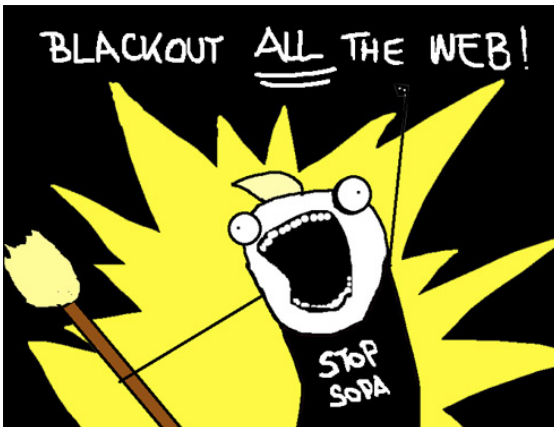
Scienza e Pace, Vol. 3 N° 1 (2012)

Prospettive di libertà in rete

Appunti per la costruzione di una rete libera da controllo e censura

di ***eigenLab***



Per riuscire a comprendere ed analizzare al meglio l'odierna situazione riguardo alla regolamentazione di internet, e quindi ai processi che hanno portato alle leggi e ai trattati internazionali in discussione in questo periodo, è importante ripercorrere in maniera più o meno cronologica i passi legislativi, statunitensi e non, dal 1998 ad oggi. È infatti nel 1998, quando gli Stati Uniti d'America decidono di emanare il DMCA (*Digital Millenium Copyright Act*) per implementare e rafforzare il contenuto di due trattati redatti nel 1996 dall'Organizzazione Mondiale per la Proprietà Intellettuale delle Nazioni Unite (WIPO), che inizia un lungo processo di censura del web. Questa legge dichiara illegale la produzione e la diffusione di strumenti, servizi o tecnologie che possono aiutare ad aggirare i meccanismi di protezione della proprietà intellettuale e criminalizza qualsiasi elusione dei suddetti meccanismi di protezione, anche se non violano esplicitamente il diritto d'autore. I vari SOPA (*Stop Online Piracy Act*), PIPA (*Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act*) e ACTA (*Anti-Counterfeiting Trade Agreement*) non sono altro che formalizzazioni della linea introdotta dal DMCA.

Sono passati 14 anni da questa prima legge che stabiliva le regole su chi fossero i “siti pirata” e come dovessero essere puniti, criminalizzando il libero scambio di informazioni. Tuttavia, vista la crescita esponenziale dell'uso di Internet e, di conseguenza, anche del suo uso da parte di molte aziende, non ci si poteva aspettare che la situazione restasse invariata ancora a lungo. Il primo e-G8 convocato a Parigi da Nicholas Sarkozy il 24 e 25 maggio 2011 e la delibera n. 398/11 approvata il 6 luglio 2011 dall’AGCOM, e contenente uno schema di regolamento per “la tutela del diritto d’autore sulle reti di comunicazione elettronica”, scorso sono stati alcuni importanti segnali dell'inizio di una nuova fase di minaccia alla libertà di informazione.

Da quel lontano 1998 molte cose sono cambiate: i colossi che oggi si dividono la rete – Google Facebook, Yahoo, eBay – nel tempo hanno acquisito potere e capitali, diventando di fatto i gestori determinanti del web. Anche gli utenti sono cambiati: in un'era che molto spesso viene definita “digitale”, l'informatizzazione è diventata appannaggio di molti e il numero di chi oggi può connettersi è notevolmente aumentato. Per restare all’Italia, nel 1998 gli utenti del web erano circa 2,1 milioni secondo l’European Information Technology Observatory (EITO), mentre oggi sono più di 30 milioni. In parallelo, è cresciuto il flusso di

informazioni scambiate in maniera libera ed orizzontale dagli utenti stessi attraverso appositi canali di condivisione. La nuova ondata di legislazioni che, in molti paesi occidentali, mira a definire nuove regole soprattutto riguardo alla protezione di materiale coperto da copyright, risponde esattamente a questo mutato scenario.

Il Protect IP Act è stato presentato nel Maggio 2011 dal senatore democratico Patrick Leahy. Il progetto di legge, la cui discussione è stata sospesa per approfondimenti lo scorso 12 gennaio, vorrebbe introdurre nuove tipologie di reato rispetto alla pirateria online, alla contraffazione e alla produzione di tecnologie per eludere i meccanismi di controllo nell'accesso a materiale coperto da copyright. Tale legge stabilisce in particolare le caratteristiche che identificano un sito pirata: "A) non ha altro fine se non quello di impegnarsi, abilitare o facilitare: 1) la riproduzione, distribuzione o pubblica esibizione di materiale sotto copyright, completa o in modo sostanzialmente completo, in maniera tale da violare il copyright [secondo la sezione 501 della legge 17 (codice federale degli Stati Uniti); […]; 3) la vendita, distribuzione o promozione di beni, servizi o materiali che sostengono i marchi contraffatti, come definito nella sezione 34 (d) del Lanham Act". Il PIPA si prefigge, inoltre, di potenziare gli strumenti contro siti web registrati e operanti anche fuori dagli Stati Uniti individuati come "rogue websites" e dà la possibilità di emettere un'ordinanza giudiziaria contro tali siti. Ad emettere l'ordinanza è l'*Attorney general*, un alto funzionario del potere esecutivo americano a capo di un Dipartimento di Giustizia, e questa obbliga gestori di servizi di pagamento (paypal, visa, ecc.), gestori di servizi di pubblicità e anche motori di ricerca a interrompere i servizi forniti al sito incriminato.

A fine ottobre 2011, per rinforzare questo meccanismo e completare la limitazione delle libertà informatiche in nome della tutela del copyright, è stata depositata al Congresso un'ulteriore proposta di legge nota come SOPA. Con questo provvedimento si vorrebbe autorizzare il Dipartimento di Giustizia ad emettere un'ordinanza verso quei siti internet, al di fuori dalla giurisdizione degli Stati Uniti, accusati di violazione di copyright. Dopo l'ordinanza il procuratore generale può vietare ad un ISP (*Internet Service Provider*), motori di ricerca, circuiti pubblicitari o a servizi di pagamento come Paypal che hanno sede in America o cadono nella giurisdizione americana, di intrattenere rapporti con i siti incriminati con "misure tecnicamente possibili e ragionevoli": tra questi non è escluso il metodo più invasivo e manipolativo del filtraggio dei DNS (*Domain Name System*), in virtù del quale la richiesta di un determinato indirizzo internet da parte di un utente viene re-diretta del provider o comunque non risolta correttamente (**Figura 1**).

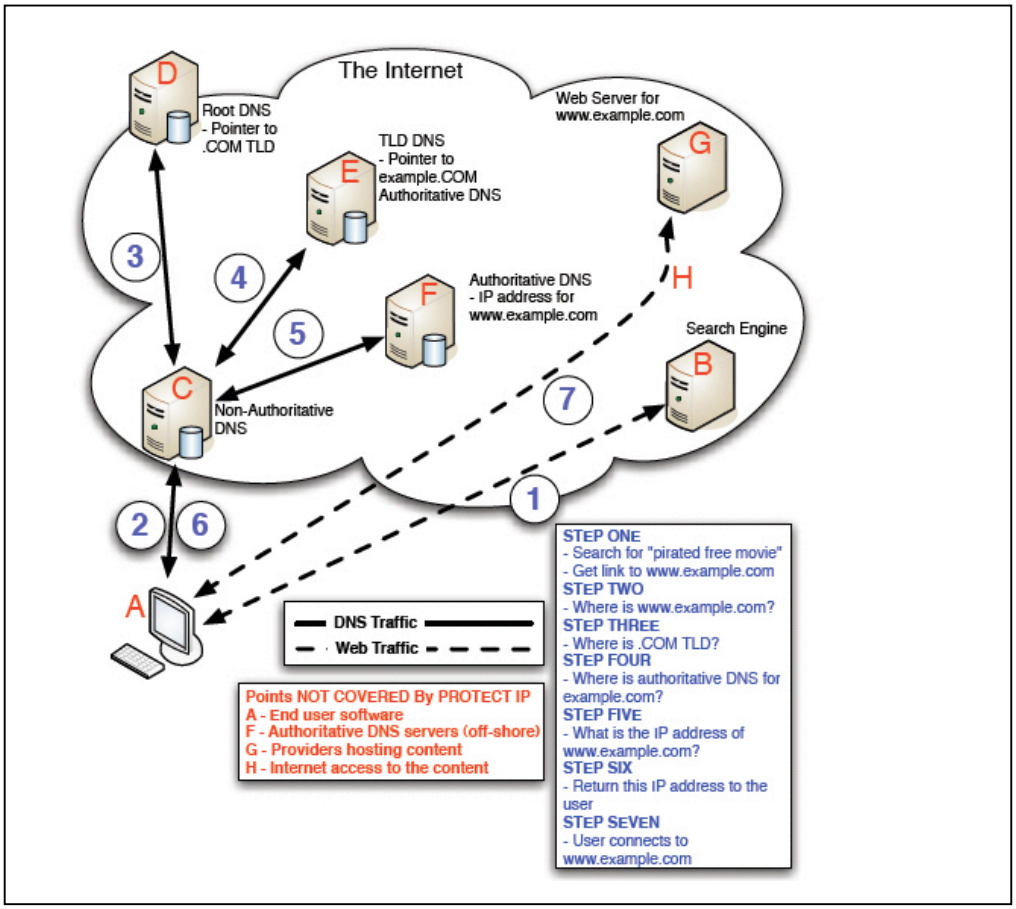


Figura 1. Esempio di filtraggio dei DNS

Il provvedimento non obbliga i suddetti circuiti a non avere rapporti con i siti "pirata". Tuttavia, in caso di "collaborazione" con il governo, a tali siti viene concessa l'immunità in un eventuale processo. Vengono, inoltre, inasprite le pene per lo streaming e per la diffusione di medicinali contraffatti, nonché di informazioni relative a operazioni e materiali militari (come avvenuto nel caso di *Wikileaks*). In pratica, quindi, lo scopo di questa legge è quello di isolare il sito a vario titolo "incriminato" dal resto della rete e questa scelta è dovuta per il semplice fatto che non si può agire a livello legale verso siti "esteri", ed in particolare questa legge non agisce sul sito in sé ma sui suoi partner commerciali.

La presentazione del PIPA e del SOPA ha prodotto, tra il 2011 e il 2012 un animato dibattito pubblico e importanti movimenti di protesta negli Stati Uniti. Da una parte, uno schieramento composito di *corporations* dell'industria culturale, sindacati dello spettacolo e grandi case discografiche, che vedono nel libero scambio di materiale sul web una falla nel meccanismo di creazione di profitti, sempre più legati alla detenzione dei diritti d'autore, tra cui la *Motion Picture Association of America*, la *U.S. Chamber of Commerce*, la *Recording Industry Association of America*, ma anche l'*Independent Film and Television Alliance*, l'*American Federation of Musicians,* il *Directors Guild of America* e lo *Screen Actors Guild*. L'obiettivo di queste leggi, create *ad hoc* per venire incontro agli interessi dei poteri forti dell'intrattenimento, ma anche dei poteri più o meni occulti, interessati a

mantenere certe informazioni nascoste, è quello di bloccare o controllare severamente il flusso di dati scambiati liberamente dagli utenti. Dall'altra parte, uno schieramento vasto e articolato di associazioni per la libertà d'informazione e la difesa dei diritti umani, come *Reporters Without Borders*, *Human Rights Watch*, l'*American Civil Liberties Union*, il *Center for Democracy and Technology*, ma anche i principali colossi del web, sia commerciali come *Google, Yahoo!, Facebook, Twitter, LinkedIn, eBay, Mozilla*, che non commerciali come la *Wikimedia Foundation*. La questione ha anche scompaginato nei due rami del parlamento le appartenenze partitiche, producendo coalizioni di sostegno e di contestazione ai due progetti di legge ampiamente trasversali.

I problemi rilevati dagli oppositori di questa legge sono diversi: da una parte, favorendo il blocco dei DNS, si attua una misura troppo radicale nei confronti dei siti incriminati, inoltre, mentre il DMCA prevedeva solo una diffida nei confronti di chi deteneva il dominio di un determinato sito, il SOPA implica un vero e proprio processo che, qualora si concludesse con un'effettiva assoluzione, obbliga il sito incriminato al pagamento delle spese processuali. Questo sicuramente va a discapito di siti *no profit e low budget*, che non potrebbero permettersi i costi di un processo e inoltre risulterebbe dannoso proprio per questi siti che possono essere messi in difficoltà e spinti a chiudere sulla scorta di accuse false. In più, rende illegali anche solo le tecnologie che danno la possibilità di avere materiale protetto da copyright, quali proxy, VPN o software per l'anonimato. L'*Electronic Frontier Foundation*, a più di 10 anni dall'entrata in vigore del *Digital Millennium Copyright Act*, realizzato un significativo rapporto sulle conseguenze inattese del provvedimento: il risultato, documentato dall'analisi di diversi casi, è che il DMCA ha limitato la libertà di parola e la ricerca scientifica, ha messo a repentaglio il *fair use* e si è dimostrato in contrasto con principi e leggi che difendono gli utenti dalle intrusioni informatiche.

Neanche l'Italia è stata esente da analoghi processi legislativi volti a limitare la libertà in rete. Da ultimo, un emendamento alla legge comunitaria depositato dal deputato della Lega Nord Giovanni Fava prevedeva che qualunque privato detentore di un qualche diritto d'autore potesse segnalare un sito internet per violazione di copyright e indurlo a chiudere, senza neanche un regolare processo. L'emendamento è stato poi bocciato. Questi processi di limitazione e controllo della libertà di informazione in rete si inquadrano in un più vasto processo globale, in corso da diversi anni e volto a privatizzare il bene comune della conoscenza, mettendola al servizio della creazione di profitti da parte delle multinazionali.

Meno conosciuto del PIPA e del SOPA, anche perché oggetto di trattative riservate, ma allo stesso modo lesivo della libertà digitale, è ad esempio il TPPA (*Trans-Pacific Partnership Agreement*), un accordo economico stipulato tra Stati Uniti e alcuni paesi dell'area del Pacifico. L'accordo prevede una liberalizzazione, con annessa eliminazione delle dogane, delle economie dei paesi coinvolti ma contiene anche delle norme riguardo al copyright. In particolare, nell'articolo 10 del trattato si fa spesso riferimento ad un accordo precedente, il TRIPs, stipulato nel 1994 che riguarda anch'esso la tutela della proprietà intellettuale, estendendola a livello mondiale per uniformare gli standard di tutela del copyright sul modello americano. Nella parte dedicata alla proprietà intellettuale, redatta sulla base della legge statunitense, si prevede l'estensione della durata del copyright, la disconnessione forzata e sanzioni penali per chi viola il diritto d'autore.

Tra le attuali strategie legislative per interdire agli utenti l'accesso a determinati materiali o informazioni va menzionato un ultimo trattato internazionale segreto, l'ACTA (*Anti-Counterfeit Trade Agreement*). L'ACTA è un trattato che contrasta la contraffazione di materiali protetti da copyright, dai film e dal materiale multimediale in genere fino ai farmaci ed agli alimenti. Non è un caso che tra i promotori di questo trattato ci siano grandi multinazionali del settore agroalimentare come la Monsanto o del settore farmaceutico come la Pfizer. Utilizzata in questo modo, la proprietà intellettuale non è più l'apparato giuridico con cui qualcuno difende dalla altrui speculazione una propria idea o una propria scoperta: diventa piuttosto quel punto di forza su cui multinazionali e *corporations* fanno leva per accaparrarsi l'idea più brillante, il farmaco più efficace, il seme più resistente o il disco più ascoltato semplicemente pagando un 'autore', che spesso si trova costretto ad accettare la cessione del proprio diritto quasi per un istinto di sopravvivenza. L'autore si priva quindi completamente dalla propria opera o invenzione, che viene rivenduta al prezzo deciso da chi detiene i mezzi di produzione e di diffusione.

Tutti questi provvedimenti nascono dalle possibilità di accesso e condivisione offerte della struttura stessa della rete. Infatti, per come si è evoluto, il web ha finito per favorire questo processo di controllo dell'informazione: esso si è venuto configurando come una struttura di fatto verticistica, in cui l'utente medio, il cosiddetto client, può avere l'accesso a internet tramite i provider, che fisicamente forniscono il servizio. Il client, al fine di ottenere i servizi della rete, deve connettersi ad un server, che gestisce le prestazioni e svolge il ruolo di database delle informazioni. A questo punto, è sufficiente per una grande azienda o un governo esercitare la giusta pressione sui provider affinché impongano restrizioni nella fornitura dei servizi oppure per ottenere le informazioni personali sugli utenti conservate nei server. Un esempio recente, concernente la censura, riguarda il caso di Twitter, che ha ceduto alle pressioni dei governi acconsentendo di rimuovere determinati tweet qualora fossero ritenuti 'scomodi' o dovessero infrangere in qualche modo le leggi del paese in cui l'utente risiede. In maniera diversa, la multinazionale Facebook da diversi anni vende informazioni private dei suoi iscritti ad aziende che le sfruttano per il loro marketing: non solo la rete non è libera da censure, ma in essa le informazioni private subiscono sempre più spesso una subdola mercificazione a fine di lucro, a discapito degli utenti.

Gli effetti di una struttura verticistica del web sono evidenti nell'eclatante caso della Cina, in cui il governo è di fatto proprietario della rete. Per accedere alla rete globale sono stati introdotti sei "cancelli" attraverso cui gli utenti devono necessariamente connettersi, e che sono costantemente monitorati da agenzie governative. Nonostante esistano molti Internet Service Providers (ISP) privati, questi possono operare solamente collegandosi al World Wide Web tramite i sei cancelli, e pagando dunque il "pedaggio" (in termini di censure politiche) imposto dal governo. Possiamo definire quindi la rete Cinese come una sorta di intra-net, ossia una rete a circuito chiuso su scala nazionale, con accessi limitati all'internet globale. Il mezzo più potente con cui si estrinseca il controllo governativo è naturalmente la censura, soprannominata *The Great Firewall of China*. In Cina non possono essere raggiunti più di 19.000 siti dei più diversi tipi: dal sito della BBC a quello di Amnesty International, fino a Wikipedia. Oltre a questo tipo di censura macroscopica, ne esiste un'altra di tipo microscopico, che consiste nel censurare selettivamente determinate schermate che contengono parole o immagini che figurano in una sorta di grosso 'libro nero' del governo. Più di 30.000 tecnici sono impiegati dalla Cina per controllare l'informazione, supportati da appositi software talvolta 'made in China' o in altri casi venduti da qualche multinazionale occidentale, che filtrano le parole, cancellano, bloccano,

censurano i messaggi. Alcuni di questi agiscono all'insaputa stessa degli utenti, secondo il modello del 'cavallo di Troia': ad esempio l'azienda cinese Tencent, che produce il software Qq molto diffuso per la messaggistica istantanea, su disposizione delle autorità ha incollato ad esso un programma che automaticamente blocca tutte le parole proibite.

La situazione cinese, sebbene sia la più clamorosa in termini di esercizio del controllo della rete e della censura, non è l'unico esempio di tentativo da parte del governo coadiuvato da grandi aziende di mettere le mani sulle libertà degli utenti della rete. In Tunisia, durante la rivolta scoppiata nel gennaio 2011 e che ha portato alla caduta del governo di Ben Alì, la cyber polizia del paese ha attuato una brutale azione di *phishing* (operazioni tramite internet che permettono la raccolta di dati sensibili in maniera coercitiva ed illecita), volta a sottrarre le password di Facebook e Gmail dei cittadini per poterne controllare direttamente i profili e le email. In pratica sono state create delle false homepage dette "siti civetta" in cui gli utenti inserivano i propri dati convinti di effettuare normalmente l'accesso al social network o alla propria casella email, mentre invece essi venivano direttamente raccolti dalla cyber polizia. Il tentativo fu vanificato inizialmente dall'imposizione da parte di Google di un protocollo di sicurezza HTTPS (difficilmente falsificabile), assicurando così tutti gli utenti che il sito di riferimento fosse l'originale. Il governo si appoggiò allora al colosso Microsoft che fornì un metodo alternativo ed infallibile per spacciarsi nuovamente per Google e Facebook e che consentiva di aggirare i certificati. In poche parole, Microsoft ha concesso allo Stato tunisino, che ha una propria capacità di "autocertificazione", la facoltà di etichettare tutti i domini possibili e non solo quelli governativi, naturalmente, dietro un cospicuo compenso.

Contro questi meccanismi di censura sviluppati dai governi con la collaborazione di grandi aziende che mirano solo al guadagno, e contro i vari provvedimenti che si stanno tentando di varare, si schierano diverse unioni di *hacktivists* (attivisti hacker), che si coordinano sotto il ben conosciuto nome di Anonymous, e che si mobilitano tramite operazioni di hacking con diversi target. Una delle proteste di Anonymous che ha raggiunto i toni più alti è stata quella effettuata dopo la chiusura di MegaUpload, il noto sito di condivisione di file, a cui è prontamente seguito la pubblicazione via YouTube di un comunicato in cui viene attaccato il governo degli Stati Uniti che ha "ordito intrighi, tramando modi per incrementare la censura attraverso il blocco degli ISP, il blocco dei DNS, la censura dei motori di ricerca, dei siti". Nei mesi scorsi la protesta di Anonymous si è prodotta in particolare in attacchi DDoS, cioè nel sovraccarico e nel conseguente oscuramento di determinati siti collegati al decreto SOPA, quali i siti di FBI, il sito del governo USA e, in Italia, quello della SIAE. Tuttavia, come anche sottolineato nel comunicato stesso, questi attacchi non possono e non vogliono essere risolutivi, ma vogliono tenere aperto uno spazio pubblico di discussione e di mobilitazione: come recita un comunicato di Anonymus, "cosa può mai risolvere un attacco DDoS? Che cosa può essere attaccare un sito rispetto i poteri corrotti del governo?"

L'invito di Anonymous non è quello di limitare l'azione esclusivamente ad internet. La rete deve essere, proprio per la sua globalità e velocità di diffusione, il mezzo con cui sensibilizzare quante più persone possibili riguardo ai gravi avvenimenti che stanno accadendo, rendendo consapevoli i cittadini di tutti gli stati che anche loro, prima o poi, dovranno far fronte ad un attentato alle proprie libertà fondamentali. Il fine ultimo è quello di dare seguito alla protesta telematica con una protesta fisica, far sì che la gente scenda in piazza e lotti per difendere quei diritti che possono sembrare scontati, ma che a tutti gli

effetti i governi vogliono toglierci. L'appello mira a impedire l'approvazione e la messa in pratica delle leggi SOPA e PIPA negli Stati Uniti, dell'ACTA in Europa e del TPPA tra diversi stati del Pacifico, e scoraggiare in prospettiva ulteriori tentativi di altri governi di estendere il controllo della rete passando attraverso la tutela del copyright.

Alla luce degli avvenimenti recenti e delle considerazioni critiche che li hanno accompagnati, emerge con forza la necessità di creare un'alternativa 'dal basso' ad una rete ormai mercé dei poteri forti, economici e politici. Per creare questa alternativa bisogna innanzitutto decentralizzare e rendere indipendente la rete dai provider e dai loro server. Questo è proprio ciò che ci proponiamo ad eigenLab tramite il progetto eigenNet: creare una rete *mesh*, ossia orizzontale, in cui gli utenti possano accedere a diversi servizi, senza però che le informazioni scambiate vengano filtrare da un provider centrale oppure possano essere usate per altri fini. I nodi partecipano alla rete in modo paritario e sono tra di loro indipendenti, ognuno può decidere quali servizi condividere con gli altri (come ad esempio l'accesso ad internet) e l'unico modo per oscurare eigenNet sarebbe quello di spegnere simultaneamente tutti i nodi che la compongono. Avere internet gratis, però, non è l'unico vantaggio che si ottiene entrando a far parte di eigenNet; infatti, la rete è stata concepita per offrire servizi e ospitare siti: chiunque può connettersi alla rete e creare gratuitamente un nuovo sito senza il timore di venire censurato.

Due ulteriori servizi già implementati nella nostra rete sono LiberaLibri e Diaspora*. Il primo, a cui si può accedere solamente se si è connessi con eigenNet, è un archivio di libri e testi universitari di tutte le facoltà scaricabili gratuitamente in formato pdf. Il secondo, invece, accessibile da qualunque connessione, è un social network open-source distribuito di cui noi gestiamo l'unico pod italiano. A differenza di altri ben noti social network, su Diaspora* la privacy è totalmente garantita; infatti le informazioni degli utenti, quali dati d'accesso, foto, commenti, condivisioni, sono proprietà unicamente degli utenti stessi; risiedono, per di più cifrate, unicamente nel pod di appartenenza e nel momento in cui un utente dovesse rimuovere da Diaspora* un contenuto, esso verrebbe immediatamente e definitivamente cancellato anche dal pod, non lasciando alcuna traccia di esso.

La debolezza del web, per come lo abbiamo conosciuto fino ad oggi, risiede nella sua specifica struttura centralizzata e verticistica. Ricostruirla dal basso è possibile, anche se sicuramente non facile, ed è l'unica via per sfuggire a qualsiasi tentativo di censura e controllo. Gli attacchi portati in questi anni alla libertà della rete, così come le mobilitazioni e le proteste contro censura, controllo e mercificazione del sapere, ci pongono oggi una sfida inedita: disegnare e costruire modelli reali e realizzabili di gestione partecipata e orizzontale della rete. Dobbiamo costruire noi per prim* l'idea della rete che vorremmo. Dobbiamo essere noi per prim* ad andare all'attacco e non limitarci a prendere parola in difesa agli attacchi subiti dalla nostra libertà individuale e collettiva.