalato che Twitter e Google e Sonic.net, tre servizi che uso o che ho usato, hanno ricevuto tutti quanti una notifica 2703(d), che è una forma insolita di ordinanza segreta.[4]

Julian: In base al Patriot Act?

Jacob: No, questo concerneva lo Stored Communications Act, in pratica. Il "Wall Street Journal" ha scritto che tutti questi servizi sostengono che il governo voleva i metadati, e il governo ha affermato di averne il diritto anche senza mandato. C'è una causa in corso sul diritto del governo a tenere segrete le sue tattiche, non solo al pubblico ma anche ai giudici. L'ho scoperto come tutti leggendo il "Wall Street Journal".

Julian: E così Google s'è piegata al governo Usa nelle indagini del gran giurì su WikiLeaks quando il governo ha chiesto i tuoi dati, non con un'ordinanza classica ma con questa forma speciale di ordinanza dei servizi segreti. Sempre nel 2011, era già arrivata la notizia che Twitter ha ricevuto una serie di ordinanze dallo stesso gran giurì, ma s'è mossa per poter avvertire i titolari degli account sottoposti a mandato, perché fosse tolta l'ordinanza di riservatezza. Non ho un account Twitter, perciò io non l'ho ricevuto, ma il mio nome e quello di Bradley Manning erano su tutte le ordinanze assieme alle informazioni che stavano cercando. Jake, tu avevi un account Twitter, perciò Twitter ha ricevuto un mandato che ti riguarda. Anche Google l'ha ricevuto, ma non ha tentato di renderlo pubblico.[5]

Jacob: A quanto pare. Così ho letto sul “Wall Street Journal”. Potrebbe anche non essere permesso citarlo se non in collegamento con il “Wall Street Journal”.

Julian: Ma perché queste ordinanze hanno una clausola bavaglio? È stato dichiarato incostituzionale, no?

Jacob: Forse no. Nel caso di Twitter è notorio che ci è stata respinta la mozione di rinvio in cui obiettavamo che rivelare questi dati al governo avrebbe recato danni irreparabili poiché una volta che li hanno ottenuti non potranno mai scordarseli. Praticamente hanno detto: “Bene, la vostra mozione è stata rigettata, Twitter deve rivelare questi dati”. Siamo in appello, in particolare riguardo alla riservatezza della registrazione della sentenza, e non ne potrei parlare, però, per dire come siamo messi, il tribunale ha spiegato che in Internet non puoi aspettarti la privacy quando rilasci spontaneamente informazioni a terzi. Tra l’altro in Internet tutti sono terzi.

Julian: Persino se una struttura come Twitter o Facebook sostiene che non divulgherà le informazioni.

Jacob: Certo. È qui che diventa sfumato il confine fra stato e imprese. Forse è la cosa più importante da tenere presente, cioè che la nsa e Google hanno una partnership nel campo della cibersicurezza per la difesa nazionale Usa.

Andy: Qualunque cosa significhi in questo contesto “cibersicurezza”. È un termine molto vago.

Jacob: Stanno cercando di escludere tutto dal Freedom of Information Act per tenere tutto quanto segreto. Inoltre il governo Usa sostiene di avere il diritto di inviare un mandato amministrativo, che ha una soglia più bassa del mandato di perquisizione. La terza parte non te ne può parlare e tu non hai il diritto di opporti perché è direttamente coinvolta una terza parte, la quale non ha nemmeno le basi costituzionali per proteggere i tuoi dati.

Julian: La terza parte sarebbe Twitter o Facebook o il tuo provider.

Jacob: O chiunque. Hanno detto che era una specie di mappa in scala uno a uno, che combaciava alla perfezione con la privacy bancaria e con l'uso del telefono. Tu riveli volontariamente il numero alla compagnia telefonica quando lo usi. Lo sapevi, no? Usando il telefono stai chiaramente dicendo: "Non mi aspetto di godere di privacy" quando componi quei numeri. Qui c'è persino un collegamento meno esplicito con la macchina. La gente non sa come funziona Internet, del resto non capisce nemmeno le reti telefoniche. Però i giudici hanno deciso unanimemente che è così, e finora nella nostra causa Twitter, di cui purtroppo non posso parlare perché non vivo in un paese davvero libero, sostengono in pratica la medesima cosa.[6]

È assolutamente folle pensare che stiamo cedendo tutti i nostri dati personali a queste imprese, che sono diventate in pratica tante polizie segrete private. E nel caso di Facebook abbiamo persino la sorveglianza democratizzata. Invece di pagare la gente come faceva la Stasi nella Germania Est, li ricompensiamo culturalmente, ora scopano. Riferiscono ai loro amici, "ehi, la tale sta con uno", "oh, la tale ha rotto", "ah, so chi chiamare adesso".

Andy: Certuni sono riusciti a costringere Facebook a cedere tutti i dati conservati su di loro in base alla legge europea sulla protezione dei dati, e l'ammontare minore di dati era 30 mega, il più grosso attorno agli 800.[7] La cosa interessante è che con questa legge è stata resa nota la struttura del database di Facebook. Ogni volta che fai login il numero IP e tutto il resto vengono conservati, ogni tuo clic, ogni volta, anche la quantità di volte che ti fermi su una pagina così possono capire se ti piace o no eccetera. In questo modo si è saputo che l'identificatore chiave della struttura del database era la parola "target". Non chiamano la gente "abbonati" o "utenti" o altro, li chiamano "target", al che si potrebbe dire "ho capito, è un termine del marketing".

Julian: Però era una cosa interna.

Andy: Sì, ma potrebbe essere un bersaglio anche in senso militare, o in senso spionistico. Perciò è solo questione delle circostanze in cui vengono usati i dati.

Julian: Certo. È la cosa spaventosa in questa faccenda.

Andy: Penso che sia molto utile. Con Facebook usavamo dire che l'utente non è in realtà il cliente. L'utente di Facebook è il prodotto, e il vero cliente sono le agenzie pubblicitarie. È la spiegazione meno paranoica e più innocua di quanto sta succedendo.

Però il problema è che non puoi criticare un'azienda perché si adegua alle leggi del paese. Lo definiscono normale, e definiscono reato se non si adeguano alle leggi del paese. Perciò è un tantino problematico dire: "Ehi, obbediscono alla legge". Che razza di accusa sarebbe?

Jacob: No, devo obiettare su una cosa. Se costruisci un sistema che registra tutto su una persona e sai di vivere in un paese con leggi che costringeranno il governo a cedere i dati, allora forse non dovresti costruire questo tipo di sistema. Ed è questa la differenza tra approccio privacy-grazie-alla-politica e privacy-grazie-al-progetto nella creazione dei sistemi sicuri. Quando stai cercando di prendere di mira le persone e sai di vivere in un paese che prende di mira esplicitamente le persone, allora se Facebook piazza i suoi server nella Libia di Gheddafi o nella Siria di Assad non cambia nulla. Eppure nessuna delle National Security Letters uscite, mi pare uno o due anni fa, era per terrorismo. Le 250.000 lettere sono state inviate per tutto, ma non per terrorismo.[8] Perciò se sai che è così, queste imprese hanno una grave responsabilità etica che nasce dal fatto che stanno costruendo questi sistemi e hanno fatto la scelta economica di vendere in pratica i propri utenti. E non è nemmeno una cosa tecnica. Non riguarda minimamente la tecnologia, è questione di economia. Hanno deciso che è più importante collaborare con lo stato e vendere i propri utenti e violare la

loro privacy e far parte di un sistema di controllo, essere ripagati perché partecipano a una cultura della sorveglianza, del controllo, piuttosto che opporsi a essa, quindi ne diventano parte. Sono complici e responsabili.

ANDY: In questo momento la responsabilità etica non ha un grande appeal promozionale, no?

Jérémie: A questo punto può sorgere la questione di quale può essere la soluzione sia per l'utente singolo che per la società nel suo complesso. Ci sono soluzioni tecniche, i servizi decentrati, dove tutti ospitano i propri dati, dati cifrati, dove tutti si affidano al server più vicino perché li aiuti con i servizi di cifratura dati e così via. E ci sono le possibilità politiche di cui abbiamo discusso. Non sono sicuro che a questo stadio, in questo periodo, siamo in grado di rispondere alla domanda se una delle due strategie è migliore. Credo che dovremmo svilupparle in parallelo. Dobbiamo avere un software libero che tutti possano capire, tutti possano modificare e tutti possano esaminare per essere sicuri di cosa fa. Io credo che il software libero sia una delle basi per una libera società online, per avere la possibilità di controllare sempre la macchina e non permettere che sia lei a controllare te. Dobbiamo avere una crittografia forte per essere sicuri che quando vuoi che i tuoi dati siano letti solo da te non li possa leggere nessun altro. Ci servono strumenti di comunicazione come Tor o come il Cryptophone per poter comunicare soltanto con la gente che vogliamo. Però il potere dello stato e quello di certe aziende può sempre superare quello di noi smanettoni e la nostra capacità di costruire e diffondere queste tecnologie. Potremmo avere anche bisogno, mentre costruiamo queste tecnologie, di leggi e strumenti che siano nelle mani dei cittadini per controllare ciò che si fa con la tecnologia, anche se non sempre in tempo reale, e punire chi usa quella tecnologia in un modo poco etico e che viola la privacy dei cittadini.

Julian: Vorrei soffermarmi su quella che mi sembra una differenza tra ottica cypherpunk Usa ed europea. Il Secondo emendamento sancisce il diritto a portare armi. Poco tempo fa ho visto un filmato girato da un amico negli Stati Uniti sul diritto di girare armati. Sopra un'armeria campeggiava un cartello che diceva: "Democrazia, con il colpo in canna". È così che ti assicuri di non avere un regime totalitario, la gente è armata e se è abbastanza incazzata allora imbraccia il fucile e si riprende il potere con la forza. Questa tesi è ancora valida oggi? È davvero una domanda interessante a causa della differenza nel tipo di armi intervenuta nell'ultimo trentennio. Possiamo anche tornare all'affermazione che la creazione di codici, fornire codici crittografici segreti che il governo non possa spiare, equivale in pratica al fornire munizioni. Abbiamo combattuto una guerra durissima negli anni novanta per cercare di mettere la crittografia alla portata di tutti, e nel complesso l'abbiamo vinta.[1]

Jacob: In Occidente.

Julian: In Occidente l'abbiamo complessivamente vinta tanto che la trovi in tutti i browser, anche se forse adesso ci sono delle backdoor ed è manipolata in tanti modi diversi.[2] Il discorso è che non puoi fidarti del fatto che un governo applichi le politiche che dice, e pertanto dobbiamo fornire gli strumenti impliciti, strumenti crittografici che noi controlliamo, una sorta di uso della forza nel senso che i codici reggeranno per quanto il governo provi con la forza a intrufolarsi direttamente nelle tue comunicazioni.

Jacob: La forza di quasi tutte le autorità moderne deriva dalla violenza o dalla minaccia di usare la violenza. Devi ammettere che con la crittografia nessuna violenza a nessun livello potrà mai risolvere un problema matematico.

Julian: Esatto.

Jacob: È questa la chiave. Non significa che non puoi essere torturato, non significa che non cercheranno di piazzarti delle

microspie in casa o di metterla a soqquadro in qualche modo, però significa che, se trovano un messaggio crittato, non conta nulla se hanno la forza dell'autorità dietro tutto quello che fanno, non potranno comunque risolvere quel problema matematico. Però questa è la cosa che risulta assolutamente ostica alla gente non del settore, e che deve essere ribadita. Se fosse possibile risolvere tutti quei problemi matematici sarebbe una faccenda diversa, e ovviamente anche il governo potrebbe risolverli.

JULIAN: Però è un dato di fatto: così come puoi costruire bombe atomiche, ci sono dei problemi matematici che puoi creare e che nemmeno lo stato più forte potrà risolvere. Credo che l'idea esercitasse un fascino immenso sui libertarian californiani e su altri che credevano in questa specie di "democrazia con il colpo in canna" perché era un modo molto intellettuale di farlo, un paio di individui armati di crittografia che si oppongono alla forza bruta della più grande potenza al mondo.

Così c'è una proprietà dell'universo che sta dalla parte della privacy, perché alcuni algoritmi crittografici sono impermeabili a qualsiasi governo, sempre. Ce ne sono altri che sappiamo essere estremamente duri da risolvere anche per la NSA. Lo sappiamo perché li raccomandano ai contractor dell'esercito americano per proteggere le comunicazioni militari top secret Usa, e se ci fosse stata una qualche backdoor i russi e i cinesi l'avrebbero trovata in un amen, con gravi conseguenze per chiunque avesse deciso di raccomandare un codice insicuro. Perciò oggi i codici sono piuttosto all'altezza, ne siamo abbastanza certi. Purtroppo non puoi essere affatto sicuro della macchina su cui girano, quindi è un problema. Però questo non porta alle intercettazioni di massa, porta all'individuazione dei computer di specifiche persone da usare come bersaglio. Se non sei un esperto della sicurezza è difficilissimo rendere sicuro un computer, però la crittografia può risolvere il problema dell'intercettazione di massa, ed è questo il problema, questo delle intercettazioni di massa, che minaccia

la civilizzazione globale. I bersagli individuali non sono la vera minaccia.

Nondimeno, penso che abbiamo a che fare con forze politiche ed economiche incredibilmente grosse, come diceva Jérémie, e l'esito probabile è che l'efficienza naturale delle tecnologie per la sorveglianza rispetto al numero di esseri umani significherà che pian piano finiremo con una società della sorveglianza totalitaria globale (per totalitaria intendo sorveglianza totale) e che forse ci saranno solo poche ultime persone libere, quelli che sapranno usare questa crittografia come difesa contro la sorveglianza completa, totale. Certe persone sono completamente fuori dal quadro, i neoluddisti che si sono rintanati nelle grotte, oppure le tribù che non dispongono di alcun vantaggio dell'economia moderna, e quindi la loro capacità di agire è minima. Naturalmente chiunque può rimanere fuori da Internet, ma poi difficilmente potrà esercitare una qualsivoglia influenza. Facendo così impedisce a se stesso di avere influenza. È uguale con il telefonino, puoi decidere di non averlo però riduci la tua possibilità di intervento. Non è un passo avanti.

JÉRÉMIE: Se guardiamo la faccenda nell'ottica di mercato, sono convinto che nella privacy ci siano possibilità di mercato finora perlopiù inesplorate, perciò forse ci sarà una spinta economica per le aziende a sviluppare strumenti che regalino agli utenti la capacità individuale di controllare i propri dati e comunicazioni. Forse è così che potremo risolvere questo problema. Non sono sicuro che questa cosa possa funzionare da sola, ma potrebbe succedere e noi potremmo anche non accorgercene.

JULIAN: La crittografia sarà dappertutto. Viene già utilizzata dalle principali organizzazioni di tutto il mondo, in una lenta avanzata verso le città-stato in rete. Se pensi alle autostrade delle comunicazioni su Internet, con i veloci flussi transnazionali di denaro, le organizzazioni transnazionali, le interconnessioni tra le sottocomponenti delle organizzazioni, tutti questi flussi di comunicazioni passano attraverso canali

specifici di cui non ci si può fidare. È come un organismo privo di pelle. Hai organizzazioni e stati che si mescolano, ogni rete di influenza mondiale lotta per ricavare un vantaggio, e i loro flussi di comunicazioni sono esposti agli opportunisti, agli stati concorrenti e così via. Così le nuove reti, reti private virtuali, vengono costruite in cima a Internet e la loro privacy è garantita dalla crittografia. È una base di potere industriale che sta impedendo la messa al bando della crittografia.

Se per esempio esamini il telefono BlackBerry, ha un sistema di cifratura interno da usare entro la rete BlackBerry. Research in Motion, l'azienda canadese che lo gestisce, può decrittare il traffico degli utenti regolari con i suoi centri dati in Canada e nel Regno Unito, come minimo, perciò l'alleanza spionistica angloamericana può arrivare fino alle comunicazioni mondiali da un BlackBerry all'altro. Comunque le grandi imprese lo stanno usando in maniera più sicura. Ai governi occidentali questo è andato bene fino a quando non ha iniziato a diffondersi oltre le multinazionali, agli individui, e a quel punto abbiamo riscontrato le medesime reazioni ostili della politica viste nell'Egitto di Mubarak.[3]

Credo che l'unica difesa efficace contro la prossima distopia della sorveglianza sia prendere delle contromisure per salvaguardare la nostra privacy perché non c'è alcun incentivo ad autolimitarsi per le persone che hanno la possibilità di intercettare tutto. Potremmo fare un paragone storico con quando la gente ha imparato che doveva lavarsi le mani. Ci voleva la conferma della teoria batterica delle malattie e poi la sua volgarizzazione, e che fosse inculcata la paura della diffusione del morbo per mezzo di roba invisibile sulle tue mani, proprio come non puoi vedere l'intercettazione di massa. Una volta che si è arrivati a una comprensione sufficiente, i fabbricanti di sapone hanno sfornato prodotti che la gente consumava per placare la paura. È necessario inculcare la paura nella gente perché capisca il problema e crei abbastanza domanda di una soluzione.

C'è un problema anche dal lato opposto dell'equazione,

cioè che i programmi che sostengono di essere sicuri, di avere la crittografia inserita, spesso sono una truffa perché la crittografia è complessa e la truffa può annidarsi nella complessità.[4]

Perciò la gente dovrà pensarci. L'unica domanda è in quale dei due modi ci penserà. O penseranno "devo stare attento a quel che dico, devo conformarmi" per tutto il tempo, in qualsiasi interazione. Oppure penseranno "devo dominare piccole componenti di questa tecnologia e installare cose che mi proteggono per essere in grado di esprimere i miei pensieri liberamente e comunicare liberamente con gli amici e le persone che mi interessano". Se la gente non sceglie questa seconda opzione allora avremo il politically correct universale perché persino quando le persone comunicheranno con gli amici più intimi si autocensureranno e si priveranno del ruolo di persone politicamente attive nel mondo.

Jérémie: È interessante vedere il potere che hanno gli hacker, “hacker” nel senso originario del termine, non nel senso di criminale. Un hacker è un appassionato di tecnologia, uno a cui piace capire come funziona, che non vuole restare prigioniero della tecnologia ma farla funzionare meglio. Immagino che quando avevate cinque o sette anni abbiate cercato di aprire le macchinette con il cacciavite per vedere com’erano dentro. Un hacker è questo, e gli hacker hanno costruito Internet per tanti motivi, compreso perché era divertente, e l’hanno sviluppata e hanno regalato Internet a tutti gli altri. Poi aziende come Google e Facebook hanno colto la palla al balzo per costruire modelli commerciali basati sulla cattura dei dati personali degli utenti. Eppure vediamo che c’è ancora una forma di potere nelle mani degli hacker. Il mio principale interesse in questi giorni è far sì che questi hacker acquisiscano potere persino nelle arene politiche. Negli Stati Uniti ci sono state le leggi SOPA (Stop Online Piracy Act) e PIPA (Protect IP Act), duri provvedimenti a difesa del copyright che in pratica regalano a Hollywood il potere di ordinare a qualsiasi impresa Internet di limitare l’accesso e di esercitare la censura.[1]

Julian: E il blocco dei conti correnti come quello che sta subendo WikiLeaks.[2]

Jérémie: Esatto. Quello che hanno fatto le banche a WikiLeaks stava diventando il metodo standard per combattere i cattivi pirati del copyright che hanno ucciso Hollywood eccetera. Siamo allora stati testimoni della

mostruosa insurrezione della società civile in Internet, e non solo negli Stati Uniti: non avrebbe funzionato se fossero stati solo i cittadini Usa a insorgere contro SOPA e PIPA. Ha partecipato gente da tutto il mondo, e il cuore della rivolta sono stati gli hacker che hanno fornito agli altri gli strumenti per partecipare al dibattito pubblico.

JULIAN: Per aiutare a montare la campagna.

JÉRÉMIE: Come in Tumblr o in qualche sito del genere, dove la homepage ti chiede di inserire il tuo numero di telefono, così poi ti richiamano e sei in contatto con il Congresso. A quel punto inizi a parlare con qualcuno per dirgli che è una porcheria.

JACOB: Internet è stata utilizzata in sua propria difesa.

JÉRÉMIE: Secondo me, noi hacker siamo responsabili degli strumenti che creiamo e diamo al resto del mondo, e forse stiamo assistendo all'inizio del funzionamento efficiente di questa responsabilità quando la usiamo collettivamente. Attualmente nell'Unione europea siamo in pieno dibattito sull'ACTA (Anti-Counterfeiting Trade Agreement), un trattato multinazionale che è stato il modello per SOPA e PIPA.[3] Sono appena tornato dal Parlamento europeo dove noi, come semplici individui, individui barbuti e puzzolenti, stavamo dando indicazioni a una commissione parlamentare. Gli stavamo indicando certi articoli del regolamento procedurale del Parlamento europeo che a quanto pareva quelli stavano cercando per la prima volta e gli dicevamo come comportarsi, poi c'è stata una votazione che abbiamo vinto 21 a 5 e ha messo all'angolo il relatore britannico. È una minima parte di un minimo punto procedurale sulla strada per sconfiggere l'ACTA, questo mostruoso accordo globale progettato alle nostre spalle per aggirare la democrazia stessa. Però forse noi come cittadini saremo in grado di uccidere il mostro, e facilmente, con gli strumenti Internet, le mailing list, i wiki, le chat room IRC eccetera, e credo che forse stiamo assistendo all'approdo alla maturità, all'adolescenza di Internet e a come

può essere usata dalla società intera per cercare di cambiare le cose. Credo sia di immensa importanza che noi hacker ci facciamo trovare qui con la nostra competenza tecnica per guidare la gente e dirle: “Dovreste usare questa tecnologia che consente il controllo della vostra privacy, invece di Facebook o Google” e che le due cose si articolino abbastanza bene, o possano articolarsi abbastanza bene. C’è un barlume di ottimismo.

Julian: Jake, sempre a proposito di questa radicalizzazione della gioventù di Internet, soprattutto negli ultimi due anni tu hai girato il mondo per parlare di Tor, per parlare a quelli che vogliono l’anonimato, che vogliono la privacy nel loro rapporto con il governo, e devi avere notato questo fenomeno in tanti paesi diversi. È una cosa significativa?

Jacob: Certo. Credo sia assolutamente significativa. L’esempio canonico che mi viene subito in mente è la Tunisia. Sono stato in Tunisia dopo la caduta del regime di Ben Alì e abbiamo discusso di Tor in un corso di informatica seguito da persone molto competenti dell’università. Una ragazza ha alzato la mano e ha chiesto: “E per quanto riguarda i cattivi?”. Poi ha elencato i Quattro Cavalieri dell’Infocalisse, riciclaggio, droghe, terrorismo e pornografia infantile. “E i cattivi?” Queste quattro menate saltano sempre fuori e sono usate insieme per affondare le tecnologie che difendono la privacy perché è ovvio che dobbiamo sconfiggere questi quattro pericoli. Così ho chiesto alla classe: “Chi di voi ha visto la pagina Ammar 404?”, che sarebbe la schermata di censura usata dal regime di Ben Alì prima e durante la rivoluzione per impedire l’accesso ai siti. Ogni singola persona nell’aula, a parte quella che aveva posto la domanda, ma compreso il docente, ha alzato la mano. Poi, rivolto alla ragazza della domanda, ho detto: “Guardi le persone che ha attorno. Sono i suoi compagni di corso. Crede sul serio che valga la pena di reprimere ogni persona in questa stanza per combattere quelle cose?”. E lei: “In realtà anch’io sto alzando la mano”.

È stato un po’ più stiracchiato di così, ma essenzialmente la gente che se lo vede contestualizzare capisce come stanno le cose. Cambia radicalmente le carte in tavola. E succede in tutto il mondo, tutti i giorni, però di solito dopo, cioè la gente capisce con il senno di poi che avrebbe potuto usare la tecnologia, capisce che “oh, sì, è vero, non sono solo i cattivi, in realtà anch’io divento un cattivo se dico come la penso su qualcosa e a un potente non piace quel che dico”. E ti accorgi che si svegliano.

Però è sbagliato dire che succede solo da un paio d’anni. Julian, mi dispiace farti questo, ma tu hai contribuito alla radicalizzazione della mia generazione. Io sono un cypherpunk di terza generazione, se proprio dovessi contarle. Il lavoro che tu e Ralf Weinmann avete fatto sul sistema Rubberhose mi ha spinto in parte a lavorare sui crittosistemi. Il crypto file system che ho progettato, il M.A.I.D., l’ho creato come reazione a cose come i poteri di indagine restrittivi nel Regno Unito, dove in pratica lo stato ha deciso che sono le regole restrittive la soluzione alla crittografia, dove ti possono prendere la password.[4] Certo, nel caso di Julian l’hanno creato perché i regimi repressivi torturano la gente per una passphrase, così dovevi essere in grado di dare più di una passphrase per adattarti alla loro tortura. Il mio sistema M.A.I.D. è stato progettato per un sistema giudiziario in cui l’accusato ha il diritto di rimanere in silenzio ma possa dimostrare, se costretto, che sta dicendo la verità senza violare la riservatezza. Avevo capito vedendo il lavoro di Julian che puoi usare la tecnologia per aiutare la gente comune a cambiare il mondo. Se risaliamo molto, molto indietro alla vecchia mailing list Cypherpunk con Tim May, uno dei suoi fondatori, e leggiamo i vecchi post di Julian sulla list Cypherpunk, dico che è stato proprio questo a spingere un’intera generazione a diventare davvero più radicalizzata perché tanta gente ha capito che non era più isolata, che poteva dedicare un po’ di tempo a scrivere un software che rafforzasse milioni di persone.[5]

Ci sono alcune conseguenze impreviste nel modo in cui la cosa s’è sviluppata, perché la gente che ha creato Google non

è partita per creare Google, la massima macchina di sorveglianza mai esistita. Però in pratica è stato creato questo, e appena la gente inizierà a capirlo quelli inizieranno a spedire le lettere della National Security. Giusto?

Jérémie: Mi pare che ci siano tre punti fondamentali in quello che hai appena detto.

Jacob: Solo tre?

Jérémie: Tra i tanti.

Andy: Allora lasciatemi aggiungere un quarto, se vi va.

Jacob: Ma se non sai ancora quali sono.

Jérémie: Vedo tre punti intrecciati. Non sto dicendo che andrebbero affrontati separatamente, ma uno sono i regimi autoritari e i poteri dei regimi autoritari nell'era delle tecnologie digitali. Nel caso del regime di Ben Alì, ed è evidente in tanti regimi odierni, puoi decidere che cosa la gente può imparare o con chi può comunicare. È un potere tremendo a cui bisognerebbe opporsi. Un altro punto è la costruzione di migliori strumenti e di una tecnologia migliore, una tecnologia che possa tentare di aggirare problemi come la censura, comunque in pratica la costruzione di strumenti che entrino in quell'infrastruttura e che aiutino a rovesciare i dittatori. E un altro problema ancora è la favoletta politica che hai appena citato, quella dei Quattro Cavalieri dell'Infocalisse, i pretesti che usano ogni giorno i politici attraverso i media. "Moriremo tutti a causa del terrorismo? Allora ci serve un Patriot Act." "I pedofili e la pornografia infantile sono ovunque." "Internet pullula di pedo-nazi, perciò ci serve la censura."

Jacob: Pedo-nazi?

Jérémie: Sì, pedo-nazi. Pedo-nazi.com è già assegnato. "Gli artisti moriranno e non ci sarà più il cinema, perciò dobbiamo

regalare a Hollywood il potere di censurare Internet" eccetera. Ripeto, penso che Internet sia uno strumento, un antidoto contro la favoletta politica, che si basa sull'emotività e su un tempo d'attenzione dei media che è estremamente corto, l'informazione appare per scomparire ventiquattr'ore dopo, sostituita da una nuova notizia. Con Internet ho la sensazione che stiamo creando quello che chiamo il tempo di Internet. Visto che la grande Internet non dimentica mai, possiamo accumulare negli anni dei dossier, giorno dopo giorno, e possiamo elaborare, analizzare. È quello che facciamo da tre anni con l'ACTA. Ancora una volta WikiLeaks è stato per noi una fonte di ispirazione perché la prima versione dell'ACTA che è filtrata è stata soffiata a WikiLeaks nel 2008.[6]

JULIAN: Sì, l'abbiamo raccolta noi.

JÉRÉMIE: Anche noi abbiamo fatto filtrare due versioni. Ci sono cinque versioni del testo in tre anni che potremmo prendere per dire paragrafo dopo paragrafo, riga su riga, che il tale sta facendo questo, che questa è l'industria che chiede la tal cosa, e poi coinvolgere esperti legali e di tecnologia per elaborare una versione della favoletta politica diversa da quella ufficiale, "oh, ci serve l'ACTA per salvare la cultura e salvare i bambini dai farmaci taroccati" e compagnia bella. E così abbiamo elaborato la nostra linea politica con il tempo di Internet, con analisi precise, con il duro lavoro, connettendo le persone perché partecipassero.

JULIAN: È vero, e credo che questa immagine di ACTA sia riuscita a convincere l'opinione pubblica.

JÉRÉMIE: Fin qui tutto bene.

JULIAN: Penso che sarà così che passerà alla storia, ma dietro le quinte, questo cosiddetto accordo commerciale anticontraffazione, che è nato dall'industria del copyright Usa ed è stato usato in realtà in un bel numero di trattati bilaterali per cercare di creare un nuovo regime

internazionale su ciò che è legale e non è legale per quanto riguarda le pubblicazioni, e decidere quali meccanismi possono impedire alla gente di pubblicare varie cose. Normalizza una versione più dura del sistema americano DMCA (il Digital Millennium Copyright Act) in base al quale se mandi una lettera a qualcuno chiedendo che tolga qualcosa da Internet quello deve toglierlo, e c'è una specie di procedura di due settimane in cui quello può presentare obiezioni eccetera ma essendo costoso per ogni editore ISP presentare queste controtesi lo tolgono immediatamente e lasciano che sia l'autore o colui che ha caricato a provare a sbrigarsela da solo. Le ricadute sono state abbastanza gravi negli Stati Uniti, dato che ha eliminato un bel po' di contenuti. Scientology ne ha abusato per far rimuovere letteralmente migliaia di video da YouTube.[7]

Allora, diamo per scontato che l'ACTA sia stato respinto nel Parlamento europeo, effettivamente, almeno in questa occasione. Eppure le principali ricadute dell'ACTA sembrano palesarsi comunque: abbiamo avuto il dibattito democratico, la legge ACTA è stata demonizzata nella sfera pubblica, abbiamo vinto nella versione ufficiale, però dietro le quinte si sono svolte trattative bilaterali segrete che stanno ottenendo il medesimo risultato, sovvertendo il processo democratico. Per esempio, WikiLeaks s'è impossessata del nuovo accordo sul libero scambio fra Unione europea e India, in cui sono inseriti grossi pezzi dell'ACTA, e l'ha pubblicato.[8] È successo con tanti altri accordi e leggi. Possiamo anche tagliare la testa all'ACTA ma il corpo si scinderà in più pezzi che si insinueranno tutti quanti nelle cose, nell'ordinamento internazionale sotto forma di tutti questi trattati bilaterali. Puoi anche strappare le tue vittorie democratiche che avverranno in pubblico, sulla superficie, ma sotto sotto quelle cose sono fatte ancora comunque. Questo solo per dimostrare che non credo che la via giusta sia una riforma politica o legislativa, anche se non puoi lasciare campo libero all'avversario perché poi lui se ne approfitterà. Così è importante tenerli sotto controllo in tanti modi, come con l'ACTA. Li rallenta. Ma perfino una vittoria in parlamento su

una legge non ferma questa attività sotterranea.

Jacob: Una cosa che penso andrebbe sottolineata è che Roger Dingledine, uno dei creatori di Tor, una specie di mio mentore che mi ha dato davvero tanto da pensare su come aggirare la censura e sull'anonimato online, sostiene, per esempio, che i firewall non sono solo utili tecnicamente (ed è importante comprendere la tecnologia sottostante se vuoi costruire una tecnologia che gli resista) ma anche socialmente. La gente che lotta contro l'ACTA sta usando la tecnologia, e questa le permette di resistere, però in realtà qui è importante comprendere la capacità di agire della gente comune, e le tecnociance, il gergo tecnico, non sono la cosa importante. Quel che conta è che la gente sia realmente coinvolta in questa narrazione e la cambi finché ha ancora il potere di farlo. In realtà è l'aspetto umano la parte più importante. WikiLeaks ha diffuso documenti che permettono ciò, e la condivisione di informazioni è importante, ma conta anche la gente che prende questa fondamentale informazione e la trasferisce. Perché c'è almeno qualche possibilità che molti di noi vivano in una democrazia, che siamo liberi, cioè che siamo governati in teoria attraverso il consenso. E quindi se tutti capiscono cosa succede e scopriamo che è una faccenda che non ha il nostro consenso, allora è molto difficile continuare così e farle passare come leggi senza il consenso dei governati.

Jérémie: Significa aumentare il costo politico delle decisioni sbagliate per coloro che le prendono, e possiamo farlo collettivamente con un'Internet libera finché l'abbiamo in mano nostra.

Jacob: Però potresti riuscirci anche senza Internet, perché in passato ci sono state società libere pre-Internet, era solo più costoso dal punto di vista economico, sotto certi aspetti più difficile, e in effetti è per questo che è tanto importante il movimento peer-to-peer.[9]

Andy: Il quarto punto è, secondo me, che la dimensione

architettonica dei sistemi decentrati è una cosa cruciale che deve anch'essa essere posta nelle mani della gente perché adesso abbiamo questo cloud computing centralizzato.[10]

JULIAN: Facebook è totalmente centralizzato. Twitter è totalmente centralizzato. Google pure. Tutti sono negli Stati Uniti, tutti controllabili da chiunque sia a detenere la forza coercitiva. Proprio come la censura avviata dopo che WikiLeaks ha diffuso i documenti Cablegate, quando Amazon ha eliminato il nostro sito dai suoi server.[11]

ANDY: E abbiamo il cloud computing che fornisce un incentivo economico alle aziende grazie a una modalità meno costosa di elaborare i propri dati nei cosiddetti centri dati internazionali gestiti dalle multinazionali Usa, che significa portare i dati sotto giurisdizione americana, come le strutture per i pagamenti eccetera.

JULIAN: C'è una tendenza abbastanza preoccupante in questo passaggio al cloud computing. Tengono enormi cluster di server tutti in un posto perché è più efficiente standardizzare il controllo dell'ambiente, standardizzare il sistema di pagamento. È una tecnica concorrenziale perché ammassare i server in una sola postazione costa meno che tenerli sparpagliati. Gran parte della comunicazione in Internet, a parte lo streaming dei film, avviene da un server all'altro, così se li piazzi vicini costa meno. Finiamo con l'avere questi grossi formicai di server comunicanti. Per Google ha senso, per esempio, piazzare i server presso i grandi fornitori di contenuti, o l'inverso, perché le pagine sono indicizzate da Google in modo da essere analizzabili. Quindi vediamo enormi edifici negli Stati Uniti stipati di server di tante aziende diverse. È qui che la NSA piazza alcuni dei suoi punti di raccolta per l'intercettazione di massa. Internet potrebbe esistere senza questa centralizzazione, la tecnologia non è impossibile, solo che è banalmente più efficiente averla centralizzata. Nella contesa economica vince la versione centralizzata.

ANDY: Anche se è molto importante capire l'ottica architettonica (le infrastrutture centrali rendono molto facile il controllo dal centro e l'abuso di potere), è un po' come far fallire il supermercatino sotto casa aprendo un centro commerciale.

JULIAN: E dover andare da una grossa, grossissima multinazionale come Safeway.

ANDY: Sì, proprio come è successo con i negozi. È molto importante mantenere un'ottica infrastrutturale decentrata. Quando facevo parte dell'ICANN, Internet Corporation for Assigned Names and Numbers, l'ente che assegna e regolamenta i nomi dei domini in Internet, ho imparato tante cose da Vince Cerf, il signore che ha inventato almeno una parte del protocollo TCP/IP, il fondamentale protocollo per comunicare in Internet. Diceva sempre: "Sai, una cosa positiva dei governi è che non sono mai al singolare, sono sempre al plurale". Così anche nei governi ci sono quelli che preferiscono avere una propria sfera decentrata di potere, e perfino lì ci sono diverse fazioni in lotta tra di loro. Sarà questo che alla fine ci salverà dal Grande Fratello, perché saranno in troppi a voler essere il Grande Fratello e a combattersi.

JULIAN: Io la vedo in maniera diversa, Andy. Io credo che un tempo avevamo delle élite nazionali in forte competizione tra di loro, mentre adesso si stanno coalizzando e stanno spossessando le rispettive popolazioni.

ANDY: Si stanno unendo, in questo hai ragione, e non sono tanto sicuro che ci salverà la pelle, però c'è la possibilità di mantenere la nostra identità. Dobbiamo tenerci aggrappati alla nostra infrastruttura, è la cosa importante da capire adesso, che se vogliamo opporci allo stato della sorveglianza, al Grande Fratello unico, dobbiamo studiare che cos'è, se è davvero un'unione di stati centrali che dicono "ehi, se ci mettiamo insieme possiamo guadagnare ancora di più". E dobbiamo capire qual è il nostro ruolo, ed è restare

decentrati, avere la nostra infrastruttura, non basarci sul cloud computing e altre stronzate, ma avere una cosa nostra.

Julian: Però potremmo ritrovarci con un dominio della tecnica. È un dato di fatto che è più facile usare Twitter che fondare un tuo Twitter, è un dato di fatto che è più facile usare Facebook che diaspora o qualche sua alternativa, è un dato di fatto che il cloud computing costa meno, pertanto queste tecniche e servizi domineranno.[12] Non si tratta di affermare che dovremmo fondare i nostri servizi locali, perché questi servizi locali non saranno banalmente concorrenziali e saranno sempre utilizzati da una ristretta minoranza di persone. Ci serve qualcosa di meglio rispetto a dire che dovremmo avere la versione povera di Facebook e aspettarci che la gente la usi.

Andy: Be', per tornare alla chiesa cattolica, stiamo ritornando ai giorni in cui c'era un solo grande distributore di libri dato che Amazon sta cercando di controllare l'intera catena di distribuzione degli e-book, perciò dobbiamo avere le nostre strutture di pubblicazione/stampa. Potrebbe sembrare un tantino esagerato, ma abbiamo visto cosa possono fare queste aziende se loro o gli enti governativi da cui dipendono come giurisdizione non vogliono che succedano certe cose. E credo che il prossimo passo sarà ovviamente che avremo bisogno dei nostri soldi, così anche se a loro non piace che sosteniamo progetti come WikiLeaks o simili avremo la nostra maniera di farlo senza doverci basare su un'infrastruttura centrale che passa tutta sotto una sola giurisdizione.

Jérémie: Vorrei dichiararmi d'accordo con Andy. Credo che l'architettura conti e che sia cruciale per tutto ciò a cui teniamo. Però è nostro dovere far arrivare questo messaggio al pubblico, perché noi lo capiamo bene, come hacker, come tecnici che costruiscono Internet tutti i giorni e ci giocano. E forse ci permetterà di conquistare i cuori e le menti delle generazioni più giovani. Credo sia per questo che sono così essenziali le leggi sul diritto d'autore, perché con le

tecnologie peer-to-peer, dopo Napster nel 1999, la gente ha capito, ha afferrato che condividendo file tra singoli…

Julian: Sei proprio un criminale.

Jérémie: No, davvero, ci puoi costruire una cultura migliore.

Julian: No, sei un criminale.

Jérémie: È la versione corrente, ma se costruisci una cultura migliore per te tutti useranno Napster.[13]

Andy: La storia della specie umana e la storia della cultura sono la storia dei pensieri copiati, modificati ed elaborati ulteriormente, e se lo definisci furto allora sei come tutti i cinici.

Jérémie: Esatto, esatto! La cultura è fatta per essere condivisa.

Julian: Be', in Occidente abbiamo una cultura industriale sin dagli anni cinquanta. La nostra cultura è diventata un prodotto dell'industria.

Jérémie: Stiamo solo nutrendo il mostro qui presente, che si diverte a recitare la parte dell'avvocato del diavolo e lo fa alla grande.

Jacob: Non passa. Sono scemenze talmente palesi.

Jérémie: Sono scemenze. Nella favoletta politica lo definiscono furto, ma vorrei ricordare che tutti quelli che usavano Napster nel 1999 sono diventati appassionati di musica e poi sono andati ai concerti e sono diventati strumenti di propaganda che raccontavano in giro "devi ascoltare quelli, dovresti andare a quel concerto" e così via. In questo modo la gente ha potuto vedere l'esempio pratico del modo in cui la tecnologia peer-to-peer decentralizzava l'architettura. In realtà Napster era un tantino centralizzato all'epoca, ma ha seminato l'idea dell'architettura decentrata.

Tutti vedevano un esempio concreto di come un'architettura decentrata faceva del bene alla società, e quando si parla di cultura condivisa è esattamente lo stesso di quando si parla di conoscenza condivisa. La condivisione della conoscenza è ciò di cui parliamo quando discutiamo su come aggirare la censura o fare a pezzi la favola politica per costruire un sistema democratico migliore e rendere migliore la società.

Così abbiamo degli esempi in cui i servizi decentrati e la condivisione tra individui migliorano le cose, e il controesempio è l'avvocato del diavolo che sta interpretando Julian, quando un dato settore salta su a dire: "Oh, ma questo è un furto e sta facendo fuori tutti, ammazza gli attori, ammazza Hollywood, ammazza il cinema, ammazza i gattini eccetera". Hanno vinto delle battaglie in passato, ma adesso forse noi stiamo per vincere la battaglia sull'ACTA. E ancora una volta mi devo dichiarare in disaccordo con l'avvocato del diavolo che recitava poco fa Julian. L'ACTA è stato finora il più grande esempio di aggiramento della democrazia, di presa in giro del parlamento e delle istituzioni internazionali, dell'opinione pubblica, e di come si fa a imporre di soppiatto misure inaccettabili. Se riusciamo a farlo fuori allora avremo stabilito un precedente, allora avremo l'occasione buona per proporre un'agenda positiva, per dire "l'ACTA è acqua passata, adesso passiamo a fare qualcosa che sia davvero a favore del pubblico". Stiamo lavorando per questo, e alcuni membri del Parlamento europeo ora capiscono che quando gli individui condividono le cose, quando condividono i file senza trarne profitto, non dovrebbero andare in galera, non dovrebbero essere puniti. Credo che se riusciremo in questo avremo robuste basi per dimostrare al resto del mondo che la condivisione della conoscenza, la condivisione dell'informazione migliorano le cose, che dobbiamo favorirle e non combatterle, e che qualsiasi tentativo, che sia legislativo o di un dittatore o di un'azienda, di minare la nostra capacità di condividere informazioni e conoscenza in modo decentrato va combattuto, punto e basta. Credo che potremmo imporre una tendenza.

Julian: E il dibattito PIPA/SOPA negli Stati Uniti? Sono due nuove leggi proposte al Congresso di Washington per imporre un embargo finanziario e di Internet per conto delle industrie americane.

Jacob: Sono state pensate espressamente per attaccare WikiLeaks e tutto quanto abbia rapporti con WikiLeaks o somigli a WikiLeaks.

Julian: Al Congresso il blocco bancario contro di noi è stato citato specificamente in quanto strumento efficace.[14]

Jérémie: E vogliono regalare questo strumento a Hollywood.

Julian: Così è nata una grande campagna comunitaria contro queste leggi e alla fine ci si sono uniti anche Google e Wikipedia e un gruppo d'altre aziende. Però non è stata una cosa della serie "bene, fantastico, abbiamo vinto questa battaglia". A me sono venuti i sudori freddi perché di colpo Google ha iniziato a considerarsi un protagonista politico e non solo un distributore, e adesso sentiva di avere un potere tremendo, enorme sul Congresso.

Jérémie: Google è stato solo un pezzetto della coalizione anti-PIPA/SOPA.

Jacob: Un attimo, mi pare che Tumblr abbia avuto più peso di Google.

Andy: Tumblr e Wikipedia e vagonate di singole iniziative, azioni minuscole di cui forse non avete mai sentito parlare, tutto s'è fatto sentire. Sono stati in migliaia ad agire in parallelo, nel senso che andavano nella medesima direzione, ed è stata, lo ripeto, un'iniziativa politica decentrata. Siamo stati testimoni di un movimento politico decentrato. Forse Google è stato solo il protagonista che è spiccato sugli altri.

Julian: Be', il Congresso ha affermato di essersene accorto.

Jacob: Io sono un tantino in disaccordo con quanto ha detto

Jérémie poco fa perché tu in pratica incoraggi l'idea di avanguardia politica. Non credo che intendessi questo, e volevo fermarti a questo punto perché il movimento peer-to-peer è esplicitamente contrario alle avanguardie politiche. È l'idea che siamo tutti pari, peer, e possiamo condividere tra di noi, possiamo fornire diversi servizi e diverse funzionalità. Un giorno Ross Anderson mi ha detto "quando sono entrato nel movimento peer-to-peer cinquant'anni fa", e già questo m'è sembrato un inizio fantastico, poi ha spiegato che voleva essere sicuro che non disinventassimo la stampa perché quando cominciamo a centralizzare i servizi, quando cominciamo a centralizzare i sistemi di controllo dell'informazione, in realtà iniziamo a disinventare la stampa nel senso che l'*Encyclopædia Britannica* non stampa più libri ma cd. Se non possiedi un computer classico che legge quei cd non hai accesso a quel sapere. Be', nel caso dell'*Encyclopædia Britannica* non importa dato che abbiamo Wikipedia e un sacco di altra roba. Ma non credo che come società siamo pronti.

Andy: Non sono tanto sicuro che Wikipedia sia così valida come risorsa, al confronto. Non mi fido di una sola pagina che non ho riscritto io.

Jacob: Però l'*Encyclopædia Britannica* non è diversa. È solo una risorsa fra tante, e quello che conta è la verifica dei dati. Voglio solo dire che non dovremmo promuovere questa idea di un'avanguardia perché è molto pericolosa.

Julian: Un attimo. Perché? Io sono un po' un'avanguardia. Che problema c'è?

Jérémie: Io non voglio parlare di avanguardie, sto solo dicendo che abbiamo nuovi strumenti in mano. Stavamo citando la stampa. Un altro visionario, il mio amico Benjamin Bayart, forse poco noto nel mondo non francofono, ha detto: "La stampa ha insegnato alla gente a leggere, Internet ha insegnato alla gente a scrivere".[15] È una cosa molto nuova, una nuova possibilità per tutti di scrivere ed esprimersi.

Andy: Sì, ma oggigiorno diventa ancor più importante filtrare.

Jérémie: Certo, perché tutti parlano e molti dicono scemenze. Come possono confermarti l'accademico e attivista Larry Lessig e, credo, tanti altri docenti, noi insegniamo a scrivere alla gente ma quando gli studenti ti consegnano le loro tesine il novantanove e rotti percento sono merda. Comunque gli insegniamo a scrivere.[16] E naturalmente la gente dice scemenze in Internet, è ovvio. Però essere in grado di usare questa modalità di esprimersi in pubblico ti rende nel tempo sempre più strutturato nel modo di parlare, sempre più capace di partecipare a discussioni complesse. E tutti i fenomeni che stiamo descrivendo sono costruiti attorno alla complessità progettata, che dobbiamo suddividere in piccole parti per poter capire e dibattere con calma. Non è questione di avanguardie politiche, è questione di incanalare nel sistema politico questa nuova capacità di esprimerci che abbiamo tutti per le mani, condividere i pensieri, partecipare alla condivisione della conoscenza senza essere membri di un partito politico, di una struttura mediatica o di qualsiasi struttura centralizzata di cui avevi bisogno in passato per poterti esprimere.

Julian: Vorrei riflettere su tre libertà di base. Quando ho intervistato il capo di Hezbollah, Hassan Nasrallah…

Jacob: Dov’è il drone del cazzo? Cos’è quella roba in cielo?

Julian: Be’, era in un certo senso anche lui agli arresti domiciliari perché non può lasciare la sua località segreta.

Jacob: Non sono tanto sicuro che farei questo paragone. Per favore, non farlo.

Julian: Si sta discutendo se Hezbollah abbia i requisiti di uno stato. È realmente diventato uno stato? È una cosa che viene citata nei cablogrammi dell’ambasciata americana, cioè che Hezbollah ha sviluppato la propria rete a fibre ottiche nel Sud del Libano.[1] Perciò possiede i tre requisiti principali di uno stato, il controllo delle forze armate in una particolare regione, controlla l’infrastruttura delle comunicazioni e ha anche un’infrastruttura finanziaria. Possiamo anche considerarle tre libertà di base. La libertà di movimento, la libertà fisica di muoversi, la capacità di andare da un posto all’altro e di non vedersi una forza armata piazzata contro. Possiamo pensare alla libertà di pensiero, e anche di comunicazione, che è intrinseca nella libertà di pensiero: se ti minacciano perché parli in pubblico, l’unico modo per salvaguardare il tuo diritto di comunicare è poterlo fare in privato. E per finire, la libertà di interazione economica, che va a braccetto, come la libertà di comunicazione, con la privacy delle interazioni economiche. Allora parliamo un po’

di queste idee che covano tra i cypherpunk sin dagli anni novanta, quelle che cercano di garantire questa importantissima terza libertà, cioè la libertà di interazione economica.

Jérémie: Ma perché solo tre libertà? Nella mia Carta europea dei diritti fondamentali ce ne sono di più.

Julian: La privacy diventa importante o in un'ottica comunitaria, cioè ti serve la privacy per comunicare liberamente e pensare liberamente, oppure perché ti serve in qualche modo per le interazioni economiche. Penso che esistano altre libertà secondarie, ma queste, le prime tre che ho citato, sono quelle fondamentali da cui derivano le altre.

Jérémie: Mah, c'è una definizione legale di libertà fondamentale.

Julian: Però mi sono letto la Carta dell'Unione europea e posso dirti che è un totale guazzabuglio di banalità.

Jérémie: Sì, certo, e le lobby sono riuscite a infilare la proprietà intellettuale nella Carta europea.

Julian: Un mucchio di cose pazzesche, pazzesche.

Andy: Credo ci sia un punto su cui possiamo essere d'accordo, cioè che il sistema monetario, l'infrastruttura economica per l'interscambio di soldi, al momento fa totalmente schifo. E perfino tutti quelli che hanno anche solo un account eBay saranno d'accordissimo, visto quello che sta combinando Paypal, per quello che stanno facendo Visa e MasterCard, stanno costringendo la gente ad accettare una situazione di monopolio di fatto. C'è stata anche questa cosa interessantissima dei cablo di WikiLeaks secondo i quali il governo russo ha cercato di negoziare una maniera perché i pagamenti Visa e MasterCard di cittadini russi in Russia fossero processati lì, ma Visa e MasterCard si sono rifiutati.[2]

Julian: Sì, il potere congiunto di ambasciata Usa e Visa è stato sufficiente a impedire persino alla Russia di avere il proprio sistema interno di pagamento con carte di credito.

Andy: Significa che persino i pagamenti dei cittadini russi nei negozi di russi per russi saranno trattati nei centri dati americani. Così il governo Usa avrà il controllo giurisdizionale, o almeno una finestra.

Julian: E così, quando Putin esce a comprarsi una Coca, trenta secondi dopo a Washington lo sanno.

Andy: E naturalmente è una situazione molto fastidiosa, indipendentemente dal fatto che mi piacciano o no gli Stati Uniti. È una faccenda molto pericolosa avere un punto centrale in cui sono conservati tutti i pagamenti effettuati perché invita a ogni sorta di utilizzo di questi dati.

Jacob: Una delle cose fondamentali che hanno capito i cypherpunk è che l'architettura influenza concretamente la situazione politica, perciò se hai un'architettura centralizzata, persino se saranno le migliori persone al mondo a controllarla, attirerà gli stronzi e questi stronzi faranno con il loro potere cose che i progettisti originari non avrebbero fatto. Ed è importante sapere che vale anche con i soldi.

Julian: Come i pozzi petroliferi in Arabia Saudita, la maledizione del petrolio.

Jacob: Ovunque gettiamo l'occhio possiamo vedere, soprattutto nei sistemi finanziari, che in pratica, anche se la gente ha le migliori intenzioni, non conta nulla. La verità è l'architettura. È la verità di Internet per quanto riguarda le comunicazioni. I cosiddetti sistemi legali di intercettazione, che è solo un modo carino di dire che spii la gente…

Julian: È un ossimoro, intercettazione legale.

Jacob: Assolutamente, come assassinio legale.

Andy: O tortura legale.

Jacob: Avete sentito degli attacchi legali con i droni a cittadini americani ordinati dal presidente Obama? Quando ha ammazzato il figlio sedicenne di Anwar al-Awlaki nello Yemen è stato un omicidio legale, o mirato, come l'hanno chiamato.[3] Le cosiddette intercettazioni legali sono la medesima cosa, basta che piazzi legale accanto a una parola e allora di colpo tutto diventa legittimo perché lo fa lo stato. Però in realtà è solo l'architettura dello stato che gli permette di farlo, è l'architettura delle leggi e della tecnologia, così come l'architettura dei sistemi finanziari.

I cypherpunk volevano creare sistemi che ci permettessero di pagarci in maniera davvero libera, con cui non fosse possibile interferire. Come le valute chaumiane, cioè il denaro elettronico progettato in base alle specifiche di David Chaum, il padre dell'eCash (una moneta elettronica totalmente anonima), anche se potresti ribattere che sono più centralizzate del necessario. L'idea è quella di riuscire a creare monete anonime, al contrario di Visa/MasterCard, che sono sistemi tracciabili. Anche se costruite attorno a un'autorità centrale, le monete chaumiane usano i protocolli crittografici inventati da David Chaum per garantire l'anonimato delle transazioni.[4]

Julian: Allora in pratica è denaro elettronico, però senza, che so, i numeri di serie sul contante.

Jacob: O con i numeri di serie che ti permettono di capire che è moneta valida ma non di sapere che Julian ha pagato Andy, o quanto era il totale.

Jérémie: In effetti è la riproposizione del contante nel mondo digitale.

Julian: Creare una valuta elettronica è una faccenda grossa proprio perché il controllo del mezzo di scambio è uno dei tre ingredienti di uno stato, come stavo dicendo parlando di Hezbollah. Se sottrai il monopolio statale dei mezzi di

interazione economica allora elimini una delle tre principali prerogative dello stato. Nel modello di stato mafioso, che funge da racket delle estorsioni, lo stato spreme soldi alla gente in ogni maniera possibile. Controllare i flussi di denaro è importante per le entrate fiscali dello stato ma anche semplicemente per controllare che cosa fa la gente, incentivare una cosa, disincentivarne un'altra, mettere completamente al bando una data attività o un'organizzazione, o le interazioni fra organizzazioni. Così, per esempio, nel caso dello straordinario embargo finanziario contro WikiLeaks non è il libero mercato che ha deciso il blocco perché non è un libero mercato, perché le regole statali hanno piazzato lassù in cima precisi attori finanziari e non permettono l'ingresso di altri nel mercato. La libertà economica è stata distorta da un'élite che è in grado di influenzare sia le regole che i principi relativi a quelle banche.[5]

ANDY: Triste dirlo, è il problema irrisolto del mondo elettronico in questo momento. Due istituti di credito, entrambi con una infrastruttura elettronica di vidimazione con base negli Stati Uniti, cioè con accesso ai dati nella giurisdizione Usa, controllano quasi tutti i pagamenti con carta di credito del pianeta. Aziende come Paypal, che è pure sotto giurisdizione Usa, applicano le politiche Usa, che sia il blocco della vendita di sigari cubani per i mercanti online tedeschi o il blocco dei pagamenti a WikiLeaks da giurisdizioni non-Usa. Significa che il governo americano ha accesso ai dati e ha la possibilità di imporre controlli ai pagamenti in tutto il mondo. Anche se i cittadini americani potrebbero ribattere che è la migliore democrazia che si può avere con i soldi, per i cittadini europei è una cosa senza prezzo.

JULIAN: Nel nostro mondo tradizionale abbiamo avuto entro certi limiti libertà di movimento, non così grande in certi casi.

JACOB: Ne sei sicuro, Julian? Secondo me la tua libertà di movimento è un perfetto esempio di quanto siamo realmente

liberi.

Julian: Be', no, in effetti, il Regno Unito ha annunciato che porrà 100.000 persone all'anno nelle mie condizioni.[6] Pertanto penso che sia una cosa, entro certi limiti, secondaria.

Jacob: È il motivo per cui i fondatori del mio paese sparavano agli inglesi. C'è una ragione per cui sparavamo agli inglesi. Ed esiste ancora oggi! La tirannide esiste ancora.

Jérémie: Non andiamo sul personale.

Andy: Quello che sta facendo attualmente il tuo paese, gli Stati Uniti, è privatizzare le prigioni e trattare contratti che garantiscano un tasso di riempimento del 90% alle imprese che gestiscono queste ex prigioni pubbliche americane.[7] Allora cos'è questo? È il capitalismo al massimo dell'assurdo.

Julian: Ci sono più persone in galera negli Stati Uniti di quante ce ne fossero in Unione Sovietica.

Jacob: È il classico tipo di situazione paradossale in cui, solo perché protesto contro una cosa sbagliata, tu puoi insinuare che faccio parte di qualcosa che è altrettanto sbagliato. Non sto dicendo che gli Stati Uniti siano perfetti. Credo però che gli Stati Uniti siano in realtà abbastanza grandiosi sotto tanti aspetti, ma nello specifico per quanto riguarda la retorica dei Padri fondatori.

Julian: La retorica dei Padri fondatori è in evidente disarmo da dieci anni.

Jacob: Non dobbiamo dimenticare che tante idee sulla retorica dei Padri fondatori sono pura mitologia e dovremmo stare attenti a idolatrarli. Sì, certo. Quello che volevo dire con il mio commento sulla tirannide britannica e la situazione in cui si trova Julian è che si tratta in realtà di una cosa culturale. È qui che entra in ballo la società e che diventa

molto importante, ed è difficilissimo che la tecnologia possa soppiantarla. E i problemi finanziari sono la cosa più rischiosa su cui lavorare. Ci sarà un motivo perché la persona che ha creato un'altra moneta elettronica, Bitcoin, l'ha fatto anonimamente. Non vuoi essere la persona che inventa la prima vera valuta elettronica di successo.[8]

JULIAN: I tipi che hanno creato l'e-gold sono finiti sotto processo negli Stati Uniti.[9]

JACOB: È incredibilmente frustrante.

JULIAN: Vorrei tornare alle tre libertà fondamentali: libertà di comunicazione, libertà di movimento e libertà di interazione economica. Se analizziamo la transizione della nostra società globale verso Internet, quando abbiamo attuato questa transizione la libertà di movimento non è intrinsecamente cambiata. La libertà di comunicazione è sotto certi aspetti aumentata in maniera spettacolare, nel senso che ora possiamo comunicare con molte più persone, ma d'altro canto è anche peggiorata enormemente perché non c'è più privacy e così le nostre comunicazioni possono essere spiate, e infatti sono spiate e conservate e, alla fine, usate contro di noi. E così questa elementare interazione fisica che abbiamo con la gente va in malora.

ANDY: La privacy è ottenibile ma ha un costo.

JULIAN: Le nostre interazioni economiche hanno subìto esattamente lo stesso destino. In una tradizionale interazione economica chi è che viene a saperlo? La gente che t'ha visto andare al mercato. Oggi chi è che viene a sapere della tua interazione economica? Se compri qualcosa dal tuo vicino con la Visa, un gesto che avresti fatto in una tradizionale società di mercato in maniera quasi totalmente privata, oggi chi lo sa?

JACOB: Tutti.

Julian: Lo sanno tutti. Hanno la condivisione dati fra tutte le grandi potenze occidentali, sanno tutto e lo conservano in eterno.

Andy: Julian, quel che dici non è sbagliato, ma non sono sicuro che tu possa davvero tracciare una distinzione fra libertà di comunicazione e libertà di interazione economica perché l'Internet che abbiamo oggi è l'infrastruttura di tutte le nostre interazioni sociali, economiche, culturali, politiche, tutte.

Jacob: Di sicuro della libertà di movimento.

Andy: Quale che sia l'architettura delle comunicazioni, i soldi sono solo bit. È solo un possibile utilizzo di Internet. Così se il sistema economico si basa sull'infrastruttura elettronica, l'architettura di questa infrastruttura dice qualcosa su come procede il flusso di denaro, su come viene controllato, su come è centralizzato eccetera. Forse Internet non è stata nemmeno pensata come infrastruttura per tutto quanto nei primi giorni, però la logica economica ha detto: "Be', è meno costoso farlo su Internet". Prima le banche e le compagnie delle carte di credito avevano i bancomat con interfaccia X.25, che dieci o venti anni fa erano una rete separata, ma ora è tutto TCP/IP perché costa di meno.[10] Così l'architettura della tecnologia sta diventando un tema chiave perché influenza tutte le altre aree, ed è questo che dovremmo davvero ripensare, nel senso che se vogliamo un modo decentrato di gestire i nostri pagamenti dobbiamo riprenderci l'infrastruttura.

Jacob: Bitcoin è in pratica una moneta elettronica.

Andy: Senza inflazione.

Jacob: Tende a operare in maniera decentrata, così invece di avere la Federal Reserve hai un tot di persone in tutto il mondo che sono d'accordo su cos'è reale e qual è la loro moneta attuale.

Julian: E ci sono certi programmi informatici che aiutano a farlo.

Jacob: Vorrei spiegarlo in maniera poco tecnica. È una valuta elettronica che è più un bene che una valuta, nel senso che la gente decide quanti euro vale un Bitcoin. Insomma, è un po' come l'oro, sotto questo aspetto, e c'è un costo per la cosiddetta estrazione dei Bitcoin, quando fai una ricerca su un computer per trovare un Bitcoin, e l'idea di base è che c'è una certa complessità computazionale ed è legata al valore della cosa. Così, messo in termini per non esperti, per me è un modo di spedire soldi a Julian e per Julian di confermarlo senza che Andy possa realmente interferire o impedirlo. Però c'è qualche problemino, non è una moneta realmente anonima, e a parer mio è davvero una brutta cosa.

Julian: Bitcoin è un ibrido molto interessante dato che i titolari degli account sono totalmente privati e puoi creare un account a piacimento, ma le transazioni dell'intera economia Bitcoin sono totalmente pubbliche. E funziona così, deve essere così perché tutti possano essere d'accordo che c'è stata una transazione, che l'account che invia ha ora meno soldi e il destinatario ne ha altrettanti in più. È uno dei pochi modi per gestire un sistema monetario distribuito che non richieda un server centrale, che diventerebbe un bersaglio ghiotto per il controllo coercitivo. In Bitcoin è la distribuzione a essere davvero innovativa, e anche gli algoritmi che permettono questa distribuzione, dove tu non devi fidarti di una parte particolare, che so, della rete bancaria Bitcoin. Invece la fiducia è distribuita. E il rispetto delle regole non avviene attraverso leggi o regolamenti o verifiche, avviene grazie alla difficoltà computazionale crittografica da cui deve passare qualsiasi parte della rete per dimostrare che fa quel che afferma. Quindi il rispetto dell'onesta "attività bancaria" con Bitcoin è insito nell'architettura del sistema. Il calcolo si traduce in costi di energia per ogni filiale della banca Bitcoin, pertanto possiamo attribuire un costo alle frodi, in termini di prezzo della corrente elettrica. Il lavoro necessario per

commettere una frode è destinato a essere più alto quanto a bolletta elettrica del beneficio economico che ne deriva. È molto innovativo, non perché siano idee mai esplorate prima (sulla carta lo erano da vent'anni) ma perché Bitcoin ha un equilibrio quasi perfetto e ha aggiunto un'idea molto innovativa su come dimostrare un vero consenso globale sulle transazioni dell'economia Bitcoin, persino dando per scontato che molte banche siano truffaldine e che chiunque potrebbe aprirne una.

Certo, come con qualsiasi altra moneta devi basare la valuta su qualcos'altro, sul lavoro, oppure i Bitcoin vengono scambiati con altre valute, ci sono gruppi di cambio con l'estero che lo fanno. Ci sono alcune altre limitazioni. Ci vogliono circa dieci minuti di tempo per l'accordo, ci vogliono circa dieci minuti di lavoro di calcolo tra la cessione della moneta e la sicurezza dell'altra parte che c'è un consenso globale sul fatto che la transazione sia avvenuta. È esattamente come il contante, quindi ha tutti i problemi di furto del contante. Ha anche tutti i benefici: una volta che sei sicuro di essere stato pagato, l'assegno non può essere cancellato, la banca non può ritirarlo. I rapporti di forza coercitivi sono tranciati. D'altro canto devi anche fare la guardia al contante. Questo, secondo me, è il problema più grosso. Però è abbastanza facile inserire passaggi ulteriori, organizzare servizi di deposito a garanzia in cui tu depositi i Bitcoin presso un servizio specificamente progettato per tenerli al sicuro e aggiungere anche l'assicurazione contro il furto.

Jacob: Cosa interessante, se la gente che ha creato Bitcoin avesse reso obbligatorio usare Tor, in modo da non creare un conto ma degli identificatori crittografici, sarebbe stato possibile, qualora tutto fosse passato da Tor come progetto centrale, avere l'anonimato della localizzazione, pur avendo tu identificatori a lungo termine che portano a te in modo da permetterti di ricollegare le tue transazioni.

Jérémie: Senza entrare nel tecnico, potremmo dichiararci

tutti d’accordo che Bitcoin ha alcune idee eccellenti ma qualche difetto. Ha una natura deflazionista perché il denaro tende a sparire da Bitcoin. Perciò non può funzionare alla lunga, però presenta concetti che possono essere migliorati. In questo momento dev’essere alla versione 0.7 o 0.8.

Jacob: È come reinventare David Chaum.[11]

Andy: Bitcoin è stato il tentativo più fortunato di introdurre una valuta digitale negli ultimi dieci anni, secondo me.

Julian: Hanno ottenuto un equilibrio quasi perfetto. Credo che Bitcoin attecchirà. È una moneta efficiente, puoi aprire un conto in dieci secondi e per trasferire soldi non hai altri costi oltre a quello della connessione Internet e di qualche minuto di energia elettrica. È decisamente concorrenziale rispetto a qualsiasi altra forma di bonifico bancario. Credo che avrà successo. Guardate cos’è capitato dopo parecchi furti di Bitcoin e la successiva campagna di stampa negativa nell’estate 2011 che ha fatto scendere il tasso di cambio a tre dollari Usa.[12] Bitcoin è gradualmente risalito a dodici dollari. Non ha avuto rimbalzi bruschi, è cresciuto secondo una curva graduale che sembra dimostrare una forte domanda della moneta. Sospetto che un sacco di domanda riguardi il piccolo spaccio di droga, ordini postali di marijuana e così via.[13] Però Bitcoin ha scarsi costi come valuta. Molti provider, soprattutto in posti che non hanno facilità di servizi di carta di credito, come l’ex Unione Sovietica, stanno iniziando a usarlo.

Ci sarà una stretta se continuerà a crescere. Non farà fuori Bitcoin perché la crittografia impedisce che abbiano successo i semplici attacchi usando la forza, però i servizi di cambio di valuta che convertono da e per Bitcoin potrebbero essere presi di mira molto più facilmente. Di contro, questi scambi possono avvenire ovunque nel mondo, così ci sono un bel po’ di giurisdizioni da passare prima che non ci siano più scambi, e poi il mercato clandestino ha la sua logica di scambio. Io credo che con Bitcoin ci si dovrebbe comportare in questo modo: farlo adottare dai provider e dal settore Internet dei

giochini che compri su Facebook eccetera, perché è davvero efficiente, e una volta che sarà adottato da una galassia di imprese e settori quelli formeranno una lobby che ne impedirà la messa al bando. È un po' così che è stata adottata la crittografia. Era bollata come traffico di armi, e alcuni di noi erano diventati mercanti d'armi, ma quando se la sono trovata nei browser ed è stata usata per le attività bancarie è nata una lobby abbastanza potente da impedire che fosse proibita, anche se ammetto che ci stanno provando di nuovo.

JACOB: Il problema è che i timori sulla privacy sono errati. Vediamo di essere onesti. È sbagliato suggerire che l'economia della situazione sia diversa con o senza Internet. Quando sono venuto qui e ho comprato le sterline britanniche ho dovuto dare il numero della previdenza sociale, che è il mio unico documento d'identità negli Stati Uniti, ho dovuto dare il nome, collegarlo a un conto corrente, allungargli dei soldi. Hanno registrato tutti i numeri di serie e poi hanno inviato tutte queste informazioni al governo federale. È questa l'analogia. È sinceramente più difficile ottenere valuta straniera negli Stati Uniti perché siamo tanto lontani da tutti gli altri. Però c'è una tendenza storica al controllo della valuta e non lo vediamo solo per quanto riguarda Internet. In realtà, da quanto ne so, ci sono bancomat nelle varie filiali che registrano i numeri di serie delle banconote e poi li tracciano per svolgere analisi di flusso del contante e vedere dove è stato speso e chi ci ha fatto cosa.

Se guardiamo questi sistemi e poi Internet, vediamo che non hanno rafforzato la privacy mentre migravamo in rete. In realtà l'hanno mantenuta debole come all'inizio. In questo senso ritengo molto importante verificare le tendenze del mondo pre-Internet per vedere dove eravamo diretti. Troveremo che se hai un sacco di soldi puoi pagare un extra per conservare la privacy, mentre se non hai tanti soldi non hai quasi di sicuro la minima privacy. E con Internet è peggio. Una cosa come Bitcoin è un passo nella direzione giusta perché, se associata a un canale per le comunicazioni anonime, come per esempio Tor, ti permette di inviare a

WikiLeaks un Bitcoin con Tor e tutti quelli che noteranno questa transazione vedranno solo un utente Tor che manda un Bitcoin e te che lo ricevi. È possibile farlo, sotto certi aspetti è molto meglio del contante.

JULIAN: Tutti facciamo un gran parlare della privacy delle comunicazioni e del diritto di pubblicare. È una cosa abbastanza facile da capire, ha una lunga storia, e in effetti i giornalisti adorano parlarne perché stanno proteggendo i propri interessi. Però se paragoniamo questo valore al valore della privacy e della libertà delle interazioni economiche, in pratica ogni volta che la CIA vede un'interazione economica può verificare che è questa parte da questa località che invia a quest'altra parte in quest'altra località, e si fa un'idea del valore e dell'importanza dell'interazione. Allora la libertà, o privacy, delle interazioni economiche non è forse più importante della libertà di parola dato che le interazioni economiche sorreggono praticamente l'intera struttura sociale?

JACOB: Sono intrinsecamente connesse. Credo che qui tu possa capire la differenza fra cypherpunk americani ed europei perché gran parte dei cypherpunk americani direbbe che sono esattamente la medesima cosa. Perché in una società che ha un libero mercato si direbbe che metti i soldi dove sta la bocca, cioè in ciò in cui credi.

JULIAN: Metti i soldi dove metti il tuo potere.

JACOB: Esatto. Non sto dicendo che sia giusto, è quasi un atteggiamento "retto", di destra, e forse non è quello che vogliamo. Forse, per esempio, vogliamo un capitalismo socialmente limitato.

JULIAN: Guardiamola in una semplice ottica di intelligence. Hai dieci milioni di dollari come budget per la raccolta informazioni. Puoi spiare le interazioni della gente via e-mail oppure avere la sorveglianza totale delle sue interazioni economiche. Quale preferiresti?

Andy: Mah, di questi tempi diranno: “Bene, costringeremo le banche e le strutture finanziarie di pagamento a usare Internet, così avremo entrambe le cose”. Ed è esattamente quello che hanno fatto. Quindi il punto è proprio che non c’è una via d’uscita facile. Puoi fare cose come usare Tor per proteggere le tue comunicazioni, puoi crittare le telefonate, puoi usare messaggerie sicure. Con il contante è molto più complicato e abbiamo quelle cose come le leggi contro il riciclaggio eccetera, inoltre ci dicono che i narcotrafficanti e le organizzazioni terroriste abusano di questa infrastruttura per fare cose brutte.

Jacob: Riecco i Cavalieri dell’Infocalisse.

Andy: In realtà sarei più interessato ad avere molta più trasparenza riguardo le aziende di sorveglianza e la spesa statale in questi campi. La domanda da porci è: che cosa compriamo quando garantiamo l’anonimato totale solo del sistema monetario? Che cosa succederebbe realmente? Io credo che potrebbe portare qui e là ad aree interessanti in cui la gente si sentirebbe un po’ più a suo agio e direbbe: “Be’, sai, posso alzare la voce, posso andare in parlamento ma posso anche comprare qualche politico”.

Jérémie: Stai parlando degli Stati Uniti, vero?

Jacob: Non è un segreto.

Andy: Non sono tanto sicuro che sia limitato agli Stati Uniti. In Germania non la chiamiamo corruzione, le chiamiamo fondazioni per comprare quadri dipinti dalle mogli dei politici, e così si svolge tutto nel mercato dell’arte o in altri campi. Quindi abbiamo solo nomi più carini. Forse in Francia le chiamate feste per gli amici e altri lo chiamano ingaggiare prostitute.

Jérémie: Negli Stati Uniti è speciale perché il legame fra il sistema politico e i soldi è molto stretto. Dopo dieci anni di lavoro sui temi del copyright, Larry Lessig ha detto che ha

smesso di cercare di correggere il copyright (non è vero che ha smesso) perché ha scoperto che il problema non era la comprensione dei politici di quella che sarebbe una buona politica dei diritti d'autore, il problema era che c'erano banalmente troppi legami con i capitani d'industria che spingevano per un pessimo regime dei diritti d'autore.[14] Quindi è un vero problema.

JULIAN: Jérémie, sei sicuro che sia un problema? Forse in realtà è positivo che quei settori siano produttivi…

ANDY: Direi che adesso l'avvocato del diavolo sta bevendo il mio whisky.

JACOB: Vediamo se riusciamo a finire la frase senza scoppiare a ridere. Mastro Troll, ci provochi.

JULIAN: I settori che sono produttivi, che producono benessere per l'intera società, utilizzano una fetta dei propri soldi per essere sicuri di continuare a essere produttivi, abbattendo leggi a capocchia scaturite dalla mitologia politica innescata dalle campagne di stampa. E il miglior modo per riuscirci è, in pratica, comprare i parlamentari, prendere i frutti del lavoro del proprio settore produttivo e usarli per modificare la legge, il tutto per far andare avanti la natura produttiva dell'industria.

JACOB: Aspetta, ci sono. Pronti? Pronti? Adesso siete pronti? No.

JULIAN: Perché no?

JACOB: C'è un paio di motivi, ma intanto noto un circolo vizioso estremamente negativo. Per esempio, credo che uno dei massimi donatori nelle campagne politiche nello stato della California sia il sindacato degli agenti carcerari, e in parte succede perché amano fare pressione a favore di leggi più severe non perché gliene freghi della legalità ma perché significano un incentivo alla creazione di posti di lavoro.[15]

Così se vedete che questa gente preme per costruire più prigioni, per sbattere in galera più persone, per ottenere sentenze più lunghe, che cosa stanno facendo in realtà? Stanno sfruttando i soldi ricevuti per un lavoro utile (è discutibile) per allargare il monopolio che lo stato gli garantisce.

JULIAN: Perciò li usano solo per il trasferimento della ricchezza dai settori realmente produttivi a quelli che non lo sono?

JACOB: Potremmo riassumerlo così.

JULIAN: Ma forse è solo una componente marginale. Ogni sistema è soggetto ad abusi, forse questi scrocconi coinvolti nel trasferimento di ricchezza sono un elemento marginale e in realtà la maggior parte delle lobby, la maggioranza delle influenze sul Congresso viene dai settori produttivi che vogliono essere sicuri che le leggi continuino a permettergli di essere produttivi.

JACOB: Puoi valutarlo molto facilmente perché puoi verificare quali persone vogliono promuovere attività in cerca di rendita e vogliono limitare le libertà degli altri di creare una situazione nella quale loro stessi non potrebbero essere ciò che sono oggi. Quando lo fanno allora sai che è andato storto qualcosa e che stanno solo proteggendo quello che hanno, che hanno creato in pratica con lo sfruttamento, di solito facendo appello alle emozioni come quando dicono: “Dio mio, fermate i terroristi, fermate la pornografia infantile, fermate il riciclaggio di denaro sporco, combattete la guerra alle droghe”. Forse queste cose sono assolutamente ragionevoli nel contesto in cui sono proposte all’inizio, e di solito lo sono, perché in genere riteniamo cattive quelle attività, essendoci una componente seria in ciascuna di esse.

ANDY: Io vorrei tornare al copyright e proporvi un altro esempio. Ci furono seri problemi quando uscirono le automobili. Chi aveva una ditta di trasporto passeggeri con i

cavalli temeva che avrebbero azzerato il suo giro d'affari, ed era vero, ma forse era anche un ragionamento sensato. Sono stato invitato a parlare davanti all'associazione delle case cinematografiche tedesche, e prima del mio intervento un docente di un'università di Berlino ha parlato in maniera supermisurata dell'evoluzione della razza umana e dello sviluppo della cultura, dicendo che copiare le idee ed evolverle è la chiave di tutto, proprio come fare film significa prendere un tema ed esprimerlo secondo una struttura drammaturgica. Dopo i suoi quaranta minuti il moderatore l'ha interrotto bruscamente dicendo: "Bene, così adesso che lei ci ha detto che dovremmo legalizzare il furto, sentiamo cos'ha da dire il tizio del Chaos Computer Club". E io stavo pensando: "Ehi, che diavolo? Se dico quel che penso uscirò vivo di qui?". Insomma, alcuni settori hanno strutture d'affari che non facilitano l'evoluzione. È puro egoismo rimanere in quel modo nella loro traiettoria devoluzionista, rendendola ancor più monopolista. Anche quando sono uscite le audiocassette hanno pensato che avrebbero ammazzato l'industria discografica. È successo il contrario, l'industria discografica ha conosciuto un boom. Il problema è qual è la politica. Qual è la maniera positiva in cui formulare queste cose?

JULIAN: Mi domando solo se non potremmo in realtà standardizzare la pratica corrente negli Stati Uniti e formalizzarla in modo che puoi banalmente comprarti i senatori e i loro voti al Senato.

JÉRÉMIE: No, no, no, no.

ANDY: Metti che abbiamo i soldi.

JULIAN: Sì, e che avvenga tutto alla luce del sole e ci siano i compratori e si vada all'asta.

ANDY: Ma l'industria degli armamenti avrà sempre più soldi.

JULIAN: No, non credo. Credo che il complesso militar-

industriale finirebbe relativamente emarginato perché è capace di operare soltanto al chiuso in un sistema che non è aperto alle offerte del mercato più ampio, a livelli superiori rispetto agli altri settori.

Jacob: Il sistema ha una fondamentale disuguaglianza.

Jérémie: In un'ottica economica liberale, antimonopolista, quando dici "lasciamo che decidano i protagonisti quale sarà la politica", io ti rispondo con l'esperienza di Internet negli ultimi quindici anni, in cui l'innovazione veniva dal basso, in cui emergevano pratiche dal nulla, in cui un paio di ragazzotti in un garage inventava una tecnologia che attecchiva.

Julian: Per quasi tutto, per Apple, per Google, per YouTube, per tutto.

Jérémie: Per tutto. Tutto quello che è successo in Internet ha vissuto un boom dopo essere rimasto ignorato per mesi o anni, perciò non puoi predire quale sarà la prossima innovazione, e il ritmo dell'innovazione è talmente rapido da risultare più veloce del processo legislativo. Così quando progetti una legge che influenzi il mercato odierno, i rapporti di forza tra varie aziende e attori, se rafforzi uno che è già forte puoi impedire a un nuovo concorrente più efficiente di spuntare.

Julian: Il mercato dev'essere regolato in modo da essere libero.

Jérémie: Naturalmente devi combattere i monopoli e devi avere un potere superiore a quello delle aziende per punire i comportamenti sbagliati, ma quel che voglio dire è che è la politica che deve adattarsi alla società, e non l'inverso. Con le battaglie sul copyright abbiamo l'impressione che il legislatore cerchi di far mutare la società intera in modo che si adatti a una cornice definita da, tanto per fare un nome, Hollywood. "Bene, quello che state facendo con la vostra nuova pratica culturale è moralmente sbagliato, perciò se

non la smettete noi progetteremo strumenti legali per farvi smettere di fare quel che ritenete giusto.” Non è così che si fa una buona politica. La buona politica guarda il mondo e lo adatta in modo da correggere quello che è sbagliato e favorire quello che è giusto. Sono convinto che quando permetti ai settori industriali più potenti di decidere la politica sei sulla strada sbagliata.

Andy: Sto solo cercando di aiutare i presenti a capire quale potrebbe essere una buona politica. Quello che hai appena detto è a questo livello un filo troppo complicato per me. Sto cercando di semplificare un tantino. Un certo Heinz von Foerster, il padre della cibernetica, ha creato una serie di regole, e una era “agire sempre in maniera da accrescere le opzioni”.[16] Altrettanto vale per le politiche, la tecnologia, qualunque cosa, sempre fare quello che ti dà più, non meno opzioni.

Julian: È anche una strategia degli scacchi.

Andy: Si è detto che l’aumento della privacy nelle transazioni monetarie potrebbe avere ricadute negative, perciò dobbiamo pensare: “Oggi il sistema monetario ha una sua logica specifica e il problema è come impedire che conquisti altre aree”. Perché il sistema monetario ha la capacità, diversamente dal settore telecomunicazioni, di influenzare e limitare totalmente le opzioni della gente in altre aree. Se puoi assoldare sicari per fare certe cose, o se puoi comprare armi per fare la guerra ad altri paesi, allora stai limitando l’opzione di vivere, di agire di altre persone. Se invece metto più soldi nelle comunicazioni allora più persone avranno più opzioni. Se immetto più armi nel mercato…

Jacob: No, più sei in grado di sorvegliare più avrai il controllo.

Andy: Ed è un’altra ragione per limitare il mercato delle armi, compresa la tecnologia per la sorveglianza delle telecomunicazioni.

Jacob: Certo, se vuoi limitare la mia capacità di venderle, come fai? Come limiti la mia capacità di trasferire ricchezza? Anche attraverso le reti di comunicazione. Una delle cose più offensive dei salvataggi bancari negli Stati Uniti, che sono stati un insulto a tante persone per un'intera serie di motivi, è che hanno dimostrato che la ricchezza è solo una serie di bit in un sistema informatico. Alcune persone sono riuscite, implorando in maniera molto efficace, a far sì che tanti bit fossero quotati molto. E allora qual è la domanda da farsi? Che valore ha un sistema se puoi ingannarlo per far quotare bene i tuoi bit? E intanto tutti gli altri che si sbattono per tirare avanti non hanno nemmeno il riconoscimento di possedere dei bit che valga anche solo la pena di usare per il lancio della monetina.[17]

Andy: Stai dicendo che ci serve un sistema economico totalmente diverso? Perché oggi il valore non è accoppiato al valore economico.

Jacob: No, sto dicendo che c'è un valore economico.

Andy: Puoi fare brutte cose e ricavarci soldi, e puoi fare belle cose senza ottenere un centesimo.

Jacob: Be', no, sto dicendo che non puoi separare l'economia dalla comunicazione. Non mi sto chiedendo se ci serve o no un sistema economico diverso. Non sono un economista. Voglio solo dire che c'è un valore nei sistemi comunicativi e nella libertà di queste comunicazioni, così come c'è valore nella libertà del puro e semplice baratto: io ho il diritto di darti qualcosa in cambio del tuo lavoro, così come ho il diritto di spiegare un'idea e tu hai il diritto di dirmi che cosa pensi di questa mia idea. Il sistema economico non esiste in una specie di vuoto pneumatico. Il sistema delle comunicazioni è direttamente legato a questo, ed è una parte della società.

Se torniamo a quel concetto riduzionista di libertà, delle tre libertà citate da Julian, è ovviamente legato alla libertà di movimento: non puoi nemmeno comprare un biglietto aereo

senza usare una valuta tracciabile, altrimenti vieni segnalato. Se entri in un aeroporto e cerchi di comprare un biglietto per lo stesso giorno in contanti sei segnalato. Ti becchi ulteriori controlli di sicurezza, non puoi volare senza un'identificazione, e se fossi tanto sfortunato da comprare il volo con una carta di credito registrerebbero tutto su di te, dal tuo indirizzo IP al tuo browser. Io, grazie al Freedom of Information Act, ho i dati delle mie schede dell'Immigrazione e Dogane di un paio di anni fa perché pensavo che forse un giorno sarà interessante guardare le differenze. E naturalmente è citato Roger Dingledine, che m'ha comprato un biglietto aereo per lavoro, c'è la sua carta di credito, l'indirizzo presso cui l'ha comprato, il browser che ha usato e tutto il resto riguardante quel biglietto.

JULIAN: Ed è arrivato al governo Usa, non è rimasto dentro l'unità elaborazione dell'azienda?

JACOB: Esatto. I dati commerciali sono stati raccolti, inviati al governo e ricollegati. E la cosa che trovo davvero pazzesca è che in pratica è la fusione delle tre cose di cui parlavi. Era mio diritto viaggiare liberamente, era mia facoltà comprare quel biglietto o che fosse un altro ad acquistarlo, ed era mia facoltà essere effettivamente in grado di parlare. Stavo andando a parlare in un posto, e per farlo m'è toccato scendere a compromessi nelle altre due sfere. E in effetti questo influenza la mia capacità di parlare, soprattutto quando scopro dopo che cosa hanno raccolto e che hanno riunito i dati.

Julian: Jake, puoi parlarci un po’ del fermo che hai subìto negli aeroporti Usa e come mai è successo?

Jacob: Hanno affermato che succede “so io perché”.

Julian: Però non lo spiegano.

Andy: Posso tentare io di riassumerlo perché la sicurezza tecnica e quella degli affari pubblici sono due cose totalmente distinte. Puoi avere un sistema completamente sicuro e il governo penserà che non è bello perché ritengono sicuro solo quando possono guardarci dentro, quando possono controllarlo, quando possono insinuarsi nella sicurezza tecnica. Qui non si tratta di Jake che tentava di salire a bordo di un apparecchio per ammazzare qualcuno, per dirottare l’aereo o quant’altro. Riguardava la sua capacità di influire sugli affari pubblici recandosi in altri paesi per parlare alla gente e diffondere idee. È la cosa più pericolosa per i governi in questi giorni, vedere che la gente ha idee migliori della loro politica.

Jacob: Ti sono davvero grato perché hai apprezzato la mia dichiarazione, però vorrei precisare che è molto peggio di così perché questi sono dati che raccolgono su tutti quanti. È successo prima che io facessi alcunché di interessante, è capitato solo perché viaggiavo, e sono stati gli stessi sistemi, l’architettura, a favorire questa raccolta di informazioni. È successo prima che fossi fermato per qualcosa, prima che fossi deportato dal Libano, prima che il governo Usa avesse

un interesse speciale per me.

ANDY: Forse l'hanno previsto, forse l'hanno capito prima di te.

JACOB: Certo, in parte grazie a questa raccolta di dati. Però ti danno sempre risposte diverse. Di solito ti rifilano una risposta conclusiva, che è sempre ovunque "perché possiamo". E io dico: "Va bene, non contesto la vostra autorità, o meglio, contesto la vostra autorità ma non adesso. Vorrei solo sapere perché succede a me". Ora mi rispondono di continuo: "Ma non è evidente? Lei lavora su Tor" oppure "Sta al fianco di Julian, che cosa pretende?". Lo trovo affascinante perché tutte le diverse persone che mi trattengono, di solito negli Stati Uniti agenti della Customs and Border Protection e dell'Immigration and Customs Enforcement, mi diranno che succede perché hanno l'autorità di farlo. Li ho anche indotti a rifilarmi fesserie come "oh, ricorda l'11 settembre? Ecco perché" o "perché vogliamo che risponda ad alcune domande e questo è il posto in cui ha meno diritti di tutti, o almeno così sosteniamo".

E in questa situazione ti impediranno di rivolgerti a un avvocato, ti negheranno l'accesso al bagno però ti daranno dell'acqua, ti daranno qualcosa da bere, a mo' di diuretico, per convincerti che hai davvero voglia di collaborare in qualche modo. L'hanno fatto per mettermi pressione, per motivi politici. Mi hanno chiesto cosa pensavo della guerra in Iraq, che cosa penso della guerra in Afghanistan. In pratica a ogni passo hanno replicato le tattiche dell'FBI durante il Cointelpro (il mastodontico programma segreto di operazioni interne in corso fra il 1956 e il 1971). Per esempio, hanno specificamente cercato di far valere la loro autorità di cambiare le mie idee politiche e di spingermi non solo a cambiarle ma a regalargli un accesso speciale a quello che mi frulla in testa. E mi hanno sequestrato degli oggetti. Non sono realmente libero di discutere tutte le cose che mi sono capitate perché è un tema molto nebuloso di cui non so nemmeno se ho il permesso di parlare. Sono sicuro che è

successo ad altre persone ma non l'ho mai saputo.

Ero all'aeroporto Pearson di Toronto mentre tornavo a casa da una visita alla mia famiglia. Stavo rientrando a Seattle, dove abitavo in quei giorni, e mi hanno fermato, mi hanno messo nel controllo secondario, poi in quello terziario e alla fine in una cella. E mi hanno trattenuto tanto a lungo che quando alla fine mi hanno rilasciato avevo perso il volo. Però c'è un risvolto curioso, cioè che queste aree predetentive sono tecnicamente territorio Usa in territorio canadese, e c'è una regola che dice che se perdi il volo oppure passa molto tempo prima del prossimo sei costretto a uscire. Così sono stato tecnicamente cacciato dall'America essendo stato fermato tanto a lungo e sono stato costretto a entrare in Canada, prendere un volo interno e noleggiare un'auto per superare il confine. E quando sono arrivato alla frontiera m'hanno chiesto quanto tempo ero rimasto in Canada. Ho risposto: "Mah, cinque ore più il fermo a Toronto". Ero stato in Canada otto ore. E loro: "Be', venga che la fermiamo di nuovo". Poi m'hanno smantellato la macchina e il computer e ci hanno guardato dentro, e alla fine m'hanno trattenuto. M'hanno fatto andare in bagno dopo una mezz'ora, potremmo dire che sono stati molto misericordiosi. È quella che chiamano eccezione nei controlli alla frontiera, un comportamento giustificato perché hanno, a sentir loro, la possibilità di farlo e nessuno gliela contesta.[1]

Julian: Questo è capitato a te, ma i cinesi con cui sono in contatto, quando discutono del grande firewall in Cina, la grande muraglia tecnologica (in Occidente ne parliamo in termini di censura che impedisce ai cittadini cinesi di leggere quello che si dice all'Ovest del governo cinese, e anche cosa dicono i dissidenti cinesi e Falun Gong e la BBC e, a dirla tutta, la vera e propria propaganda sulla Cina), la loro vera preoccupazione non è la censura. È che per avere una censura di Internet ci deve essere anche la sorveglianza di Internet. Per controllare quello che guarda uno, per verificare se è permesso o proibito, devi vederlo, e pertanto se lo vedi puoi anche registrarlo. Ha avuto un tremendo

effetto paralizzante sui cinesi, non perché sono censurati ma perché tutto quello che leggono è spiato e registrato. In realtà vale per tutti noi. È una cosa che modifica le persone quando ne sono coscienti. Modifica il loro comportamento, diventano meno risolute nelle lamentele contro i vari tipi di autorità.

Jacob: Però è la risposta sbagliata a questo tipo di influenza. La mia persecuzione alla frontiera, per esempio, non è isolata, nel senso che qualsiasi arabo-americano, dall'11 settembre ma anche prima, ci si è dovuto scontrare. È solo che io rifiuto che vada sprecato il privilegio di avere la pelle bianca e un passaporto americano e mi rifiuto di stare zitto perché le cose che fanno sono sbagliate, e perché abusano del potere che utilizzano. E dobbiamo opporci a queste cose proprio come ci sono persone coraggiose in Cina che si oppongono a questa situazione, come Isaac Mao, per esempio.[2] Isaac si batte con forza proprio contro questo tipo di censura perché la risposta giusta non è cedere a questo tipo di pressione soltanto perché il governo afferma che può farlo.

Jérémie: Però stiamo di nuovo parlando di politica, perché in pratica tu dici che la gente dovrebbe difendere i propri diritti, ma prima la gente deve capire perché dovrebbe e poi avere la possibilità di comunicare con gli altri. Ho avuto modo di parlare con alcuni cinesi, e non so se occupavano una qualche posizione statale o se erano stati selezionati per poter uscire a parlare con me, ma quando discutevo con loro della censura in Internet molto spesso ottenevo questa risposta: "Mah, è per il bene del Popolo. Certo che c'è la censura perché se non ci fosse allora ci sarebbero comportamenti estremisti, ci sarebbero cose che tutti odieremmo e così il governo prende queste misure per essere sicuro che tutto vada per il meglio".

Jacob: Dicono la stessa cosa con il traffico di organi. Non lasciamo che gli organi vadano sprecati!

Jérémie: Se guardate come è condotta la censura cinese notate da un punto di vista tecnico che è uno dei sistemi più avanzati al mondo.

Jacob: Assolutamente.

Jérémie: E ho sentito che su Weibo, che è l'equivalente cinese di Twitter, il governo è in grado di filtrare certi hashtag per essere sicuro che non escano da una provincia selezionata.

Jacob: È fondamentale ricordare che quando la gente parla di censura in Asia ama parlarne in termini di "gli altri", dato che tocca solo la gente del "Lontanistan". È importantissimo sapere che, quando fai una ricerca su Google negli Stati Uniti, qualche volta sostengono di avere omesso certi risultati a causa di limitazioni legali. C'è una differenza tra le due cose, sia per come sono implementate e, naturalmente, nella realtà sociale del come, perché e dove, però una grossa componente è in realtà l'architettura. Per esempio, l'Internet americana è molto decentrata, è durissimo attuare la censura alla cinese.

Julian: Mah, una grossa fetta è Google, e puoi censurare Google. Un sacco di pagine che citano WikiLeaks sono censurate da Google.

Jacob: Sì, senza dubbio. E dato che l'indice è libero è possibile fare un'analisi differenziale.

Julian: Sì, in teoria.

Jacob: In teoria. E nella pratica ci sono persone che lavorano su questo genere di rilevazione della censura cercando le differenze fra le diverse prospettive nel mondo. Io credo che sia importante ricordare che la censura e la sorveglianza non sono problemi di "altri posti". La gente in Occidente ama dire che "gli iraniani e i cinesi e nordcoreani hanno bisogno dell'anonimato e della libertà, noi qui no". E

con “qui” di solito intendono “negli Stati Uniti”. Ma in realtà non sono solo i regimi repressivi perché se ti capita di trovarti sul gradino più alto di qualsiasi regime per te non è repressivo. Noi riteniamo che il Regno Unito sia un posto meraviglioso, di solito la gente pensa che la Svezia sia un posto mica male, eppure puoi verificare che quando esci dalle grazie di quelli al potere non ti trovi in una posizione gradevole. Però Julian è ancora vivo, no? Così chiaramente è un simbolo del fatto che è un paese libero. Sbaglio?

JULIAN: Ho lavorato duramente per preservare la mia attuale posizione. Ma forse dovremmo discutere della censura di Internet in Occidente. È molto interessante. Se torniamo al 1953 e andiamo a guardare la grande enciclopedia sovietica, che era onnipresente, certe volte conteneva delle correzioni con il cambiare della politica in Unione Sovietica. Nel 1953 morì Beria, il capo dello NKVD, la polizia segreta, e uscì dal favore politico, pertanto la voce a lui dedicata, che lo descriveva in toni entusiastici, fu eliminata dall’autorità competente dell’enciclopedia che inviò una correzione da incollare su tutti i volumi. Era una cosa che saltava all’occhio. Cito questo esempio perché era talmente evidente e individuabile che il tentativo è passato alla storia. Invece in Gran Bretagna abbiamo il “Guardian” e altre grandi testate che eliminano gli articoli dai loro archivi Internet in segreto senza alcuna spiegazione. Se vai adesso a quelle pagine e cerchi di aprirle, per esempio gli articoli sulla truffa del miliardario Nadhmi Auchi, ottieni “pagina non trovata”, e sono stati anche rimossi dagli indici.

Lasciate che vi racconti il mio coinvolgimento nel caso Nadhmi Auchi. Nel 1990 l’Iraq invase il Kuwait, scatenando la prima guerra del Golfo. Il governo kuwaitiano in esilio, ma anche durante il rientro, aveva bisogno di liquidi, perciò iniziò a vendere varie proprietà tra cui parecchie raffinerie fuori dal Kuwait. Un affarista britannico, Nadhmi Auchi, immigrato nel Regno Unito nei primi anni ottanta dall’Iraq, dove era stato una figura di spicco del regime di Saddam Hussein, funse da mediatore di questo affare e in seguito fu accusato

di coinvolgimento nella distribuzione di commesse illegali per 118 milioni di dollari. Quell'indagine è stata la più grossa inchiesta per corruzione nella storia postbellica europea. Nel 2003 Auchi fu accusato di frode in quello che sarebbe diventato noto come lo scandalo Elf Aquitaine. Comunque oggi ha oltre 200 imprese registrate attraverso la sua holding lussemburghese, e altre a Panama. È coinvolto nei contratti per i cellulari nell'Iraq postbellico e in molti altri affari in tutto il mondo.[3]

Negli Stati Uniti c'era Tony Rezko, fundraiser per la campagna senatoriale di Barack Obama e amico di lunga data di Auchi, che era stato il suo consulente finanziario. Auchi e Rezko entrarono in affari anche con l'ex governatore dell'Illinois, Rod Blagojevich. Sia Rezko che Blagojevich sono stati condannati per corruzione, Rezko nel 2008 e Blagojevich nel 2010-2011 (quando i federali lo registrarono al telefono mentre cercava di vendere l'ex seggio di Obama al Senato). Nel 2007-2008, mentre Obama correva per diventare il candidato democratico alla presidenza, la stampa Usa iniziò a indagare i suoi contatti. Investigarono Rezko e segnalarono alcuni contatti relativi all'acquisto della casa di Barack Obama. Nel 2008, poco prima del suo processo, Rezko ricevette un bonifico di 3,5 milioni di dollari da Auchi che non riferì ai magistrati, nonostante gli fosse stato richiesto, e per questo finì al fresco. Così i riflettori della stampa Usa si concentrarono su Auchi, che a quel punto diede indicazioni allo studio legale britannico Carter-Ruck di avviare una campagna aggressiva su buona parte del reportage del 2003 sullo scandalo Elf Aquitaine e sulla sua condanna in Francia. Gli andò molto bene. Prese di mira la stampa inglese e persino i blog Usa, e fece rimuovere quasi una dozzina di articoli, che io sappia. Quasi tutti, compresi quelli negli archivi dei giornali britannici, semplicemente sparirono. Come se non fossero mai esistiti. Non ci fu alcun "abbiamo ricevuto una querela e abbiamo deciso di eliminare l'articolo". Sono persino spariti dagli indici. WikiLeaks li ha dissepolti e li ha ripubblicati.[4]

Jacob: Cancellano la storia.

Julian: La storia non viene solo modificata, ha cessato di esistere. È l'aforisma di Orwell: "Colui che controlla il presente controlla il passato, e colui che controlla il passato controlla il futuro". È la cancellazione invisibile della storia in Occidente, e stiamo ancora parlando solo della censura post-pubblicazione. L'autocensura pre-pubblicazione è molto più estrema ma spesso più difficile da individuare. L'abbiamo visto con il Cablegate dato che WikiLeaks collabora con diversi media in tutto il mondo, pertanto possiamo verificare quali sono quelli che censurano il nostro materiale.[5]

Per esempio, il "New York Times" ha tagliato un cablo secondo il quale sono stati distribuiti milioni di dollari per influenzare in segreto alcuni cittadini libici legati alla politica tramite le compagnie petrolifere operanti in Libia. Il cablo non citava nemmeno una compagnia specifica, il "New York Times" ha semplicemente tagliato la frase "compagnie di servizi petroliferi".[6] Forse il caso più clamoroso è stato l'uso da parte del "Times" di un cablo di 62 pagine sul programma missilistico nordcoreano e sulla possibilità che avessero venduto missili agli iraniani, del quale il giornale ha utilizzato due paragrafi per sostenere, in un articolo, che l'Iran possedeva missili in grado di colpire l'Europa, mentre in altri punti del cablo si sosteneva l'esatto opposto.[7]

Il "Guardian" ha manipolato un cablo su Yulia Tymoshenko, l'ex primo ministro ucraino, in cui si diceva che forse nascondeva i suoi soldi a Londra.[8] Ha censurato le accuse secondo le quali l'élite del Kazakistan in toto era corrotta, non ha citato nemmeno una persona, e anche l'accusa secondo la quale sia l'Eni, la compagnia energetica italiana attiva in Kazakistan, sia la British Gas erano corrotte.[9] In pratica il "Guardian" censurava i passaggi in cui una persona ricca era accusata di qualcosa in un cablo, a meno che il "Guardian" non avesse progetti istituzionali contro quella persona ricca.[10] Così, tanto per fare un esempio, in un cablo sulla criminalità organizzata bulgara compariva un russo, e il "Guardian" ha fatto sembrare che tutta la faccenda

riguardasse lui, ma era solo una persona all'interno di una lunga lista di organizzazioni e individui associati al crimine organizzato bulgaro.[11] "Der Spiegel" ha censurato un paragrafo su quello che faceva la Merkel, non per scrupoli relativi ai diritti umani, per puri timori politici sulla Merkel.[12] Ci sono tantissimi esempi.[13]

ANDY: La nostra idea di libertà di informazione e di libero flusso di informazioni è in un certo senso un nuovo concetto molto radicale per il pianeta Terra. Direi che non è tanto diverso tra l'Europa e gli altri paesi. Sì, ci sono paesi che hanno un'impostazione democratica, che significa che puoi leggere e capire e forse perfino combattere legalmente l'infrastruttura censoria, ma non significa che non esista, mentre avrai i tuoi bei problemi a provarci in Arabia Saudita o in Cina.

JULIAN: La mia esperienza con l'Occidente è che è solo molto più sofisticato nella quantità di livelli di sviamento e occultamento di quanto sta accadendo realmente. Questi strati sono lì per permettere di negare la censura in corso. Potete raffigurarvi la censura come una piramide. Di questa piramide emerge dalla sabbia solo la punta, ed è voluto. La punta è la parte alla luce del sole, cause per diffamazione, omicidi di giornalisti, telecamere sequestrate dai militari eccetera, cioè la censura pubblicamente ammessa. Ma è la parte minimale. Sotto la punta lo strato successivo comprende tutte quelle persone che non vogliono stare sulla punta, che applicano l'autocensura per non finirci. Poi lo strato successivo sono tutte le forme di sollecitazione economica o di patrocinio offerte alla gente perché scriva su una o l'altra cosa. Lo strato ancora più sotto è l'economia allo stato puro, che cos'è conveniente scrivere, anche non considerando i i fattori economici dalla parte superiore della piramide. Poi c'è lo strato del pregiudizio dei lettori che hanno solo un certo livello di istruzione, quindi da un lato sono facili da manipolare con informazioni false, e dall'altro non puoi nemmeno rivelargli una verità complessa. L'ultimo

strato è la distribuzione: per esempio, certe persone non hanno semplicemente accesso alle informazioni in una data lingua. È la piramide della censura. Quello che sta facendo il "Guardian" con le sue manipolazioni di Cablegate appartiene al secondo strato.

Possono negare che esista questa censura o perché avviene lontano dalla luce del sole o perché non esistono istruzioni di censurare una particolare tesi. È raro che ai giornalisti ordinino "non stampate nulla su quello" oppure "non pubblicate quel fatto". Piuttosto sono loro a capire che ci si aspetta questo da loro perché comprendono gli interessi di coloro che desiderano tenersi buoni o che vogliono frequentare. Se farai il bravo ti daranno le pacchette sulla testa e ti ricompenseranno, se non farai il bravo no. È semplicissimo. Amo fare questo esempio: l'evidente censura che avveniva in Unione Sovietica, la censura su cui facevano tanta propaganda in Occidente, energumeni che andavano a prendere i giornalisti nel cuore della notte per portarli via da casa, è stata semplicemente spostata di dodici ore. Oggi aspettiamo che sia giorno per prelevare i giornalisti quando perdono la protezione o non possono rispettare il loro debito. Portano via da casa i giornalisti portando via la casa ai giornalisti. Le società occidentali sono specializzate nella ripulitura della censura e nello strutturare gli affari dei potenti in modo che ogni residua libertà di parola abbia difficoltà a colpire le vere relazioni di potere di una società altamente finanziarizzata perché queste relazioni sono nascoste da strati e strati di complessità e segretezza.

Andy: Jérémie ha citato i pedo-nazisti.

Jacob: E così siamo tornati ai pedo-nazi.

Jérémie: Due Cavalieri in un colpo solo.

Andy: I pedo-nazi riassumono abbastanza bene la filosofia della censura tedesca, o forse di parte dell'Europa. La Germania non vuole contenuti razzisti in Internet per via del suo passato, e naturalmente se dici alla gente che poni limiti

a Internet per colpa dei pedofili a quel punto potrai fare qualsiasi cosa. Fra l'altro c'è stato un documento interno della Commissione europea sulla riservatezza dei dati che diceva: "Dovremmo parlare di più della pornografia infantile, così la gente sarà favorevole".[14]

JULIAN: Puoi parlarcene un po'? Cioè che se censuriamo solo una cosa, mettiamo soltanto la pornografia infantile, allora per impedire con la censura che la gente la veda dobbiamo sorvegliare tutto quello che fanno tutti. Dobbiamo costruire un'infrastruttura del genere. Dobbiamo impiantare un massiccio sistema di spionaggio e censura per censurare soltanto una cosa.

ANDY: Sta tutto nei dettagli del meccanismo: in Germania il cosiddetto sistema precensorio ti obbliga a indicare il responsabile legale per tutto quanto pubblichi. In questo modo, per sintetizzare, se pubblichi qualcosa, che sia su carta o in Internet, senza dire chi è legalmente responsabile dei contenuti, già violi la legge. Significa che se vedi un responsabile e qualcuno viola la legge diffondendo, che so, pornografia infantile o tesi razziste, a quel punto puoi solo dire: "Bene, vediamo dove sta quel tizio e becchiamolo e togliamo la roba dalla rete".

JULIAN: Cioè censuriamo chi pubblica invece di censurare chi legge.

ANDY: Sì. E questo è quando guardi cose specifiche. Posso anche essere d'accordo sul fatto che non tutto deve essere sempre disponibile perché se penso alle tematiche razziste ci sono certe volte delle robe con l'indirizzo di casa delle persone eccetera che potrebbero portare a situazioni a cui non sono favorevole.

JULIAN: Però, Andy, è una storia molto tedesca. Per farlo, per decidere che cosa sarà accettabile e cosa non lo sarà, devi insediare una commissione, devi piazzare persone in questa commissione, devi avere una procedura di selezione per

questa commissione…

Andy: Sì, abbiamo puttanate del genere. Le stragi tedesche nella Seconda guerra mondiale, tutto quello che hanno combinato i nazisti, ogni proprietà che hanno sequestrato, ogni volta rilasciavano una ricevuta, tenevano l'elenco. Erano attività burocratiche. Puoi sostenere che i tedeschi hanno ammazzato senza giustificazione un sacco di gente, è vero, ma l'hanno fatto in maniera burocratica. La Germania è così.

Julian: Se hai qualcuno che decide che cosa deve essere o non essere censurato allora devi avere due cose. Intanto devi allestire un'architettura tecnica per applicare la censura. Devi costruire una macchina censoria nazionale che lo faccia con efficienza. E poi devi avere una commissione e una burocrazia censoria. E la commissione deve essere intrinsecamente segreta perché sarà assolutamente inutile se non lo è, pertanto hai una giustizia segreta.

Andy: Sai una cosa? In Germania abbiamo un principio molto valido.

Jacob: Solo uno?

Andy: Il principio è che se non è realistico applicare una legge allora non dovrebbe esistere. Se una legge non ha senso, tipo che proibisci i mulini o cos'altro, allora noi diciamo "ehi, dai, lascia perdere". Noi qui siamo influenzati da Internet come la conoscevamo mentre cresceva, dal libero flusso di informazioni, libero nel senso di illimitato, non bloccato, non censurato, non filtrato. Così se applichiamo la nostra idea di libero flusso di informazioni al pianeta Terra, e più o meno è stata applicata all'intero pianeta Terra, naturalmente vediamo i governi influenzati da esso e dal modo in cui il potere è stato esercitato ed è stata gestita la censura, che sia precensura, postcensura o quant'altro. Abbiamo visto tutti i complessi conflitti che ne nascono. Il problema è qual è il nostro concetto di governo o qual è il futuro di una Organizzazione post-governativa (forse

WikiLeaks è la prima o una delle prime di queste opg) perché non sono tanto sicuro che i governi siano la risposta giusta a tutti i problemi di questo pianeta, come i temi ambientali.

JULIAN: Nemmeno i governi sono molto sicuri del confine tra cosa è o non è un governo. I governi occupano spazio, ma WikiLeaks occupa una parte dello spazio di Internet. Lo spazio di Internet è incorporato nello spazio reale, ma il livello di complessità tra l'oggetto incorporato e lo spazio in cui è inserito significa che non è facile per lo spazio dire che l'oggetto inserito ne fa parte. Insomma, è per questo che abbiamo una certa immagine del ciberspazio, cioè che sia un altro luogo che esiste da qualche parte, a causa del livello di complessità, universalità e non direzionalità. Quando leggi un file in Internet in un posto è uguale che leggerlo in un altro posto o in futuro. Questa è la sua universalità. Così a questo livello, come organizzazione che occupa il ciberspazio ed è impegnata a far girare le sue informazioni nel contenitore circostante, forse siamo un'organizzazione post-statuale a causa della carenza di controllo geografico.

Non voglio portare troppo oltre questa analogia perché mi trovo agli arresti domiciliari. La forza coercitiva degli stati ricade ovviamente su tutta la nostra gente, ovunque sia nota. Ma il resto della stampa ama dire che siamo un'organizzazione mediatica priva di stato e hanno abbastanza ragione sull'importanza di essere privi di stato. Io ero solito dire: "E allora, cosa credete che sia Newscorp? È una grossa multinazionale". Ugualmente Newscorp è strutturato in modo che tu puoi arrivare alle sue componenti chiave, ed è per questo che ha avuto tanti problemi qui nel Regno Unito con lo scandalo delle intercettazioni telefoniche e si danna tanto a blandire il potere Usa. Ma se gli asset di un'organizzazione sono principalmente le sue informazioni, allora può essere transnazionale e pertanto sarà abbastanza difficile fermarla grazie alla crittografia. C'è un motivo per l'embargo finanziario contro di noi: le altre facce della nostra organizzazione sono più difficili da reprimere.[15]

Jacob: Se vogliamo parlare in termini utopici, dobbiamo tornare indietro un tantino. Mi avete chiesto delle persecuzioni a cui sono stato sottoposto, della censura in Occidente, e poco fa ho accennato al programma di omicidi mirati di Obama, che sostengono essere legale perché c'è una procedura, pertanto conta come giusto processo.

Julian: Be', un processo segreto.

Jacob: Possiamo anche ricollegare la questione a John Gilmore. A un certo punto di uno dei processi di John Gilmore sulla possibilità di viaggiare in maniera anonima negli Stati Uniti la corte ha detto letteralmente: "Senta, andremo a consultare la legge, che è segretata. Leggeremo il codice e scopriremo, quando leggeremo questi provvedimenti segreti, se le è permesso fare le cose che le è consentito fare". E hanno scoperto quando hanno letto la legge segretata che in realtà gli era permesso farlo perché il dettato non lo limitava. Lui non ha mai saputo che cosa fosse questa legge segretata e in seguito hanno cambiato le *politiche* relative alla US Transportation Security Administration e del ministero della Sicurezza interna proprio come reazione alla causa vinta da lui, perché alla fine hanno scoperto che la legge segretata non era abbastanza limitante sotto questo aspetto.[16]

Julian: Quindi l'hanno resa più restrittiva?

Jacob: Infatti, attivando leggi burocratiche. Però è importante ricordare che il programma di omicidi mirati, le persecuzioni che deve subire la gente alla frontiera, la censura che troviamo online, la censura delle multinazionali per conto di un governo o di un'altra multinazionale, queste cose sono tutte collegate. E quello che abbiamo nella realtà è che lo stato ha troppo potere in ognuno dei posti in cui vediamo emergere queste cose. Succede perché il potere s'è concentrato in queste aree e ha attirato individui che ne abusano o che spingono per il suo utilizzo. E persino se certe volte ci sono utilizzi legittimi, vediamo che il mondo starebbe meglio se non ci fosse questa centralizzazione, se non ci fosse

la tendenza all'autoritarismo.

Sotto questo aspetto l'Occidente non è affatto speciale perché poi si scopre che se hai un mastino della cibersicurezza, be', non è poi tanto diverso dai mastini delle forze di sicurezza interne di un'altra nazione cinquant'anni fa. Stiamo costruendo lo stesso tipo di strutture autoritarie di controllo che attireranno le persone che ne abuseranno, ed è una cosa che facciamo finta possa essere diversa in Occidente. In Occidente non è diverso perché c'è un continuum nella governance, che va dall'autoritarismo al libertarismo. Non l'intendo nel senso del partito politico americano ma in questo senso: in questo continuum gli Stati Uniti sono molto lontani dall'Unione Sovietica sotto tanti, tanti aspetti ma sono assai più vicini all'Unione Sovietica di Christiania, il quartiere autonomo in piena Copenaghen, in Danimarca.[17] E sono ancora più distanti, credo, da un potenziale mondo utopico nel caso andassimo a creare una colonia nuova di zecca su Marte. Noi vorremmo tenere il più possibile lontano quello che costruiremo su Marte dal totalitarismo e dall'autoritarismo. È un problema quando non succede.

Jérémie: Ancora una volta tutti questi argomenti sono collegati. Quando parliamo di concentrazione del potere stiamo anche qui parlando di architettura. E quando parliamo di censura in Internet significa centralizzare il potere per decidere a cosa potrà accedere la gente, e se la censura del governo o anche dei privati è un potere indebito. Sentite questo esempio: il nostro sito web laquadrature. net è stato censurato in Gran Bretagna dalla Orange UK per parecchie settimane. Figurava in un elenco di siti web che la Orange escludeva a chi ha meno di diciotto anni. Forse avevamo citato il termine pornografia infantile quando ci opponevamo a quel genere di leggi, o forse semplicemente non gli stavamo simpatici perché siamo contrari alla loro politica contro la neutralità della rete, dato che chiediamo una legge che impedisca di discriminare le comunicazioni dei loro utenti.[18] Non lo sapremo mai. Però qui abbiamo un privato

che, come servizio, si stava offrendo di togliere alla gente la possibilità di accedere alle informazioni in Internet. In questo scorgo un grosso rischio oltre il potere che diamo a Orange o al governo cinese o ad altri.

Jacob: Precisazione: quando dici privato nel Regno Unito intendi che possiedono realmente ogni linea, ogni connessione via fibre e compagnia bella, oppure che utilizzano alcune risorse statali? Come sono state assegnate le licenze nell'etere? Non c'è alcun coinvolgimento dello stato? Non hanno un dovere di diligenza?

Jérémie: Ci sono state le assegnazioni delle licenze. Che sia il governo o un'impresa, stanno cambiando l'architettura di Internet da rete universale a una balcanizzazione in tante piccole sottoreti. Però quello di cui stiamo discutendo sin dall'inizio sono tutti temi globali, che parlassimo del sistema finanziario che va a ramengo, che parlassimo di corruzione, che parlassimo di geopolitica o di energia o di ambiente. Tutti questi sono problemi globali che oggi l'umanità deve affrontare, e abbiamo ancora per le mani uno strumento globale che consente migliori comunicazioni, maggiore condivisione della conoscenza, maggiore partecipazione ai processi politici e democratici. Temo che un'Internet universale globale sia l'unico strumento che abbiamo per risolvere questi problemi globali ed è per questo che la lotta per un'Internet libera è la lotta centrale che tutti dobbiamo combattere.

Andy: Sono assolutamente d'accordo sul fatto che dobbiamo garantire che Internet sia vista come rete universale con un libero flusso di informazioni, che non dobbiamo solo delineare molto bene questo ma anche smascherare quelle aziende e quei provider che forniscono una roba che chiamano Internet ma è in realtà qualcosa di totalmente diverso. Però mi sa che non abbiamo risposto alla domanda cruciale oltre questa storia del filtraggio. Voglio farvi un esempio di ciò a cui secondo me dovremmo dare una risposta. Alcuni anni fa, circa una decina, abbiamo protestato

contro la Siemens perché forniva il cosiddetto software di filtraggio “smart”. La Siemens è una delle più grosse aziende di telecomunicazione tedesche e un fornitore di software per la raccolta informazioni. E ha venduto questo sistema di filtraggio alle aziende perché, per esempio, i dipendenti non potessero guardare il sito dei sindacati per informarsi dei loro diritti come lavoratori eccetera. Ma hanno anche bloccato il sito del Chaos Computer Club, e questo ci ha fatto incazzare. Hanno parlato di “contenuti criminali” o qualcosa del genere, e per questo li abbiamo denunciati. Comunque durante una fiera abbiamo deciso di tenere una grande manifestazione di protesta circondando gli stand della Siemens e filtrando la gente che entrava e usciva. La cosa divertente è stata che l’abbiamo annunciato nel nostro sito per richiamare più gente possibile tramite Internet, e quelli dello stand Siemens non ne avevano il minimo schifoso sentore perché anche loro usavano il software di filtraggio pertanto non potevano leggere l’avvertimento che stava sotto gli occhi di tutti in rete.

JULIAN: Il Pentagono ha piazzato un sistema di filtraggio in modo che fossero bloccate tutte le e-mail inviate al Pentagono contenenti la parola WikiLeaks. E così nel processo a Bradley Manning la pubblica accusa, nel tentativo di portare avanti la causa, ha inviato e-mail su “WikiLeaks” a persone esterne alle cerchie militari ma non ha mai ricevuto le loro risposte perché contenevano la parola “WikiLeaks”.[19] Lo stato della sicurezza nazionale rischia di divorare se stesso.

ANDY: Il che ci riporta alla domanda veramente basilare: esiste una cosa come l’informazione con effetti negativi? Dal punto di vista della società, vogliamo un’Internet censurata perché è meglio per la società oppure no? Persino se parliamo di pornografia con minori potresti ribattere: “Un attimo, questa pornografia infantile evidenzia un problema, cioè l’abuso che si fa dei bambini, e se vogliamo risolvere il problema dobbiamo conoscere il problema”.

Jacob: Perché fornisce le prove del reato.

Julian: Be', no, fornisce una lobby.

Andy: Sarebbe l'approccio più radicale, ma se parliamo di nazisti o simili devi ancora spiegare di cosa stiamo parlando. Quelli con famiglia si chiederanno: "Mah, è meglio per la società filtrare le cose brutte in modo da mantenerci su solo quelle belle, o non significa limitare la nostra capacità di vedere i problemi e gestirli e affrontarli e risolverli?".

Jérémie: Credo che la soluzione giusta sia sempre diversa dalla censura. Quando parliamo di pornografia infantile non dovremmo nemmeno usare il termine pornografia, è una rappresentazione di scene criminali che prevedono l'abuso di minori. La cosa da fare è andare nei server, disabilitarli, identificare le persone che hanno caricato i contenuti per identificare chi ha prodotto i contenuti, chi ha abusato dei bambini. E ogni volta che trovi una rete di persone, una rete commerciale e simili, arrestare quella gente. E quando approviamo una legge, e ne abbiamo una in Francia che prevede un'autorità amministrativa del ministero dell'Interno che decide quali siti web saranno bloccati, eliminiamo l'incentivo per i servizi investigativi di andare a trovare la gente che fa roba brutta, dicendo invece "oh, noi togliamo solo l'accesso alla roba brutta", come se piazzando una mano sugli occhi di uno che guarda un problema avessimo risolto il problema. Pertanto, solo in questa ottica, penso che basti metterla così: che siamo tutti d'accordo che dovremmo togliere quelle immagini da Internet.

Jacob: Mi dispiace ma sto friggendo. È così innervosente sentire quello che dici. Mi vien da vomitare perché in pratica hai detto: "Voglio sfruttare la mia posizione di potere per affermare la mia autorità sulle altre persone, voglio cancellare la storia". Forse in questo sarò estremista, e di sicuro lo sono in tanti altri casi, ma sono disposto a mettermi in minoranza. È davvero un perfetto esempio di quando cancellando la storia fai un disservizio. Scopriamo che con

Internet abbiamo saputo che c'è nella società un'epidemia di abusi minorili. È quello che abbiamo imparato con questo problema della pornografia infantile (credo sarebbe meglio definirlo sfruttamento infantile), ne abbiamo visto le prove. Insabbiarlo, cancellarlo è, secondo me, un travisamento perché in realtà puoi imparare molto sulla società nel suo complesso. Per esempio, puoi imparare (e io ovviamente non avrò mai un futuro in politica dopo avere finito questa frase, ma solo per essere chiari)… per esempio, puoi imparare chi è che la produce, e sapere della gente che viene vittimizzata. Sarà impossibile per la gente ignorare il problema. Significa che devi iniziare a cercare la causa, chi lo crea, cioè chi sfrutta i bambini. Ironia della sorte, certe tecnologie della sorveglianza potrebbero venire utili con il riconoscimento facciale delle persone e guardando i metadati nelle immagini. Cancellare ciò, fare in modo di vivere in un mondo in cui è possibile cancellare certa roba e non altra, creare questi enti amministrativi di censura e controllo è una china scivolosa che, come abbiamo visto, ha portato direttamente al copyright, ha portato a molti altri sistemi.

Solo perché è una nobile causa da perseguire non dovremmo scegliere la soluzione facile, forse in realtà dovremmo cercare di risolvere i vari casi, forse dovremmo cercare di aiutare le vittime anche se questo tipo di aiuto ha un costo. Forse invece di ignorare il problema dovremmo accettare il fatto che la società nel suo complesso ha questo grosso problema che si manifesta in Internet in modo particolare.

Solo per fare un esempio, è come quando la Polaroid ha creato la fotocamera Swinger (la macchinetta per le foto istantanee) e la gente ha iniziato a scattare anche foto schifose. Però la risposta giusta non sta nel distruggere quel mezzo, o nel controllare quel mezzo. È invece quando trovi le prove per perseguire i crimini che quel mezzo ha documentato. Non sta nell'indebolire il mezzo, nell'azzoppare la società intera per questa storia. Visto che stiamo parlando di pedofili, parliamo anche della polizia. La polizia in tanti paesi abusa regolarmente della gente. Ci sono forse più

poliziotti marci in Internet che pedofili in Internet.

JULIAN: Sicuramente di più.

JACOB: Sappiamo che c'è un numero "n" di poliziotti nel mondo e sappiamo che c'è un numero "x" di poliziotti che hanno commesso violazioni dell'etica professionale, di solito violenze. Se guardiamo il movimento Occupy, per esempio, ne abbiamo la prova. Censureremo Internet perché sappiamo che qualche poliziotto è marcio? Azzopperemo la capacità della polizia di compiere un buon lavoro di polizia?

JULIAN: Be, c'è il problema della rivittimizzazione, cioè quando scopriamo che il minore, in seguito, o da adulto o nei suoi contatti sociali, rivede le immagini di abusi sui minori.

JACOB: Finché quegli sbirri sono online io vengo rivittimizzato.

JULIAN: Potresti sostenere che vedere un'immagine in cui sei picchiato da un poliziotto è una rivittimizzazione. Posso anche aggiungere che nel nostro mondo è più importante la tutela dell'integrità della storia di quanto è realmente successo; che la rivittimizzazione avviene, ma ugualmente impiantare un regime censorio capace di rimuovere pezzi di storia significa che non potremo affrontare il problema perché non possiamo vedere cos'è il problema. Negli anni novanta ho lavorato in una struttura di consulenza Internet per gli sbirri cacciatori di pedofili in Australia, la Victorian Child Exploitation Unit. Questi sbirri non erano contenti dei sistemi di filtraggio perché quando la gente non può vedere che esiste la pornografia infantile in Internet indebolisce la lobby che fa sì che gli sbirri ottengano i finanziamenti per fermare l'abuso di minori.

JÉRÉMIE: Il punto su cui sono d'accordo, e credo che sia il più importante, è che alla fine è la responsabilità individuale delle persone che creano i contenuti (i materiali con abuso di minori e cose del genere) a contare realmente, ed è su

questa che dovrebbero lavorare gli sbirri.

Jacob: Qui non siamo d’accordo. Non è quel che stavo dicendo.

Julian: No, Jérémie sta parlando di fare, non di pubblicare. C’è una differenza.

Jacob: In realtà il problema non è la produzione di contenuti. Solo una precisazione marginale: se, per esempio, hai abusato di un bambino e Andy l’ha fotografato come prova, non credo che Andy dovrebbe essere perseguito.

Jérémie: No, è gente che abusa. Dai, è favoreggiamento.

Andy: Però certa gente abusa dei bambini per produrre i filmati, no?

Jacob: Certo.

Andy: Potrebbe esserci anche un risvolto economico.

Jacob: Sono totalmente d’accordo. Sto solo facendo una distinzione, cioè che se il contenuto è un dato storico che è anche la prova di un crimine, allora è la prova di un crimine gravissimo, e non dovremmo mai perdere di vista il fatto che c’è una rivittimizzazione, ma c’è la vittimizzazione originaria ed è quella il vero nocciolo della questione, che ci siano o no le immagini.

Jérémie: Certo. È questo che intendo.

Jacob: È quasi irrilevante che ci siano o no le immagini. Quando ci sono è molto importante ricordare che devi tenere d’occhio la meta, e che la meta in realtà è fermare il danno, fermare gli abusi. In gran parte significa fare in modo che ci siano le prove e che ci sia un incentivo per la gente che ha gli strumenti giusti affinché risolva i crimini. Questo è incredibilmente importante, secondo me, e la gente tende a perdere di vista la cosa perché la scelta più facile è fingere

che non esista, e poi fermarlo e dire che così hanno fermato gli abusi. Mentre non è vero.

Andy: E il problema è che oggi tanta gente prediligerà ovviamente la soluzione facile perché è molto scomodo guardare cosa succede realmente nella società. Io penso che tu abbia la possibilità di risolvere un problema politico se non tenti di portare avanti una politica che ignori il problema o lo renda invisibile. In un certo senso potrebbe essere ciberpolitica, ma è anche questione di come una società gestisce i problemi, perciò ho forti dubbi che esista un'informazione che danneggi direttamente. Naturalmente c'entra qualcosa la capacità di filtrare, ed è anche vero che non voglio vedere tutte le immagini disponibili in Internet. Alcune le trovo davvero disgustose e distraenti, ma altrettanto vale per il videonoleggio all'angolo che propone film brutti e fasulli. Quindi la domanda è: ho la capacità di gestire quello che vedo e quello che elaboro e che leggo? Ed è l'approccio filtrante. Wau Holland, il fondatore del Chaos Computer Club, ha detto una cosa buffa: "Sai, il filtraggio dovrebbe essere fatto dall'utente finale, e nello strumento finale dell'utente finale".[20]

Julian: Quindi dovrebbe essere attuato dalla gente che riceve le informazioni.

Andy: Dovrebbe essere fatto qui. Qui! [indicando la propria testa]

Julian: Nel cervello.

Andy: Nello strumento finale dell'utente finale, cioè questa cosa che abbiamo in mezzo alle orecchie. È qui che dovresti filtrare, e non dovrebbe essere il governo a farlo per conto della gente. Se la gente non vuole vedere certe cose, be', non è tenuta, e di questi tempi ti si richiede di filtrare comunque un sacco di cose.

JULIAN: Andy, di recente m'è capitato di parlare con il presidente della Tunisia, e gli ho chiesto che cosa sarebbe stato degli archivi dei servizi d'informazione del regime del dittatore Ben Alì, l'equivalente tunisino degli archivi della Stasi. Lui ha risposto che, per quanto fossero interessantissimi, i servizi segreti sono un problema, sono pericolosi, e lui dovrà farli fuori uno per uno. Comunque per quanto riguarda gli archivi riteneva che la scelta migliore per la coesione della società tunisina fosse che rimanessero tutti segretati per non scatenare il gioco dell'attribuzione della colpa. Tu eri un ragazzo quando è crollata la Stasi in Germania Est. Puoi dirci qualcosa degli archivi della Stasi, e che cosa pensi di questa apertura degli archivi della sicurezza di stato?

ANDY: Forse la Germania ha l'agenzia spionistica più documentata del pianeta, o una delle prime. Tutti i documenti della Staatssicherheit della Germania Est, tutti i quaderni, le carte procedurali, i documenti di addestramento, le analisi interne, sono più o meno pubblici. Nel complesso significa che non è facile accedere a tutti, però a tanti sì, e il governo ha creato un'agenzia che gestisce gli archivi in modo che i cittadini tedeschi abbiano anche il diritto di consultare il loro dossier Stasi.

JULIAN: Il governo tedesco ha creato la BSTU (la Bundesbeauftragte für die Stasi-Unterlagen), il grande distributore dei dossier degli archivi Stasi.

Andy: Sì, e i giornalisti possono fare le cosiddette richieste di ricerca, forse equiparabili alle richieste per la libertà di informazione negli Stati Uniti, che gli permettono di studiare i materiali. E c'è un sacco di libri, e anche di manuali di apprendimento comportamentale strategico su come la Stasi faceva questo e quello. In realtà credo che sia una cosa positiva da cui imparare. Capisco che è un tantino troppo pretendere che i tunisini pubblichino tutti i dati personali che accumulava l'ex servizio di intelligence, perché il presidente, quello attuale, dovrà decidere sui suoi stessi dossier, e anche su quelli degli alleati eccetera. Queste agenzie di intelligence non rispettano la privacy, quindi avrai dei dossier privati sul tuo comportamento sessuale, le tue telecomunicazioni, i tuoi bonifici, tutto quello che hai fatto e forse non vuoi che si sappia in giro.

Julian: Hai seguito la vicenda della Amn El Dawla in Egitto, la sicurezza di stato interna? Migliaia di persone hanno saccheggiato gli archivi mentre l'Amn El Dawla tentava di bruciarli e distruggerli e buttarli nel pattume, e così sono uscite vagonate di materiale da diffondere in giro. Potevi comprare un dossier per due dollari al mercato locale e caricarlo in rete. Non ha distrutto la società egiziana.

Andy: No, sto solo dicendo che mi par di capire che la gente non vuole che siano diffusi i suoi dati personali. Lo comprendo, immagino come sarebbe se vivessi in un paese in cui hanno conservato su di me quarant'anni di informazioni riservate e ogni volta che vado al cesso vengo registrato.

Julian: Però c'è l'analisi costi-benefici, no? Da come la vedo io, se sei stato infame una volta sarai sempre un infame.

Andy: Giusto, ma la posizione etica degli hacker, a grandi linee, è usare le informazioni pubbliche e tutelare i dati o informazioni privati, e credo che se difendiamo la privacy, e abbiamo ottimi motivi per farlo, non dovremmo limitarci a dire che qui c'è un equilibrio tra le cose. Possiamo distinguere. Non dobbiamo avere tutto sbattuto in pubblico.

Jacob: Però questa segretezza ha un vantaggio asimmetrico. Facciamo un passo indietro. Tu parli essenzialmente da un punto di vista totalmente sbagliato, cioè il concetto che i dati siano privati quando sono ad accesso limitato, e non è vero. Per esempio, nel mio paese se un milione di persone ha un'autorizzazione che gli consente l'accesso a questi dati privati...

Julian: 4,3 milioni...

Jacob: Come fai a definire privati questi dati? Il problema è che non è realmente segreto al 100% a tutti gli abitanti del pianeta.

Julian: È segreto per gli indifesi e non per i potenti.

Andy: Sì, hai ragione. Ma se vogliamo aprire interamente l'archivio...

Julian: È successo in certi paesi europei.

Andy: No, non conosco un solo paese in cui tutti gli archivi siano stati aperti.

Julian: I dati sono stati divulgati più che in Germania. In Polonia, per esempio.

Andy: Possibile. In realtà è successo questo, la faccia brutta dell'accordo fatto in Germania: hanno usato gli ex funzionari della Sicurezza di stato della Germania Est in modo che fosse la Stasi a gestire non solo gli archivi della Stasi ma anche una porzione della cosiddetta "Nuova Germania", l'ex parte orientale unificata. C'è una storiella interessante su un'azienda che aveva vinto il pubblico appalto per pulire il palazzo in cui conservavano gli archivi. Questa ditta vinse la gara solo perché aveva fatto l'offerta più bassa per quel servizio rispetto alla concorrenza. Dopo sei anni l'organizzazione che conservava i materiali scoprì di avere ingaggiato una ditta costituita dagli ex servizi della Germania

Est per ripulire i propri dati.

Jérémie: Su WikiLeaks c'era un rapporto su questa storia. L'ho letto. Era fantastico.[1]

Andy: WikiLeaks ha pubblicato il rapporto che parlava esattamente di questa storia, perciò hai ragione: una volta che questi dati sono stati creati e sono nelle mani dei cattivi è dura affermare che esiste la privacy.

Julian: Possiamo passare a un tema più ampio. Internet ha portato a un'esplosione della quantità di informazioni disponibili al pubblico. È straordinario. La funzione pedagogica è straordinaria. D'altro canto la gente parla di WikiLeaks e dice: "Senti, adesso tutte queste informazioni statali riservate sono pubbliche, il governo non può più tenere segreto alcunché". Io dico che è una scemenza. Dico che WikiLeaks è l'ombra di un'ombra. In realtà il fatto che abbiamo fornito migliaia di cartelle di informazioni e le abbiamo date al pubblico è funzione dell'enorme esplosione della quantità di materiale segreto che c'è in giro. In realtà i gruppi di potere hanno ormai una così grande quantità di materiali segreti che ridicolizza la quantità di materiale disponibile al pubblico, e le divulgazioni di Wiki-Leaks sono solo una frazione del materiale conservato in mani private. Quando rifletti su questo equilibrio tra insider potenti che sanno di ogni transazione con carta di credito al mondo da un lato, e dall'altro la gente che può cercare su Google i blog del mondo e i commenti, come lo vedi questo equilibrio?

Andy: Potrei rispondere che va bene se tutti questi dati vengono svelati perché la gente imparerà che quando usa la carta di credito lascia una traccia. Certa gente, se glielo spieghiamo, lo troverà difficilissimo da capire, molto astratto. Ma nel momento in cui leggerà i propri dati capirà.

Julian: Appena vedi i tuoi dati su Facebook, che ha su di te 800 mega di informazioni.

Andy: So che dopo la caduta del blocco sovietico, quando il cancelliere tedesco Helmut Kohl voleva unificare la Germania, gli americani imposero una condizione all'interno dei cosiddetti colloqui 2+4, dicendo che volevano mantenere il controllo delle telecomunicazioni tedesche, mantenerlo sotto la loro sorveglianza, e Kohl riteneva che non fosse importante perché non capiva che cos'è la sorveglianza delle telecomunicazioni. Ho parlato con qualcuno della sua squadra. Sostenevano di essere davvero sconvolti. Alla fine fecero in modo di procurarsi tipo ottomila pagine di trascrizioni delle sue telefonate fatte dalla Stasi e che gli fossero recapitate su due carrelli in ufficio. Allora Kohl chiese che diavolo era. Loro: "Oh, sono le sue telefonate degli ultimi dieci anni, comprese quelle con le amichette e sua moglie e la segretaria eccetera". In questo modo gli fecero capire che cosa sono le intercettazioni. E infatti questi dati dei servizi d'informazione aiutano la gente a capire che cosa combinano i servizi. Pertanto possiamo anche sostenere l'apertura completa, e se dovessimo votare adesso non sono sicuro che sarei realmente contrario.

Julian: Non voglio parlarne a lungo, dato che ci sono ovviamente dei casi in cui indaghi la mafia e in cui durante l'inchiesta devi tenere riservati i materiali. Ci sono circostanze in cui può essere considerato legittimo. Non sto dicendo che come politica sia legittima, sto dicendo che è politicamente inevitabile. Ci sono esigenze politicamente cogenti, tipo "quei tizi hanno già ammazzato, stanno tramando un altro omicidio", che ti spingono alle intercettazioni, che tu pensi o meno che dovrebbero essere permesse. Non puoi vincere questa battaglia politica. Però questo tipo di sorveglianza tattica ha il vantaggio che può essere parzialmente regolato e che il danno può essere confinato a un numero minimo di persone. Quando usano l'intercettazione tattica per la tutela dell'ordine (in quanto opposta all'intelligence) spesso fa parte della raccolta delle prove. La prova finisce nel processo e perciò diventa pubblica. Così hai una supervisione, almeno per parte del

tempo, di quello che succede. E puoi interrogare in aula per sapere come sono state raccolte queste informazioni e perché dovremmo dare per scontato che sono valide. Puoi tenere d'occhio la faccenda. Però regolamentare le intercettazioni strategiche è totalmente assurdo. Per definizione significa intercettare tutti, perciò quali leggi fai valere se la premessa è intercettare tutti?

JÉRÉMIE: Questo dibattito sulla trasparenza totale mi fa venire in mente il gruppo noto come LulzSec, che ha diffuso settanta milioni di registrazioni della Sony, tutti i dati degli utenti della Sony, di modo che potevi vedere nomi, indirizzi di e-mail e password. Credo che ci fossero persino i dettagli delle carte di credito di settanta milioni di utenti. In quanto militante per i diritti di base ho pensato: "Uau, c'è qualcosa di sbagliato se per dimostrare la tua tesi o per divertirti riveli i dati personali della gente". È stato molto fastidioso vedere gli indirizzi di e-mail della gente. Quelle persone, secondo me, si stavano divertendo con la sicurezza informatica, e volevano dimostrare che un'azienda famosa e potente come la Sony non poteva tenere segreti i suoi dati sugli utenti, e se quei settanta milioni di utenti avessero cercato in un motore di ricerca il loro indirizzo di posta elettronica o il loro nome e avessero trovato questi dati gli avrebbe fatto capire di colpo: "Ehi, che ho combinato quando ho rivelato questi dati alla Sony? Che significa dare i dati personali a un'impresa?".

JACOB: Poi sparano all'ambasciator che porta pena.

Julian: Abbiamo passato in rassegna tutti questi scenari pessimisti, perciò adesso vorrei parlare di un potenziale scenario utopico. Da un lato abbiamo la radicalizzazione della gioventù internettiana, e adesso la gioventù di Internet sta per diventare la maggioranza dei giovani. Di contro abbiamo i disperati tentativi di colpire l'anonimizzazione e le libertà di pubblicazione, la libertà dalla censura, con una lunga serie di interazioni fra lo stato e il settore privato che le sono ostili. Comunque diamo per scontato che infileremo la rotta più positiva. Secondo voi che aspetto ha?

Jacob: Credo che ci serva il diritto di leggere e di parlare liberamente senza eccezioni per ogni singolo individuo, nessun essere umano escluso, senza la minima eccezione, per parafrasare Bill Hicks.[1] Lui ne parlava a proposito dell'istruzione, dei vestiti e del cibo, ma alla fine si riduce a questo: tutti hanno il diritto di leggere, tutti hanno il diritto di parlare liberamente. Questo comporta il diritto al discorso anonimo, la possibilità di pagare la gente in modo che non ci sia interferenza di terzi, la capacità di viaggiare liberamente, la capacità di correggere i dati su di te nei sistemi. Avere trasparenza e obbligo di rendiconto per qualsiasi sistema in cui vediamo una qualche specie di ente o organismo.

Andy: Io aggiungerei l'idea che con l'aumento dei sistemi di elaborazione delle informazioni e dell'aspetto di rete di questa situazione, e con la disponibilità di strumenti come Tor e la crittografia eccetera, la quantità di dati che può essere soppressa è abbastanza bassa, cioè i governi devono fare

soltanto questo, e lo sanno. Sanno che agire in segreto in questi giorni significa soltanto agire in segreto per un certo lasso di tempo, prima o poi tutto sarà sottoposto allo scrutinio dell'opinione pubblica, ed è una bella cosa. Questo cambia il loro comportamento. Significa che sanno di dover rendere conto. Significa anche che in realtà facilitano quelli che cantano nelle indagini, come con la legge Sarbanes-Oxley che richiede alle aziende quotate presso la borsa statunitense di dotarsi di un'infrastruttura per le soffiate in modo che chi ha bisogno di riferire un comportamento criminale o comunque scorretto dei superiori possa aver modo di farlo senza essere influenzato direttamente da quelli su cui riferisce.[2] Quindi è una cosa positiva e porterà a processi più sostenibili nel lungo termine.

Jérémie: Per aggiungere una cosa a quello che ha appena detto Jake, credo che dovremmo chiarire a tutti che un'Internet libera, aperta e universale è forse lo strumento più importante che abbiamo per affrontare i problemi globali che sono in ballo, che proteggerla è forse uno dei compiti più essenziali per la nostra generazione, e che quando qualcuno da qualche parte, che sia un governo o un'azienda, limita la capacità di accedere all'Internet universale, ne viene colpita l'intera Internet. Viene limitata l'umanità intera. Stiamo vedendo con i nostri occhi che possiamo aumentare collettivamente il costo politico di questa decisione, e che tutti i cittadini che accedono a un'Internet libera possono intralciare questo comportamento. Stiamo iniziando a vedere che come cittadini della rete esercitiamo un potere sulle decisioni politiche e possiamo indurre a una maggiore trasparenza i nostri rappresentanti eletti e i nostri governi in ciò che fanno quando prendono decisioni sbagliate che toccano le nostre libertà fondamentali e influenzano un'Internet globale libera e universale.

Perciò penso che dovremmo esercitarci in questo. Dovremmo continuare a condividere il sapere pratico. Dovremmo continuare a migliorare i nostri modi di agire, come ci passiamo le tattiche relative ai rapporti con il

parlamento, come si fa a portare alla luce quello che combinano gli uomini politici, come smascherare l'influenza delle lobby industriali e delle procedure politiche. Dovremmo continuare a costruire strumenti che facilitino ai cittadini la costruzione di infrastrutture decentrate crittate, il possesso di una propria infrastruttura comunicativa. Dovremmo promuovere queste idee presso l'intera società come modo per costruire un mondo migliore, e in realtà stiamo iniziando a farlo. Dobbiamo solo andare avanti così.

JULIAN: Jake, se pensi a persone come Evgeny Morozov, alla sua descrizione dei problemi di Internet, capisci che questi temi sono stati affrontati tempo fa dai cypherpunk.[3] Non era solo una lamentela sul nascente stato della sorveglianza eccetera, ma l'affermazione che possiamo, anzi, dobbiamo costruire gli strumenti di una nuova democrazia. Possiamo davvero costruirli con la nostra mente, distribuirli agli altri e avviare la difesa collettiva. La tecnologia e la scienza non sono neutrali. Ci sono forme particolari di tecnologia che possono darci questi diritti e queste libertà fondamentali a cui tanta gente aspira da tanto tempo.

JACOB: Certo. Credo che la chiave che la gente dovrebbe acquisire, soprattutto un sedicenne o diciottenne che desidera poter fare del mondo un posto migliore, è che nessuno seduto qui o altrove nel mondo è nato con i risultati che alla fine saranno scolpiti sulla sua lapide. Tutti costruiamo alternative. Tutti qui hanno costruito alternative e tutti, soprattutto con Internet, hanno la facoltà di farlo per il contesto in cui vivono. E non è che hanno il dovere di farlo, diciamo piuttosto che, se desiderano farlo, possono. E se lo fanno influiranno su tante persone, soprattutto per quanto riguarda Internet. Costruire quelle alternative innesca un'amplificazione, un allargamento.

JULIAN: Cioè, se costruisci qualcosa solo per te dopo puoi darlo a un miliardo di persone perché lo utilizzino.

JACOB: O se partecipi alla costruzione di una rete di

anonimato, come per esempio la rete di Tor, contribuisci a costruire l'alternativa della comunicazione anonima dove prima non esisteva.

Jérémie: Significa condividere liberamente questa conoscenza e favorire canali di comunicazione perché il sapere scorra liberamente, ed è quello che stai facendo. Tor è un software libero e gratuito, e oggi è così diffuso perché inseriamo questa idea di libertà nel modo in cui costruiamo alternative e costruiamo tecnologia e costruiamo modelli.

Jacob: Ci serve il software libero per un mondo libero, e ci serve un hardware libero e aperto.

Julian: Ma con libero intendi senza limitazioni, in cui la gente può gingillarsi con gli ingranaggi, vedere come funziona?

Jacob: Sicuramente. Ci serve un software libero come le leggi in una democrazia, che tutti possano studiare, cambiare, capire realmente e fare in modo che faccia quello che si augurano che faccia. Software Libero, Hardware Libero e Aperto.[4]

Julian: Avevano mutuato dai cypherpunk il concetto che "codice è legge".

Jérémie: Viene da Larry Lessig.

Julian: In Internet quello che puoi fare è deciso dai programmi che esistono, dai programmi che girano, e pertanto il codice è legge.

Jacob: Certo, e significa che puoi costruire alternative, soprattutto in termini di programmazione ma anche in termini di stampa 3D o cose sociali come gli spazi hacker esistenti.[5] Puoi aiutare a costruire alternative, e la cosa essenziale è inserirle per bene in un processo di normalizzazione in cui la gente diventi socialmente abituata a

costruire i propri oggetti tridimensionali, a modificare il proprio software, e in cui sia consapevole che se qualcuno le impedisce di farlo allora chiunque sia a impedire non sta fornendo accesso a Internet ma a Censornet o Filternet, e in realtà sta violando il proprio dovere di diligenza.

È quello che ognuno di noi ha fatto in vita sua, e la gente dovrebbe sapere che può farlo per le future generazioni, e per questa generazione adesso. È per questo che sono qui, perché se non appoggio Julian adesso, nelle cose che sta passando, che razza di mondo sto costruendo? Che razza di messaggio mando se lascio che una ghenga di maiali mi maltratti? Non esiste, mai. Dobbiamo costruire e dobbiamo cambiare questa situazione. Come diceva Gandhi: "Devi essere tu il cambiamento che vuoi vedere nel mondo", ma devi essere anche il guaio che vuoi vedere nel mondo.[6] È una frase che viene da *A Softer World*, un webfumetto, non è l'esatta citazione di Gandhi, ma credo che la gente debba sapere che non può rimanere inerte, che deve attivarsi, e si spera che lo faccia.[7]

Andy: Mi pare che ci siano buone possibilità che le persone possano superare il punto in cui ci troviamo adesso, e che le alternative vengano dalla gente insoddisfatta dalla situazione che trova o dalle opzioni che ha.

Julian: Potresti parlarci un po' del Chaos Computer Club in questo contesto?

Andy: Sempre il ccc… fnord.[8]

Julian: In realtà è una cosa unica al mondo.

Andy: Il ccc è un'organizzazione hacker galattica per promuovere la libertà d'informazione, la trasparenza della tecnologia, e studia le relazioni tra sviluppo umano e tecnologico, perché la società e lo sviluppo interagiscano.

Julian: È diventata una faccenda politica.

Andy: Il ccc è diventato un forum della scena hacker con alcune migliaia di soci in buona parte in Germania, ma non ci vediamo come residenti in Germania, ci consideriamo residenti in Internet, che è forse una grossa parte della nostra immagine, e anche della nostra attrattiva. Siamo molto ben collegati ad altri gruppi hacker in Francia, America e altri posti.

Julian: E perché è cominciato in Germania, secondo te? Il cuore è in Germania, poi s'è allargato nel resto del mondo.

Andy: I tedeschi cercano sempre di organizzare tutto.

Jérémie: L'ingegneria tedesca è la migliore.

Julian: Però non credo che sia solo questo. È perché sta a Berlino, ed è successo a causa del crollo dell'Est.

Andy: C'entrano fattori diversi. La Germania ha fatto le cose peggiori che un paese può infliggere agli altri, perciò è forse un tantino immune alla possibilità di ripeterle, tipo scatenare una guerra contro altri paesi. L'abbiamo fatto, ci siamo già passati, siamo stati puniti duramente e abbiamo dovuto imparare, e questa mentalità decentrata e antifascista, per evitare per esempio uno stato totalitario, è ancora insegnata nelle scuole tedesche perché l'abbiamo provato nella maniera peggiore. Credo che questo aiuti a capire il ccc, che è un po' un fenomeno tedesco. Wau Holland, il fondatore del ccc, ha impresso anche una connotazione fortemente politica. Ho visto suo padre accanto alla sua tomba, la tomba del figlio morto prima di lui, e non ha avuto parole molto tenere, per esempio: "…e non ci saranno mai più attività totalitarie, non pacifiche in territorio tedesco". È stato il commento di suo padre mentre seppelliva il figlio, e mi ha fatto capire come mai Wau era tanto impegnato a influenzare e prendersi cura della gente, nelle sue attività pacifiste, perché diffondeva idee e non le limitava mai e non si comportava in modo aggressivo, ma collaborante.

L'idea di creare le cose in collaborazione, come i movimenti

open source eccetera, è stata contagiosa e combaciava con le idee dei cypherpunk americani e di Julian Assange/WikiLeaks e così via. Oggi è una cosa globale che s'è messa in moto, che vede atteggiamenti culturali molto diversi, molto decentrati, degli hacker svizzeri, tedeschi, italiani, ed è bello. Gli hacker italiani si comportano in modo totalmente diverso dai tedeschi, dovunque siano hanno bisogno di mangiare bene. Gli hacker tedeschi hanno bisogno di avere tutto organizzato al bacio. Non sto dicendo che questi siano meglio di quelli, sto solo dicendo che ciascuna di queste strutture decentrate ha le sue parti molto belle. Al convegno degli hacker italiani puoi andare in cucina e trovare un posto meraviglioso, nel campo hacker tedesco vedrai un'Internet stupenda ma è meglio se non metti piede in cucina. Comunque il succo della faccenda è che stiamo creando. E a parer mio ci troviamo situati in una specie di coscienza comune totalmente distinta dalla nostra identità nazionale, dall'essere tedeschi o italiani o americani o altro, sappiamo solo che vogliamo risolvere i problemi, che vogliamo lavorare insieme. Per noi questa censura di Internet, questa guerra dei governi alla nuova tecnologia è una forma di crisi evolutiva che dobbiamo superare.

Siamo sulla strada giusta per individuare le soluzioni e non solo i problemi, ed è una cosa positiva. Probabilmente dovremo ancora combattere un sacco di schifezze per i prossimi non so quanti anni, ma ora finalmente sta nascendo una generazione di politici che non considerano Internet il nemico ma capiscono che fa parte della soluzione e non del problema. Abbiamo ancora un mondo costruito sulle armi, sul potere della conservazione del segreto, su un'intera struttura economica eccetera, ma sta cambiando e credo che in questo momento noi siamo molto importanti nell'impostazione della politica. Possiamo discutere i problemi litigando, e in realtà è una cosa che il CCC ha fatto per tanti anni. Non siamo un gruppo omogeneo, abbiamo opinioni molto diverse. Mi fa piacere vedere che siamo qui seduti insieme e non abbiamo le risposte giuste pronte all'uso, tiriamo fuori solo domande e sbattiamo sul tavolo le idee diverse per vedere a cosa si

arriva. È questo il processo che deve proseguire, ed è per questo che ci serve Internet libera.

JULIAN: Ho chiesto come vi sembra la rotta più positiva per il futuro. Autocoscienza, diversità e reti di autodeterminazione. Una popolazione globale istruita, non intendo nel senso dell'educazione formale ma edotta di come funziona la civiltà umana a livello politico, industriale, scientifico e psicologico, come esito del libero scambio di comunicazioni, stimolando anche nuove culture vivaci e la massima diversificazione del pensiero individuale, l'accresciuta autodeterminazione regionale e l'autodeterminazione dei gruppi di pressione che saranno capaci di creare velocemente reti e trasferire valore rapidamente oltre i confini geografici. E forse questo è stato espresso nella Primavera araba e nell'attivismo panarabo che sono stati potenziati da Internet. Nel nostro lavoro con Nawaat.org, che ha creato Tunileaks, facendo filtrare i cablo del Dipartimento di stato oltre la censura del regime nella Tunisia prerivoluzionaria, abbiamo visto con i nostri occhi il potere terrificante della rete quando si tratta di far arrivare informazioni là dove servono, ed è stato tremendamente gratificante essere stati in condizione, grazie ai nostri sforzi, di contribuire a quello che sta iniziando ad accadere da quelle parti.[9] Non vedo quella lotta per l'autodeterminazione come distinta dalla nostra.

Questa traiettoria positiva comporterebbe inoltre l'autocoscienza della civiltà umana perché il passato non può essere distrutto. Significherebbe l'impossibilità pratica che nascano gli stati neototalitari a causa del libero movimento delle informazioni, della capacità della gente di parlarsi in privato e cospirare contro queste tendenze, e della capacità del microcapitale di spostarsi senza controlli dai posti inospitali per gli esseri umani.

Su queste basi puoi costruire un'ampia gamma di sistemi politici. La mia utopia potrebbe diventare una distopia se fosse soltanto una, la mia. Credo che gli ideali utopici debbano significare la diversità dei sistemi e dei modelli di interazione. Se guardiamo lo sviluppo tumultuoso dei nuovi

prodotti culturali e persino la deriva del linguaggio, e le sottoculture che creano i propri meccanismi di interazione potenziati da Internet, allora sì, posso vedere che inaugura sul serio questo possibile tragitto positivo.

Ma credo che con tutta probabilità le tendenze all'omogeneizzazione, all'universalità, all'intera civiltà umana trasformata in un unico mercato, significhino che avrai normali fenomeni di mercato come il leader del mercato stesso, un secondo e un terzo protagonista di nicchia, e poi i fanalini di coda che non fanno la minima differenza per ogni servizio e prodotto. Credo che forse significherà una poderosa omogeneizzazione del linguaggio, una poderosa omogeneizzazione culturale, una poderosa standardizzazione per rendere efficienti questi rapidi interscambi. Perciò penso che sia anche abbastanza probabile l'alternativa pessimista, e che lo stato transnazionale della sorveglianza e le infinite guerre dei droni siano praticamente la realtà che incombe su di noi.

Mi viene in mente la sera che mi sono intrufolato nella Opera House di Sydney per vedere il *Faust*. L'Opera House di Sydney è molto bella di sera, i suoi vasti spazi interni e le luci scintillano sull'acqua e contro il cielo notturno. Quando sono uscito ho sentito tre donne che discutevano appoggiate alla ringhiera che si affacciava sulla baia buia. La più anziana stava parlando dei suoi problemi al lavoro, che poi significava essere agente della CIA. S'era lamentata presso la Commissione ristretta del Senato eccetera, e adesso ne parlava sottovoce con la nipote e con un'altra signora. Ho pensato: "Allora è vero. Gli agenti della CIA frequentano sul serio l'opera di Sydney!". Poi ho guardato dentro il teatro d'opera dalle immense vetrate sul davanti, e in quel deserto lusso principesco ho visto una pantegana intrufolata all'interno dell'Opera House, che zampettava avanti e indietro e balzava sui tavoli coperti di lini finissimi per divorare le cibarie, saltava sul bancone con tutti i biglietti e se la spassava. Credo che sia il più probabile scenario per il futuro: una struttura totalitaria estremamente chiusa, omogeneizzata, postmoderna, transnazionale con incredibili

complessità, assurdità e schifezze, e dentro questa incredibile complessità uno spazio in cui possono intrufolarsi solo i topi furbi.

È una deviazione positiva nella traiettoria negativa, essendo quest'ultima lo stato transnazionale della sorveglianza, costellato di droni, il neofeudalesimo in rete dell'élite transnazionale, non in senso classico bensì in quanto complessa interazione multipartitica sorta come risultato di varie élite nelle proprie nazioni che affiorano assieme, al di sopra delle rispettive basi demografiche, e si fondono. Tutte le comunicazioni saranno sorvegliate, perennemente registrate, perennemente tracciate, ogni individuo nelle sue interazioni perennemente identificato per questo nuovo Potere come il tale individuo, dalla culla alla tomba. È una mutazione importante persino rispetto a dieci anni fa, e praticamente già ci siamo. Io penso che potrà solo produrre un habitat di controllo soffocante. Se tutte le informazioni raccolte sul mondo fossero pubbliche, questo potrebbe riequilibrare la dinamica del potere e lasciarci la possibilità di plasmare il nostro destino, come civiltà globale. Ma senza un cambiamento spettacolare non succederà. La sorveglianza di massa colpisce tanti di noi in maniera sproporzionata, trasferendo il potere a coloro che sono interni al progetto. Ciononostante, credo, non si godranno nemmeno loro questo nuovo mondo. Questo sistema coinciderà anche con la corsa alle armi telecomandate che elimineranno i confini ben definiti come li conosciamo, dato che questi confini sono prodotti dalla contesa sugli spartiacque fisici, sfociando in uno stato di guerra perpetua a mano a mano che le reti di influenza vincenti inizieranno a spremere il mondo per strappare concessioni. E nel frattempo la gente finirà sepolta sotto l'impossibile matematica della burocrazia.

Come può essere libera una persona normale entro questo sistema? Semplicemente non può, è impossibile. Non che si possa mai essere totalmente liberi entro qualsiasi sistema, però le libertà per cui ci siamo evoluti biologicamente e le libertà a cui ci siamo abituati culturalmente saranno

eliminate quasi del tutto. Perciò credo che le uniche persone che riusciranno a conservare la libertà che avevamo, che so, vent’anni fa, perché lo stato della sorveglianza ne ha già eliminata un sacco, solo che ancora non l’abbiamo capito, siano quelle fortemente consapevoli degli ingranaggi di questo sistema. Perciò sarà libera soltanto un’élite di ribelli hi-tech, gli astuti topi che scorrazzeranno dentro il teatro d’opera.

Note

Nota del curatore

[1] Detto in modo semplice, la crittografia, dal sostantivo greco che sta per “scrittura segreta”, è la pratica della comunicazione in codice.

[2] *Oxford English Dictionary Updates Some Entries & Adds New Words; Bada-Bing, Cypherpunk, and Wi-Fi Now in the OED*, in “ResourceShelf”, 16 settembre 2006: web.resourceshelf.com (accesso 24 ottobre 2012).

I partecipanti alla discussione

[1] WikiLeaks: wikileaks.org.

[2] Sul Rubberhose file system vedi: *The Idiot Savants' Guide to Rubberhose*, Suelette Dreyfus: marutukku.org (accesso 14 ottobre 2012).

[3] Per saperne di più sul libro *Underground*, vedi: www.underground-book.net. Sul film *Underground: The Julian Assange Story*, vedi Internet Movie Database: www.imdb.com (accesso 21 ottobre 2012).

[4] Noisebridge è uno spazio hacker di San Francisco che fornisce infrastrutture per i progetti tecnico-creativi, gestito collettivamente dai suoi membri: www.noisebridge.net. Il Chaos Computer Club Berlino è il ramo berlinese del Chaos Computer Club (vedi sotto): berlin.ccc.de.

[5] Tor Project: www.torproject.org.

[6] Il Chaos Computer Club è la più grossa struttura hacker in Europa. Le sue attività spaziano dalle ricerche ed esplorazioni tecniche a campagne, eventi, pubblicazioni e consulenze politiche: www.ccc.de.

[7] EDRI: www.edri.org.

[8] ICANN: www.icann.org.

[9] Buggedplanet: buggedplanet.info.

[10] Cryptophone: www.cryptophone.de.

[11] La Quadrature du Net: www.laquadrature.net.

Nota sui vari tentativi di molestare WikiLeaks e le persone a essa associate

[1] Collateral Murder: www.collateralmurder.com. The Iraq War Logs: wikileaks.org/irq. The Afghan War Diary: wikileaks.org/afg. Cablegate: wikileaks.org/cablegate.html.

[2] *Congressional Committee Holds Hearing on National Security Leak Prevention and Punishment*, Reporters Committee for Freedom of the Press, 11 luglio 2012: www.rcfp.org (accesso 21 ottobre 2012).

[3] Per ulteriori informazioni sul gran giurì di WikiLeaks, vedi timeline della giornalista freelance Alexa O'Brien: www.alexaobrien.com (accesso 22 ottobre 2012).

[4] *Bradley Manning's Treatment Was Cruel and Inhuman, UN Torture Chief Rules*, in “Guardian”, 12 marzo 2012: www.guardian.co.uk (accesso 24 ottobre 2012).

[5] *Wikileaks, Guilty Parties “Should Face Death Penalty”, in* “Telegraph”, 1 dicembre 2010:

www.telegraph.co.uk (accesso 22 ottobre 2012).

[6] *CIA Launches Task Force to Assess Impact of U.S. Cables' Exposure by WikiLeaks*, in "Washington Post", 22 dicembre 2010: www.washingtonpost.com (accesso 22 ottobre 2012).

[7] *WikiLeaks Fights to Stay Online after US Company Withdraws Domain Name,* in "Guardian", 3 dicembre 2010: www.guardian.co.uk (accesso 23 ottobre 2012).

[8] *Don't Look, Don't Read: Government Warns Its Workers Away from WikiLeaks Documents*, in "New York Times", 4 dicembre 2010: www.nytimes.com (accesso 23 ottobre 2012).

[9] *Banking Blockade,* Wikileaks: www.wikileaks.org (accesso 22 ottobre 2012).

[10] Il resoconto scritto di Jacob delle sue detenzioni è una lettura raccomandata. Vedi *Air Space – A Trip Through an Airport Detention Center*, boingboing, 31 ottobre 2011: boingboing.net. Importante è anche un'intervista a Jacob sulle detenzioni su "Democracy Now": *National Security Agency Whistleblower William Binney on Growing State Surveillance*, 20 aprile 2012: www.democracynow.org (accesso a entrambi i link 23 ottobre 2012).

[11] Il caso è ufficialmente noto come In the Matter of the 2703(d) Order Relating to Twitter Accounts: WikiLeaks Rop_G IOERROR; and BirgittaJ.

[12] *Secret Orders Target Email*, in "Wall Street Journal", 9 ottobre 2011: www.online.wsj.com (accesso 22 ottobre 2012).

[13] *Twitter Ordered to Yeld Data in WikiLeaks Case*, "New York Times", 10 novembre 2011, www.nytimes.com (accesso 22 ottobre 2012).

[14] *ACLU & EFF to Appeal Secrecy Ruling in Twitter/WikiLeaks Case*, comunicato stampa Electronic Frontier Foundation, 20 gennaio 2012: www.eff.org (accesso 22 ottobre 2012).

Aumento delle comunicazioni contro aumento della sorveglianza

[1] Era la protesta del 6 aprile 2008 in appoggio allo sciopero soppresso dei lavoratori tessili di Mahalla al-Kobra. Poco prima dello sciopero era stato creato il "Movimento 6 aprile" come gruppo Facebook concepito per spingere gli egiziani a tenere manifestazioni al Cairo e altrove in contemporanea con la protesta di fabbrica a Mahalla. La manifestazione non è andata come previsto, e gli amministratori del gruppo Facebook, Esraa Abdel Fattah Ahmed Rashid e Ahmed Maher, sono stati arrestati con altri. Maher è stato torturato per strappargli la sua password Facebook. Il Movimento giovanile 6 aprile ha svolto un ruolo nella rivoluzione egiziana del 2011. Vedi *Cairo Activists Use Facebook to Rattle Regime*, in "Wired", 20 ottobre 2008: www.wired.com (accesso 23 ottobre 2012).

[2] *How to Protest Intelligently*, autori anonimi (in arabo), distribuito all'inizio della rivolta di diciotto giorni che ha rovesciato il presidente Mubarak: www.itstime.it. Gli estratti del documento sono stati tradotti in inglese e pubblicati come *Egyptian Activists' Action Plan: Translated*, in "Atlantic", 27 gennaio 2011, www.theatlantic.com (accesso a entrambi i link 23 ottobre 2012).

[3] Il Panopticon era un carcere immaginato dal filosofo Jeremy Bentham nel 1787, progettato per permettere ai secondini di sorvegliare di nascosto tutti i detenuti in contemporanea grazie alla visibilità totale. Jeremy Bentham (a cura di Miran Bozovic), *The Panopticon Writings*, Verso, 1995, reperibile online presso: cartome.org (accesso 22 ottobre 2012).

[4] Johannes Gutenberg (1398-1468) era un fabbro tedesco che inventò la stampa meccanica a caratteri mobili, un'invenzione che generò il più significativo sommovimento sociale della storia. L'invenzione della stampa è il parallelo storico più vicino all'invenzione di Internet.

[5] John Gilmore è uno dei primi cypherpunk e uno dei fondatori della Electronic Frontier Foundation, impegnato a difesa delle libertà civili. La frase citata da Andy è stata riportata la prima volta in *First Nation in Cyberspace*, in "Time Magazine", 6 dicembre 1993. Vedi il sito di John Gilmore: www.toad.com/gnu (accesso 22 ottobre 2012).

[6] "Le tecnologie proprietarie sono ogni forma di sistema, strumento o procedura tecnica sviluppata da e per una specifica impresa commerciale... Le idee sviluppate e presentate dai dipendenti sono di solito considerate proprietà intellettuale del datore di lavoro,

qualificandole così come tecnologia proprietaria." Definizione presa da wiseGEEK: www.wisegeek.com (accesso 22 ottobre 2012).

[7] Cory Doctorow, *The Coming War on General-Purpose Computing*, boingboing, 10 gennaio 2012 (basato su un discorso introduttivo tenuto al Chaos Computer Congress, dicembre 2011): boingboing. net (accesso 15 ottobre 2012).

[8] Stuxnet è un computer worm estremamente sofisticato che si ritiene sia stato sviluppato da Stati Uniti e Israele per attaccare le macchine Siemens che si presumeva fossero usate dall'Iran per arricchire l'uranio. Per una panoramica su Stuxnet, vedi Wikipedia: en.wikipedia.org/wiki/Stuxnet. Vedi anche *WikiLeaks: US Advised to Sabotage Iran Nuclear Sites by German Thinktank*, in "Guardian", 18 gennaio 2011: www.guardian.co.uk. WikiLeaks ha pubblicato uno dei primi rapporti sugli effetti che oggi si crede siano stati causati da Stuxnet, cioè l'incidente nella struttura nucleare di Natanz in Iran. Vedi *Serious Nuclear Accident May Lay Behind Iranian Nuke Chief's Mistery Resignation*, WikiLeaks, 17 luglio 2009: wikileaks.org/wiki. Gli indizi provenienti dalla compagnia di intelligence globale Stratfor, propalati da WikiLeaks, indicano un coinvolgimento israeliano. Vedi Email ID 185945, The Global Intelligence Files: wikileaks.org (accesso a tutti i link 16 ottobre 2012).

La militarizzazione del ciberspazio

[1] Pentesting è la contrazione di penetration testing, test di penetrazione, ed è un termine dell'ingegneria della sicurezza che designa gli attacchi autorizzati a un sistema informatico o a una rete informatica come potrebbero essere tentati da un utente non autorizzato, il tutto per valutare quanto sono sicuri. Gli analisti della sicurezza vengono reclutati spesso nella comunità hacker per svolgere questi test sulla sicurezza dei sistemi.

[2] Il rubabandiera è un gioco all'aria aperta con due squadre ciascuna di guardia a una bandierina. L'obiettivo è catturare la bandiera dell'altra squadra e riportarla alla propria base. Durante i loro convegni gli hacker giocano una versione informatica del gioco, in cui le squadre devono aggredire e difendere computer e reti.

[3] Sysadmin Cup sta per System Administrator Cup, la coppa degli amministratori di sistema. L'amministratore di sistema è una persona che lavora nel settore It e gestisce e tiene aperto un sistema informatico o una rete. Jacob sta dicendo che quella manovra era una specie di torneo per amministratori di sistema.

[4] *Aaron Says Encryption Protects Privacy, Commerce*, USIS Washington File, 13 ottobre 1998: www.fas.org (accesso 21 ottobre 2012).

[5] Sito web Wassenaar Arrangement: www.wassenaar.org (accesso 21 ottobre 2012).

[6] Andy si sta riferendo a vari episodi delle "prime crittoguerre" degli anni novanta. Quando i militanti cypherpunk iniziarono a diffondere forti strumenti crittografici come software libero, l'amministrazione Usa si mosse per impedire che fossero utilizzati efficacemente, definendo la crittografia una munizione e limitandone le esportazioni, cercando inoltre di introdurre tecnologie concorrenti che fossero volutamente incomplete in modo che le forze dell'ordine potessero sempre decifrare le informazioni e tentando di imporre il controverso progetto "key escrow". Per un breve periodo a cavallo del secolo si è dato per scontato che questi tentativi fossero stati complessivamente sconfitti. Tuttavia è ora in corso una "seconda crittoguerra" che vede tentativi tecnici e legislativi di inserire backdoor nell'uso della crittografia o altrimenti rendere marginale il suo utilizzo.

[7] Il calcolo si riferisce ai presunti 196,4 miliardi di minuti di chiamate su linea terrestre in Germania nel 2010, digitalizzati con un voice-codec a 8 Kbp, per una quantità totale di 11.784 Petabyte (Pb), arrotondati a 15 con l'ingombro ulteriore. Dando per scontato che l'archiviazione semplice costi 500.000 dollari Usa per un Pb, significa 7,5 milioni di dollari o 6 milioni di euro. Aggiungetevi i costi di un centro dati decente, potenza di elaborazione, connessioni e forza lavoro. Anche aggiungendo tutti i 101 miliardi di minuti di chiamate su cellulare in Germania nel 2010, con altri 50 Pb e 18,3 milioni di euro, costa sempre meno di un solo aereo militare come l'Eurofighter (90 milioni di euro) o l'F22 (150 milioni di dollari).

[8] Per saperne di più su VASTech, vedi buggedplanet: buggedplanet.info (accesso 21 ottobre 2012).

[9] Lo scandalo della sorveglianza interna della NSA senza mandato è il caso più rilevante di sorveglianza di massa nella storia degli Stati Uniti. Il Foreign Intelligence Surveillance Act del 1978 (FISA) ha decretato illegale che le agenzie Usa spiino cittadini Usa senza mandato. Dopo l'11 settembre, la NSA ha iniziato a compiere violazioni di massa della FISA, autorizzate da un ordine esecutivo segreto di George W. Bush. L'amministrazione Bush pretendeva di avere l'autorità esecutiva per farlo in base alle leggi di emergenza del 2001 approvate dal Congresso: Authorization for the Use of Military Force (AUMF) e Patriot Act. Il programma di spionaggio interno senza mandato della NSA, che comprendeva la collaborazione delle imprese private, tra cui la AT&T, è rimasto occultato fino al 2005 quando è stato portato allo scoperto dal "New York Times". Vedi *Bush Lets U.S. Spy on Callers Without Courts*, in "New York Times", 16 dicembre 2005: www.nytimes.com.

I giornalisti del "New York Times" erano stati contattati da una talpa che aveva spifferato l'esistenza di un programma di sorveglianza senza mandato. Nel 2004 l'allora direttore esecutivo del "New York Times", Bill Keller, accettò la richiesta dell'amministrazione Bush di bloccare i reportage per un anno, fino a dopo la rielezione del presidente. Nel 2005 il "New York Times" si affrettò a pubblicare l'articolo quando seppe di una possibile ingiunzione di limitazione preventiva stile Pentagon Papers da parte dell'amministrazione. L'amministrazione Bush negò qualsiasi illegalità nel programma NSA. Il ministero della Giustizia avviò un'indagine immediata per trovare la fonte, coinvolgendo venticinque agenti federali e cinque procuratori. Alcuni esponenti di rilievo del Partito repubblicano chiesero il rinvio a giudizio del "New York Times" in base allo Espionage Act. All'indomani dell'articolo del "New York Times" si presentarono alla stampa altre talpe che gradualmente fornirono un quadro dettagliato dell'illegalità e dello spreco ai massimi livelli della NSA. Fu avviata una serie di class action da gruppi di difesa legale come la American Civil Liberties Union (ACLU) e la Electronic Frontier Foundation (EFF). In una di queste cause, ACLU contro NSA, i querelanti non poterono procedere perché non furono in grado di dimostrare che erano stati spiati personalmente. In un altro, Hepting contro AT&T, una talpa della AT&T, Mark Klein, si presentò con una deposizione giurata che rivelava la portata della collaborazione dell'azienda con il programma di spionaggio interno. Vedi la sezione Hepting contro AT&T nel sito web della EFF: www.eff.org.

Mark Klein era un teste nel processo Hepting contro AT&T. Ex impiegato della AT&T a Folsom, San Francisco, la sua deposizione giurata alla EFF nella causa rivelava l'esistenza di una "stanza 641A", una struttura di intercettazioni strategiche gestita dalla AT&T per la NSA. La struttura forniva accesso ai cavi in fibra ottica che veicolavano il traffico backbone Internet, rendendo possibile la sorveglianza di tutto il traffico Internet che passava dal palazzo, sia interno che per l'estero. Un'altra talpa NSA, William Binney, ha valutato che ci siano fino a venti strutture del genere, tutte situate in punti chiave della rete delle telecomunicazioni negli Stati Uniti. La deposizione giurata di Klein dà importanti informazioni sul carattere del programma di sorveglianza della NSA, confermato dalle talpe NSA. È un esempio di "intercettazione strategica": tutto il traffico Internet che passa dagli Stati Uniti viene registrato e stoccato a tempo indeterminato. Si sa per certo che anche il traffico interno Usa è intercettato e archiviato perché da un punto di vista tecnico quando hai a che fare con questo volume di traffico è impossibile filtrarlo per le esigenze di un mandato FISA. L'interpretazione legale ufficiale della FISA ora sostiene che una "intercettazione" si è svolta solo quando a una comunicazione interna già intercettata e stoccata dalla NSA si "accede" dal database NSA, e che è solo a questo stadio che è necessario un mandato. I cittadini Usa dovrebbero dare per assodato che tutto il loro traffico telecomunicazioni (compresi telefonate, SMS, e-mail e navigazione sul Web) è monitorato e archiviato per sempre nei centri dati della NSA.

Nel 2008, per rispondere a una caterva di cause in seguito allo scandalo delle intercettazioni, il Congresso Usa approvò emendamenti alla legge FISA del 1978, immediatamente firmati dal presidente. Questi emendamenti crearono le basi per la concessione di un'altamente controversa "immunità retroattiva" contro le incriminazioni per violazione della FISA. Il senatore Barack Obama, durante la sua campagna presidenziale, aveva inserito nella propria piattaforma la "trasparenza" e promesso di proteggere le talpe, ma quando entrò in carica nel 2009 il suo ministero della Giustizia reiterò la politica dell'amministrazione Bush, portando all'archiviazione della causa

Hepting e altre, concedendo la “immunità retroattiva” alla AT&T.

Anche se le indagini del ministero della Giustizia sulle fonti del primo articolo del “New York Times” non scoprirono la talpa, scoprirono però quelle uscite allo scoperto dopo il servizio. Una era Thomas Drake, ex alto dirigente della NSA, che da anni si lamentava presso le Commissioni di supervisione dei servizi d’informazione del Congresso a proposito della corruzione e degli sprechi nel programma “Trailblazer” della NSA. Le lamentele interne furono messe a tacere quanto i dipendenti pubblici disposti a tenerne conto. Dopo l’articolo del “New York Times” Drake aveva rivelato la storia del Trailblazer al “Baltimore Sun”. Fu incriminato da un’indagine del gran giurì, definito “nemico dello stato” e accusato in base allo Espionage Act. Vedi *The Secret Sharer*, in “New Yorker”, 23 maggio 2011: www.newyorker.com.

L’indagine su Drake è crollata a causa dell’interessamento dell’opinione pubblica nel giugno 2011. Dopo i falliti tentativi di costringere Drake al patteggiamento, il ministero della Giustizia si è accontentato della sua ammissione di colpevolezza per un reato minore. Drake è stato condannato a un anno di libertà vigilata.

Gli strascichi dello scandalo della sorveglianza NSA proseguono. La ACLU è in causa per contestare la costituzionalità degli emendamenti FISA del 2008 in Amnesty *et al.* contro Clapper. Vedi *FISA Amendment Act Challenge*, ACLU, 24 settembre 2012: www.aclu.org. Con la causa Jewel contro NSA, la EFF sta cercando di far cessare la sorveglianza senza mandato della NSA. La causa è stata archiviata nel 2009 quando l’amministrazione Obama ha fatto ricorso all’immunità trattandosi di segreti relativi alla sicurezza nazionale. Vedi la pagina EFF su Jewel contro NSA: www.eff.org/cases/jewel. Comunque il Nono circuito delle Corti d’appello ha concesso la riapertura della causa nel dicembre 2011. Thomas Drake e altre talpe NSA, William Binney e J. Kirk Wiebe, stanno fornendo prove. L’amministrazione Obama, che ha svolto una campagna elettorale con un programma di trasparenza del governo, ha intentato causa a più talpe, in base allo Espionage Act, di tutte le precedenti amministrazioni messe insieme (accesso a tutti i link di questa nota 23 ottobre 2012).

[10] Vedi la voce sul sistema Eagle in buggedplanet: buggedplanet.info (accesso 22 ottobre 2012).

Combattere la sorveglianza totale con le leggi dell’uomo

[1] *German Court Orders Stored Telecoms Data Deletion*, BBC, 2 marzo 2010: news.bbc.co.uk (accesso 15 ottobre 2012).

[2] La direttiva 2006/24/EC del Parlamento e del Consiglio europeo impone di conservare i dati relativi alle telecomunicazioni dei cittadini per un periodo da sei a ventiquattro mesi. È stata l’applicazione di questa direttiva nella legislazione tedesca a essere giudicata incostituzionale in Germania. Nel maggio 2012 la Commissione dell’Unione europea ha deferito la Germania alla Corte di giustizia europea per non essersi adeguata alla direttiva. Vedi il comunicato stampa della Commissione: europa.eu (accesso 15 ottobre 2012).

[3] Vedi *Sweden Approves Wiretapping Law*, BBC, 19 giugno 2008: news.bbc.co.uk. Per saperne di più su FRA-lagen, vedi Wikipedia: en.wikipedia.org (accesso a entrambi i link 10 ottobre 2012).

[4] Metadati significa “dati sui dati”. Nel contesto di questa discussione, metadati si riferisce ai dati diversi dal “contenuto” della comunicazione elettronica. È un po’ come il fronte della busta, indipendente dal contenuto. La sorveglianza dei metadati non è incentrata sui contenuti delle e-mail ma piuttosto sulle informazioni concomitanti, cioè da chi è stata inviata l’e-mail, gli indirizzi IP (e quindi la località) da cui è partita, ora e data di ogni e-mail ecc. Comunque il punto è che la tecnologia per intercettare i metadati è la medesima che intercetta i contenuti. Se concedi a qualcuno il diritto di sorvegliare i tuoi metadati, i suoi macchinari devono anche intercettare i contenuti delle tue comunicazioni. Oltre a ciò, tanta gente non capisce che “gli aggregati di metadati sono il contenuto”, cioè quando i metadati sono messi insieme forniscono un’immagine incredibilmente dettagliata delle comunicazioni di una persona.

[5] Amesys fa parte del gruppo Bull, un tempo concorrente della Dehomag della IBM nella vendita di sistemi di perforazione schede ai nazisti. Vedi Edwin Black, *IBM and the*

Holocaust, Crown Books, 2001; tr. it. *L'IBM e l'olocausto*, Rizzoli, Milano 2001. Per saperne di più su come Gheddafi spiava i libici nel Regno Unito usando i macchinari di sorveglianza Amesys, vedi *Exclusive: How Gaddafi Spied on the Fathers of the New Libya*, OWNI.eu, 1 dicembre 2011: owni.eu (accesso 22 ottobre 2012).

[6] WikiLeaks ha iniziato a divulgare gli Spy Files che portano alla luce la diffusione della sorveglianza di massa nel dicembre 2011. Vi si può accedere presso wikileaks.org.

[7] Per ulteriori dettagli, vedi buggedplanet: buggedplanet.info.

[8] Il Chaos Communication Congress è un incontro annuale della scena hacker internazionale, organizzato dal Chaos Computer Club.

[9] Jacob fa riferimento alla ZTE, uno dei due produttori cinesi (l'altro è la Huawei) di strumenti elettronici fortemente sospettati di contenere "backdoor". Jacob sta suggerendo che il "regalo" dell'infrastruttura delle comunicazioni ha un prezzo: sarà aperto alla sorveglianza cinese già per come è progettato.

Lo spionaggio nel settore privato

[1] Kill Your Television è il nome dato a una forma di protesta contro le comunicazioni di massa, in cui le persone si astengono dalla televisione a favore di attività sociali.

[2] L'"effetto rete" è l'effetto che una persona che compie un'attività esercita sulla probabilità che altre persone compiano la stessa attività.

[3] Per saperne di più, vedi la *Nota sui vari tentativi di molestare WikiLeaks e le persone a essa associate*, inserita prima della discussione.

[4] Secondo il "Wall Street Journal", "il governo Usa ha ottenuto un tipo controverso di ordinanza segreta del tribunale per costringere Google Inc. e il piccolo provider Internet Sonic.net Inc. a cedere informazioni dagli account e-mail del collaboratore volontario di WikiLeaks Jacob Appelbaum... secondo i documenti esaminati dal 'Wall Street Journal' il caso WikiLeaks è diventato all'inizio dell'anno un banco di prova per l'interpretazione della legge quando Twitter si è opposta a un'ordinanza per cedere i dati degli account dei sostenitori di WikiLeaks, compreso il signor Appelbaum... L'ordinanza voleva ottenere il 'protocollo Internet', o IP, gli indirizzi delle macchine da cui la gente faceva il login nei suoi account. Un indirizzo IP è un numero unico assegnato a una macchina connessa a Internet. Inoltre l'ordinanza cercava gli indirizzi di e-mail delle persone con cui comunicavano quegli account. Era stata presentata sigillata, ma Twitter ha ottenuto dal tribunale il diritto di avvertire gli abbonati le cui informazioni venivano richieste... Le ordinanze del tribunale esaminate dal 'Journal' cercano il medesimo tipo di informazione richiesto a Twitter. L'ordinanza segreta di Google reca la data 4 gennaio e indica al gigante delle ricerche in rete di cedere gli indirizzi IP da cui il signor Appelbaum si connetteva al suo account gmail.com e gli indirizzi di e-mail e IP degli utenti con cui comunicava dal primo novembre 2009. Non è chiaro se Google si è opposta o ha ceduto i documenti. L'ordinanza segreta per la Sonic è datata 15 aprile e indica alla Sonic di rilasciare lo stesso tipo di informazione sull'account di e-mail di Appelbaum dal primo novembre 2009. Il 31 agosto la corte ha accettato di togliere i sigilli all'ordinanza Sonic in modo da fornirne una copia al signor Appelbaum". *Secret Orders Target Email*, in "Wall Street Journal", 9 ottobre 2011: online.wsj.com (accesso 11 ottobre 2012). Per altri dettagli, vedi la citata nota sulle molestie che precede la discussione.

[5] *WikiLeaks Demands Google and Facebook Unseal US Subpoenas*, in "Guardian", 8 gennaio 2011: www.guardian.co.uk (accesso 16 ottobre 2012). Per ulteriori dettagli, vedi la nota sulle molestie inserita prima della discussione.

[6] Vedi la succitata nota posta prima della discussione.

[7] Per altri dettagli, vedi il sito web Europe versus Facebook: www.europe-v-facebook.org (accesso 24 ottobre 2012).

[8] Una National Security Letter o NSL è una lettera inviata da un organismo Usa per richiedere "metadati" o "dati senza contenuti" come le registrazioni delle transazioni finanziarie, i registri IP o i contatti di posta elettronica. Chiunque riceva una NSL deve cedere i dati richiesti se vuole evitare l'incriminazione. Una NSL non richiede l'autorizzazione di un giudice e può essere emanata direttamente da un'agenzia federale.

Per questo motivo è simile al cosiddetto “mandato amministrativo”, un’ordinanza che impone di fornire informazioni, necessitante solo di una supervisione amministrativa, non giudiziaria. Su queste basi le NSL violerebbero le tutele del Quarto emendamento contro perquisizioni e sequestri arbitrari. Hanno anche una componente “bavaglio” che significa che è reato per chi riceve una NSL parlarne con altri. E in questo modo violano le tutele del Primo emendamento sulla libertà di parola. In Doe contro Gonzales, il bavaglio delle NSL è stato giudicato incostituzionale. La legge è stata poi cambiata per garantire a chi riceve una NSL il diritto di contestarla davanti a un giudice, convincendo così la corte del Secondo circuito che il loro utilizzo non era più incostituzionale. Le NSL continuano a essere criticate dai gruppi per le libertà civili e contestate in tribunale.

L’uso delle NSL è enormemente aumentato dopo l’approvazione del Patriot Act nel 2001. I destinatari sono solitamente fornitori di servizi come i provider Internet o gli istituti finanziari. I dati richiesti sono di solito quelli dei loro clienti. Il destinatario non può informare il cliente che i suoi dati sono stati richiesti. Anche se i destinatari hanno il diritto di contestare le NSL davanti a un giudice, la norma bavaglio impedisce che l’obiettivo venga anche solo a sapere delle lettere e pertanto impedisce che le contesti. Per capire quanto è difficile giustificare ciò, vedi un video della vicecapo avvocato dell’FBI che tenta di rispondere alla domanda di Jacob Appelbaum: “Come posso andare da un giudice se la parte terza è impossibilitata a dirmi che mi avete preso come bersaglio?”. La risposta della donna (“Ci sono volte in cui dobbiamo disporre di cose del genere”) è agghiacciante. www.youtube.com (trovato anche con ulteriore materiale contestuale presso Privacy SOS: privacysos.org).

Secondo la Electronic Frontier Foundation, “di tutti i pericolosi poteri di sorveglianza del governo che sono stati ampliati dal Patriot Act americano, il potere delle NSL sotto la U.S.C. § 2709 come ampliata dal Patriot Act sezione 505 è uno dei più terrorizzanti e invasivi. Le lettere recapitate ai fornitori di servizi di comunicazione come le compagnie telefoniche e i provider Internet permettono all’FBI di chiedere segretamente dati sulle comunicazioni private e sull’attività in Internet dei nor-mali cittadini americani senza alcuna significativa supervisione o revisione giudiziaria pregressa. I destinatari delle NSL sono soggetti a un’ordinanza bavaglio che impedisce loro di rivelare in qualsiasi caso l’esistenza delle lettere ai colleghi, agli amici o persino ai familiari, per non parlare dell’opinione pubblica”. Vedi www.eff.org. Vedi anche la raccolta di documenti della Electronic Frontier Foundation relativi alle National Security Letters diffusi in base al Freedom of Information Act: www.eff.org DB (accesso a tutti i link di questa nota 23 ottobre 2012).

Combattere la sorveglianza totale con le leggi della fisica

[1] Vedi *supra* nota 6 del cap. “La militarizzazione del ciberspazio” sulle “prime crittoguerre” degli anni novanta del secolo scorso.

[2] Julian sta parlando di SSL/TLS, un protocollo crittografico oggi incorporato come standard in tutti i browser e usato per la navigazione sicura, per esempio quando un browser è usato per le operazioni bancarie in Internet.

[3] Per un esempio fra tanti, vedi *BlackBerry, Twitter Probed in London Riots*, in “Bloomberg”, 9 agosto 2011: www.bloomberg.com (accesso 16 ottobre 2012).

[4] Per esempio, un membro del gruppo LulzSec che ha portato allo scoperto i difetti delle misure di sicurezza della Sony rilasciando i dati personali dei clienti Sony è stato arrestato allorché la sua identità è stata acquisita dal sito proxy HideMyAss.com tramite ordinanza di tribunale negli Stati Uniti. Vedi *Lulzsec Hacker Pleads Guilty Over Sony Attack*, BBC, 15 ottobre 2012: www.bbc.com (accesso 15 ottobre 2012).

Internet e la politica

[1] SOPA sta per Stop Online Piracy Act, legge per fermare la pirateria online, PIPA per Protect Intellectual Property Act, legge per la protezione della proprietà intellettuale. Entrambe sono progetti di legge Usa arrivati all’attenzione internazionale nei primi mesi del 2012, entrambe sono evidente espressione legislativa del desiderio dell’industria dei

contenuti, rappresentata da organismi come la Recording Industry Association of America, di far rispettare su scala globale le leggi sulla proprietà intellettuale, e con la mano più pesante possibile, come risposta alla libera distribuzione online degli artefatti culturali. Entrambe le leggi proponevano di concedere poteri pesanti e allargati di censura in Internet ai tutori dell'ordine Usa, i quali hanno minacciato che avrebbero "sfasciato Internet". Entrambe le leggi si sono guadagnate l'odio di fette sostanziose della comunità internazionale online e hanno scatenato una forte reazione dei protagonisti del settore che hanno interesse a un'Internet libera e aperta. All'inizio del 2012 Reddit, Wikipedia e parecchie migliaia di altri siti hanno fermato i propri servizi per protestare contro queste leggi, invitando a una forte mobilitazione per fare pressione sui pubblici rappresentanti. Altri provider di servizi di rete, come Google, hanno avviato petizioni. Come risposta, entrambe le leggi sono state ritirate in attesa di ripensamenti e dibattiti per verificare che possano essere il migliore approccio al problema della proprietà intel-lettuale online. Questo episodio è ritenuto la prima significativa scoperta e affermazione di un efficace potere di pressione del settore Internet sul Congresso.

[2] Vedi la nota sulle persecuzioni a WikiLeaks inserita prima della discussione.

[3] ACTA è l'acronimo di Anti-Counterfeit and Trade Agreement, un trattato internazionale multilaterale negoziato in segreto nell'arco di anni, sotto l'egida di Stati Uniti e Giappone, una cui sezione inserisce nuovi obblighi draconiani per proteggere la proprietà intellettuale. Le prime stesure dell'ACTA sono state rivelate nel 2008 dopo essere state propalate a WikiLeaks, scatenando le proteste diffuse dei militanti per la cultura libera e dei difensori della rete. Vedi la sezione relativa su WikiLeaks: wikileaks.org. I cablo diplomatici Usa condivisi da WikiLeaks con La Quadrature du Net a inizio 2011 dimostravano che l'ACTA era trattata esplicitamente sottobanco per accelerare la creazione di regole durissime sui provider che potevano poi essere imposte con la forza ai paesi più poveri esclusi dall'accordo. Vedi *WikiLeaks Cables Shine Light on ACTA History*, La Quadrature du Net, 3 febbraio 2011: www.laquadrature.net (accesso 23 ottobre 2012). Nel luglio 2012, dopo una campagna capitanata da La Quadrature du Net e Jérémie Zimmer-mann, l'ACTA è stata sconfitta al Parlamento europeo.

[4] M.A.I.D., che sta per (Mutually) Assured Information Destruction, distruzione delle informazioni (reciprocamente) garantita, è "un'intelaiatura che fornisce un deposito remoto di chiave sensibile al tempo e un'autentica dimostrabile con codifica opzionale di emergenza. Distrugge automaticamente le chiavi crittografiche dopo un dato lasso di tempo configurabile dall'utente": www.noisebridge.net. Le leggi come il Regulation of Investigatory Powers Act del 2000 (RIPA) fanno del Regno Unito un regime abbastanza ostile alla crittografia. Ai sensi di questa legge i singoli possono essere obbligati a decrittare i dati o a consegnare una password dietro ordine dei poliziotti. Non è necessaria una supervisione dell'autorità giudiziaria. Il rifiuto a ottemperare può sfociare in un'incriminazione. Nel processo successivo, se l'imputato/a sostiene di aver dimenticato la password c'è l'inversione dell'onere della prova. Per evitare di essere condannato l'imputato/a deve dimostrare di averla dimenticata, e questo, secondo i critici della legge, determina una presunzione di colpevolezza. In confronto negli Stati Uniti, anche se ci sono state molte polemiche sugli stessi temi e la situazione non è per niente ideale, chi invocava il Primo e il Quarto emendamento in circostanze simili ha avuto molto più successo. Vedi il rapporto *Freedom from Suspicion, Surveillance Reform for a Digital Age*, pubblicato da JUSTICE, 4 novembre 2011, reperibile su: www.justice.org.uk. Per saperne di più sul sistema Rubberhose, vedi *The Idiot Savants' Guide to Rubberhose* di Suelette Dreyfus: marutukku.org (accesso a tutti i link 24 ottobre 2012).

[5] Un archivio della vecchia mailing list Cypherpunk può essere scaricato da: www.cryptome.org/cpunks/cpunks-92-98.zip. Tim May è stato un membro fondatore della mailing list Cypherpunk. Vedi il suo Cyphernomicon, una FAQ sulla storia e filosofia del cypherpunk: www.cypherpunks.to (accesso a entrambi i link 24 ottobre 2012).

[6] *Proposed US ACTA Plurilateral Intellectual Property Trade Agreement (2007)*, WikiLeaks, 22 maggio 2008: wikileaks.org (accesso 21 ottobre 2012).

[7] *Massive Takedown of Anti-Scientology Videos on YouTube*, Electronic Frontier Foundation, 5 settembre 2008: www.eff.org (accesso 16 ottobre 2012).

[8] *EU-India Free Trade Agreement Draft*, 24 febbraio 2009, WikiLeaks, 23 giugno 2009: wikileaks.org (accesso 21 ottobre 2012).

[9] Con peer-to-peer, o P2P, si intende una rete in cui ogni computer può fungere da client o server per tutti gli altri (ogni computer può sia ricevere che dare informazioni), permettendo la rapida condivisione di contenuti come musica, video, documenti o qualsiasi tipo di informazione digitale.

[10] Cloud computing è la situazione in cui molte funzioni di solito svolte da un computer, come la conservazione dei dati (compresi i dati dell'utente per varie applicazioni), ospitare e far girare programmi e fornire la potenza di elaborazione per far girare il software, sono svolte in remoto, fuori dal computer stesso, "nella nuvola", di solito da aziende che offrono servizi di cloud computing tramite Internet. Invece di avere bisogno di un vero personal, a tutti gli utenti basta una macchina che possa accedere a Internet, e il resto viene fornito all'utente in rete. La metafora della nuvola nasconde il fatto che tutti i dati e metadati dell'utente si trovano in un computer remoto in un centro dati, molto probabilmente controllato da una grossa azienda come Amazon, e, mentre gli utenti non hanno più il controllo completo, qualcun altro ce l'ha.

[11] Vedi la nota sulle molestie che precede la discussione.

[12] DIASPORA è un social network che permette a tutti gli utenti di fungere da proprio server installando il programma DIASPORA, il quale gli permette di mantenere il controllo dei propri dati. È stato creato come alternativa rispettosa della privacy a Facebook. È no profit e posseduto dagli stessi utenti: diasporaproject.org.

[13] Il Napster originario (1999-2001) era un pionieristico servizio peer-to-peer per condividere la musica. Diventò clamorosamente popolare ma fu presto chiuso dopo una causa per infrazione del diritto d'au-tore intentata dalla Recording Industry Association of America. Dopo il fallimento, il nome Napster è stato acquistato e usato per un diverso store online che vende musica a pagamento.

[14] Vedi la nota sulle molestie che precede la discussione.

[15] Benjamin Bayart è presidente di French Data Network, il più vecchio provider Internet attivo in Francia, e un paladino della neutralità della rete e del software libero. Vedi la sua voce su Wikipedia (in francese): fr.wikipedia.org (accesso 15 ottobre 2012).

[16] Larry Lessig è un accademico e attivista americano noto per le sue idee sul diritto d'autore e sulla cultura libera. Il suo blog è: lessig.tumblr.com (accesso 15 ottobre 2012).

Internet e l'economia

[1] Ci sono molti contenuti affascinanti nei cablogrammi diplomatici Usa diffusi da WikiLeaks su questo tema. Per una discussione interessante, consultate i seguenti (secondo identificazione riferimento cablo, accesso a tutti i link 24 ottobre 2012):
07BEIRUT1301: http://wikileaks.org/cable/2007/08/07 BEIRUT1301.html
08BEIRUT490: http://wikileaks.org/cable/2008/04/08 BEIRUT490.html
08BEIRUT505: http://wikileaks.org/cable/2008/04/08 BEIRUT505.html
08BEIRUT523: http://wikileaks.org/cable/2008/04/08 BEIRUT523.html

[2] Vedi riferimento cablo ID 10MOSCOW228, WikiLeaks: wikileaks.org (accesso 24 ottobre 2012).

[3] Per saperne di più sulle uccisioni senza giusto processo dei cittadini americani Anwar al-Awlaki e suo figlio Abdulrahman al-Awlaki, vedi Glenn Greenwald, *The Due-Process-Free Assassination of U.S. Citizens Is Now Reality*, in "Salon", 30 settembre 2011: www.salon.com. E *The Killing of Awlaki's 16-year-old Son*, in "Salon", 20 ottobre 2011: www.salon.com. "È letteralmente impossibile immaginare un rifiuto più violento del concetto base della repubblica di questo sviluppo di una branca esecutiva segreta e libera da rendiconti che raccoglie simultaneamente informazioni su tutti i cittadini e poi applica una 'matrice disposizioni' per decidere quale punizione comminare. È una classica distopia politica diventata realtà." Glenn Greenwald, *Obama Moves to Make the War on Terror Permanent*, in "Guardian", 24 ottobre 2012: www.guardian.co.uk (accesso a tutti i link 24 ottobre 2012).

[4] Per ulteriori informazioni, prego consultare *The Anonimity Bibliography, Selected Papers in Anonimity*, a cura di Roger Dingledine e Nick Mathewson: freehaven.net/anonbib

(accesso 24 ottobre 2012). Le valute chaumiane sono emanate centralmente ma utilizzano la crittografia per garantire transazioni anonime. Sono diverse da Bitcoin, un'altra moneta anonima discussa ampiamente più avanti, dove tutte le transazioni sono pubbliche ma la moneta non ha un'autorità centrale.

[5] Per saperne di più sul blocco bancario di WikiLeaks, vedi la nota sulle molestie che precede la discussione.

[6] Qui Julian fa riferimento ai piani del governo britannico per incrementare l'uso dei braccialetti elettronici. Vedi *Over 100,000 Offenders to Be Electronically Tagged*, in "Guardian", 25 marzo 2012: www.guardian.co.uk (accesso 22 ottobre 2012). All'epoca della discussione Julian era agli arresti domiciliari in attesa dell'esito della richiesta di estradizione. Dopo l'isolamento senza incriminazione nel dicembre 2010, la detenzione di Julian è stata convertita agli arresti domiciliari dietro cauzione di oltre 300.000 sterline. La condizione della cauzione era il suo rimanere confinato a un dato indirizzo in certi orari, un regime fatto rispettare da un braccialetto elettronico fissato alla caviglia, gestito da un'agenzia di sicurezza privata sotto contratto con il governo britannico. I movimenti di Julian erano controllati fino al punto che era costretto a presentarsi tutti i giorni al commissariato a un'ora particolare, per oltre 550 giorni. Al momento della pubblicazione Julian è confinato nell'ambasciata dell'Ecuador, circondata dalla London Metropolitan Police. Nel giugno 2012 Julian è entrato nell'ambasciata per chiedere asilo politico dalla persecuzione del governo degli Stati Uniti e dei suoi alleati. Ha ottenuto l'asilo nell'agosto 2012.

[7] *Is CCA Trying to Take Over the World?*, American Civil Liberties Union, 21 febbraio 2012: www.aclu.org. *Passing House Bill Will Worsen Already Pressing Civil Rights Issue*, annarbor.com, 2 agosto 2012: annarbor.com. Vedi anche *Goldman Sachs to Invest $9.6m in New York Inmate Rehabilitation*, in "Guardian", 2 agosto 2012: www.guardian.co.uk (accesso a tutti i link 24 ottobre 2012).

[8] Bitcoin (bitcoin.org) è la prima applicazione fortunata di un classico concetto cypherpunk: la moneta digitale crittografica. Si parla più a lungo di Bitcoin *infra*, ma un'eccellente introduzione esplicativa della tecnologia e della filosofia che le sta dietro è reperibile in *Understanding Bitcoin*, Al Jazeera, 9 giugno 2012: www.aljazeera.com (accesso 22 ottobre 2012).

[9] L'e-gold è una moneta digitale e anche un'impresa avviata nel 1996. I proprietari sono stati incriminati dal ministero della Giustizia americano per "cospirazione a scopo di riciclaggio di valuta". Si sono dichiarati colpevoli e hanno subìto condanne ai servizi comunitari, agli arresti domiciliari e alla libertà vigilata. Il giudice che ha emesso la sentenza ha sostenuto che si meritavano pene miti perché non intendevano intraprendere un'attività criminale: Vedi *Bullion and Bandits: The Improbable Rise and Fall of E-Gold*, in "Wired", 9 giugno 2009: www.wired.com (accesso 22 ottobre 2012).

[10] Prima di Internet, la principale rete globale per lo scambio di dati esistente in parallelo alla rete telefonica era la rete X.25. La bolletta era basata sul quantitativo di dati mandati e ricevuti, non sulla durata della connessione come con la rete telefonica. I gateway (i cosiddetti PAD) permettevano la connessione alla rete X.25 da quella telefonica mediante modem o accoppiatori acustici. Per ulteriori dettagli vedi Wikipedia: http://en.wikipedia.org (accesso 24 ottobre 2012).

[11] David Chaum è un crittografo e inventore di protocolli crittografici, pioniere delle tecnologie delle monete digitali. Ha proposto eCash, una delle prime valute elettroniche crittografiche anonime.

[12] Sugli effetti della stampa negativa, vedi *Bitcoin Implodes, Falls More than 90 Percent from June Peak*, arstechnica, 18 ottobre 2011: arstechnica.com (accesso 22 ottobre 2012).

[13] Vedi per esempio *The Underground Website Where You Can Buy Any Drug Imaginable*, in "Gawker", 1 giugno 2011: gawker.com (accesso 22 ottobre 2012).

[14] Le prime ricerche di Lawrence Lessig su copyright e cultura (per esempio nel suo libro *Free Culture* del 2004) sono stati scavalcati negli ultimi anni dall'interesse per la corruzione della democrazia americana tramite l'attività delle lobby presso il Congresso. Vedi The Lessig Wiki: wiki.lessig.org.

[15] La California Correctional Peace Officers Association è un influente gruppo

d'interesse californiano che dona di norma cifre a sei zeri alle elezioni statali, anche se anno per anno non è il più grosso singolo donatore alle campagne. Vedi *California Reelin*, in "The Economist", 17 marzo 2011: www.economist.com. E *The Golden State's Iron Bars*, in "Reason", luglio 2011: reason.com. Vedi anche la voce sulla California Correctional Peace Officers Association sul sito web FollowTheMoney del National Institute for Money in State Politics: www.followthemoney.org (accesso a tutti i link 22 ottobre 2012).

[16] Heinz von Foerster (1911-2002) era uno scienziato austro-americano, architetto della cibernetica. Il suo cosiddetto "imperativo etico" o classico motto è: "Agire sempre in modo da aumentare il numero di scelte", o, detto in tedesco: "Handle stets so, daß die Anzahl der Wahlmöglichkeiten größer wird".

[17] Jacob attribuisce questa osservazione a John Gilmore.

La censura

[1] Per saperne di più sulla persecuzione di Jacob e altre persone associate a WikiLeaks, vedi la nota prima della discussione.

[2] Isaac Mao è un blogger, programmatore e venture capitalist cinese, cofondatore di CNBlog.org e membro del consiglio del Tor Project.

[3] Vedi la pagina di WikiLeaks su Nadhmi Auchi: wikileaks.org (accesso 24 ottobre 2012).

[4] Queste storie sono reperibili su WikiLeaks qui: wikileaks.org (accesso 24 ottobre 2012).

[5] In generale, per vedere che cosa hanno tagliato i partner mediatici di WikiLeaks, cables.mrkva.eu e cablesearch.net forniscono eccellenti possibilità di raffrontare le versioni censurate dei cablo con le versioni integrali.

[6] *Qaddafi's Son Is Bisexual and Other Things the New York Times Doesn't Want You to Know*, in "Gawker", 16 settembre 2011: gawker.com. L'esempio specifico citato fa riferimento al cablo ID 06TRIPOLI198, WikiLeaks: wikileaks.org. Le censure possono essere viste sul sito web Cablegatesearch che presenta la storia delle revisioni, con le censure evidenziate in rosa: cablegatesearch.net (accesso a tutti i link 22 ottobre 2012).

[7] Per il cablo originale vedi riferimento ID 10STATE17263,WikiLeaks: wikileaks.org. Per l'articolo del "New York Times" vedi *Iran Fortifies Its Arsenal With the Aid of North Korea*, in "New York Times", 29 novembre 2010: www.nytimes.com. Lo stesso cablo fu usato anche da David Leigh del "Guardian" per il suo articolo *WikiLeaks Cables Expose Pakistan Nuclear Fears*, "Guardian", 30 novembre 2010: www.guardian.co.uk. La versione censurata del cablo pubblicata dal "Guardian", senza il numero di riferimento del cablo, l'ha ridotto a due paragrafi relativi al Pakistan. *US Embassy Cables: XXXXXXXXXXXXX*, "Guardian", 30 novembre 2010. www.guardian.co.uk. La portata dei tagli può essere visualizzata sul sito web Cablegate che presenta la storia delle revisioni, con le censure evidenziate in rosa: cablegatesearch.net (accesso a tutti i link 22 ottobre 2012).

[8] Per il cablo originale, vedi riferimento ID 08KYIV2414,WikiLeaks: wikileaks.org. Per la versione censurata del "Guardian", vedi *US Embassy Cables: Gas Supplies Linked to Russian Mafia*, 1 dicembre 2010: www.guardian.co.uk. La censura può essere visualizzata sul sito web Cablegate che presenta la storia delle revisioni, con le censure evidenziate in rosa: cablegatesearch.net (accesso a tutti i link 22 ottobre 2012).

[9] Per il cablo originale vedi riferimento ID 10ASTANA72,WikiLeaks: wikileaks.org. Per la versione censurata del "Guardian" vedi *US Embassy Cables: Kazakhstan – The Big Four*, in "Guardian", 29 novembre 2010: www.guardian.co.uk. La censura può essere visualizzata sul sito web Cablegate che presenta la storia delle revisioni, con le censure evidenziate in rosa: cablegatesearch.net (accesso a tutti i link 22 ottobre 2012).

[10] Vedi per esempio il cablo con riferimento ID 09TRIPOLI413 sulle compagnie energetiche occidentali operanti in Libia. L'immagine sul sito web Cablegatesearch, con le censure del "Guardian" evidenziate in rosa, dimostra che il giornale ha rimosso tutti i riferimenti ai nomi delle compagnie e dei loro dirigenti, a parte la Gazprom russa. Anche se parte del contenuto è abbastanza mite con le compagnie occidentali, i tagli sono complessi e la versione censurata fornisce un quadro abbastanza diverso: cablegatesearch.net (accesso 22 ottobre 2012).

[11] In questo esempio il cablo originale era di 5226 parole. La versione manipolata

pubblicata dal “Guardian” ne aveva solo 1406. Per il cablo originale vedi riferimento ID 05SOFIA1207,WikiLeaks: wikileaks.org. Per la versione censurata del “Guardian” vedi *US Embassy Cables: Organised Crime in Bulgaria*, in “Guardian”, 1 dicembre 2010: www.guardian.co.uk. Per l’articolo del “Guardian” basato sul cablo vedi *WikiLeaks Cables: Russian Government “Using Mafia for Its Dirty Work”*, in “Guardian”, 1 dicembre 2010: www.guardian.co.uk. La portata della censura può essere visualizzata sul sito web Cablegate che presenta la storia delle revisioni, con le censure evidenziate in rosa: cablegatesearch.net. Questo esempio bulgaro è discusso dal partner mediatico di WikiLeaks in Bulgaria, Bivol, in *Unedited Cable from Sofia Shows the Total Invasion of the State by Organized Crime (Update: Cable Comparison)*, in “WL Central”, 18 marzo 2011: wlcentral.org. Inoltre vedi *The Guardian: Redacting, Censoring or Lying?*, in “WL Central”, 19 marzo 2012: wlcentral.org. Notevoli anche riguardo gli articoli di “WL Central” il commento del giornalista del “Guardian” David Leigh e le risposte (accesso a tutti i link 22 ottobre 2012).

[12] È il cablo con riferimento ID 09BERLIN1108. La censura può essere visualizzata sul sito web Cablegate che presenta la storia delle revisioni, con le censure evidenziate in rosa: cablegatesearch.net (accesso 22 ottobre 2012).

[13] Per altri esempi vedi il sito web cabledrum: www.cabledrum.net.

[14] “Intercettazione delle telecomunicazioni. La presidenza ha fornito informazioni sullo stato delle cose… Ha ricordato la stampa negativa che questo problema ha avuto nei media… Su queste basi la presidenza ha pertanto ammesso che i progressi in questo campo sono molto lenti… Parecchie delegazioni hanno espresso una certa cautela per quanto riguarda la stesura di un comunicato stampa, notando che potrebbe scatenare una reazione a catena e ulteriore stampa negativa nei media. La commissione, mentre nota che la sua posizione non è cambiata, ha informato le delegazioni che un modo possibile per spezzare lo stallo potrebbe seguire una strategia simile a quella adottata affrontando il problema della pornografia infantile in Internet. Pur ammettendo che era un argomento diverso, ha anch’esso una dimensione relativa alle intercettazioni”, Commissione europea, incontro sull’intercettazione delle telecomunicazioni del gruppo di lavoro sulla collaborazione tra polizie, 13-14 ottobre 1999. Il documento integrale è presso: http://www.quintessenz.at (accesso 24 ottobre 2012).

[15] Vedi la nota sulle molestie che precede la discussione.

[16] Jacob si sta riferendo a Gilmore contro Gonzales, 435 F.3d 1125 (9th Cir. 2006). John Gilmore, uno dei primi cypherpunk, arrivò fino alla Corte suprema nazionale perché fossero rivelati i contenuti di una legge segretata, una “direttiva di sicurezza”, che limitava il diritto dei cittadini di viaggiare in aereo senza essere identificati. Oltre a contestare la costituzionalità di un provvedimento del genere, Gilmore contestava il fatto che esso fosse segretato e non potesse essere rivelato pur avendo effetti vincolanti sui cittadini statunitensi. La corte consultò la Security Directive in sessione segreta e sentenziò contro Gilmore sulla costituzionalità della direttiva. Tuttavia i contenuti della legge non sono mai stati rivelati nel corso del dibattimento. Vedi Gilmore v. Gonzales presso PapersPlease.org: papersplease.org/gilmore/facts.html (accesso 22 ottobre 2012).

[17] Christiania è un’area dichiaratasi autonoma di Copenaghen, in Danimarca. Ex caserma dell’esercito, fu occupata negli anni settanta da una folta comunità collettivista/anarchica. Si è ricavata uno status legale unico nel paese.

[18] Il principio della “neutralità della rete” impone il divieto ai provider Internet (la legge di solito lo contesta) di limitare agli utenti l’accesso alle reti che formano Internet, compresa la limitazione dei contenuti. Vedi la pagina della Electronic Frontier Foundation sulla neutralità della rete: www.eff.org (accesso 24 ottobre 2012).

[19] *Blocking WikiLeaks Emails Trips Up Bradley Manning Prosecution*, in “Politico”, 15 marzo 2012: www.politico.com (accesso 21 ottobre 2012).

[20] Per ulteriori informazioni su Wau Holland vedi la Wau Holland Stiftung: www.wauland.de.

[1] *Stasi Still in Charge of Stasi Files*, WikiLeaks, 2 ottobre 2007: www.wikileaks.org (accesso 22 ottobre 2012).

Topi alla Opera House

[1] "Ecco che cosa potete fare per cambiare il mondo, per un viaggio migliore. Prendete tutti i soldi che spendiamo per le armi e la difesa ogni anno e invece spendeteli per nutrire, vestire e istruire i poveri del mondo, e lo si può fare più volte senza escludere alcun essere umano, e potremmo anche esplorare lo spazio, interno ed esterno, insieme, per sempre, in pace", Bill Hicks. Per un video del passaggio recitato vedi *Bill Hicks – Positive Drugs Story*: http://www.youtube.com (accesso 24 ottobre 2012).

[2] Il Sarbanes-Oxley Act del 2002 è una legge statunitense approvata come risposta agli scandali aziendali e contabili di Enron, Tyco International, Adelphia, Peregrine Systems e WorldCom. Puntava a eliminare le medesime pratiche corrotte che avevano portato alle crisi. La Section 107 della legge, codificata come USC 1513(e), introduce il reato di tentativo di ritorsione contro chi rivela informazioni.

[3] Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom*, in "Public Affairs", 2011.

[4] Sul software libero, vedi *The Free Software Definition*, dal sito web del GNU Operating System: www.gnu.org/philosophy/free-sw.html. L'hardware libero significa che non è gravato da brevetti, che è progettato per gli standard aperti, e non ci sono leggi contro la manipolazione o il reverse engineering (nessuna legge anticirconvenzione) e i principi base del progetto, le istruzioni e i piani sono ottenibili liberamente da chiunque altro li detenga e abbia le risorse necessarie per costruire una replica. Per saperne di più, vedi *Exceptionally Hard and Soft Meeting: Exploring the Frontiers of Open Source and DIY*, EHSM: ehsm.eu. Vedi anche *Open-Source Hardware* su Wikipedia: en.wikipedia.org (accesso a tutti i link 24 ottobre 2012).

[5] Sulla stampa 3D che utilizza un hardware libero e aperto vedi il video introduttivo della stampante RepRap 3D: vimeo.com/5202148 (accesso 24 ottobre 2012).

[6] "Sii il guaio che vuoi vedere nel mondo" è una citazione da *A Softer World*, un webcomic fotografico: www.asofterworld.com (accesso 24 ottobre 2012).

[7] Per approfondire i temi sollevati nella discussione, Jacob raccomanda le due seguenti risorse bibliografiche: *The Anonimity Bibliography, Selected Papers in Anonimity*, a cura di Roger Dingledine e Nick Mathewson: freehaven.net; *The Censorship Bibliography: Selected Papers in Censorship*, a cura di Philipp Winter: www.cs.kau.se (accesso a entrambi i link 24 ottobre 2012).

[8] Nota lasciata volutamente in bianco.

[9] Nawaat.org è un blog collettivo indipendente tunisino partito nel 2004: nawaat.org/portail. Tunileaks è stato lanciato da Nawaat nel novembre 2010 con la pubblicazione dei cablo di WikiLeaks attinenti alla Tunisia: tunileaks.appspot.com. Per saperne di più su Tunileaks e sui tentativi di censura del governo di Ben Alì, vedi *Tunisia: Censorship Continues as Wikileaks Cables Make the Rounds*, Global Voices Advocacy, 7 dicembre 2010: advocacy.globalvoicesonline.org (accesso a tutti i link 24 ottobre 2012).

Indice