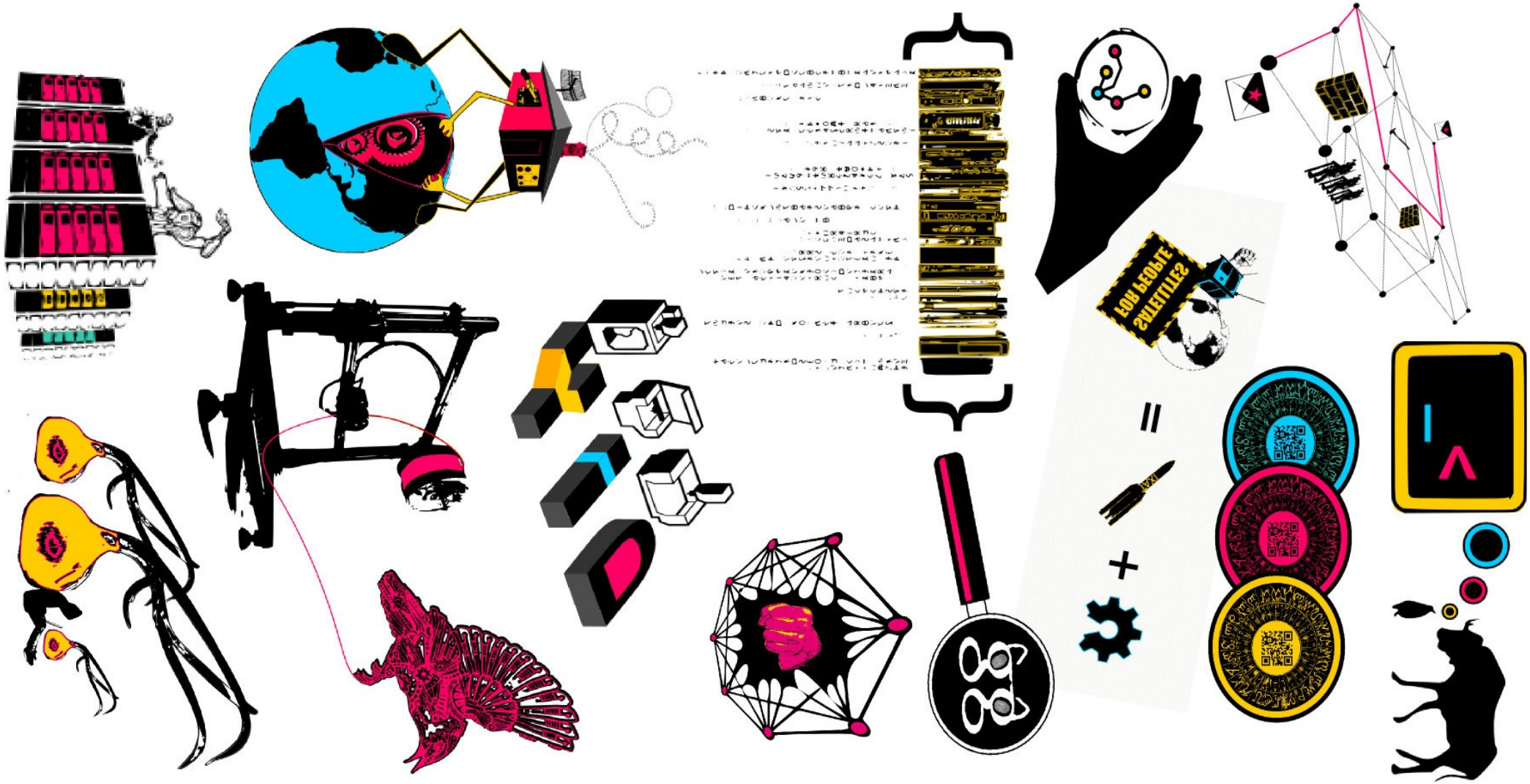


Sobirania Tecnològica

Sommario

Sovranità tecnologica

Soberanía Tecnologica è una raccolta di saggi curata dalla colonia ecoindustriale postcapitalista Calafou. Attraverso l'analisi critica dello sviluppo tecnologico della nostra società, varie tematiche sono affrontate per fornire una prospettiva differente sulle possibilità offerte dalla tecnologia contemporanea: server autogestiti, criptomonete, hacklabs e hackerspaces, motori di ricerca alternativi sono tra gli argomenti trattati. Durante il talk, alcuni di questi verranno presentati dal gruppo di traduzione in italiano del libro.

Le traduttrici

http://hacklabbo.indivia.net/

http://www.ecn.org/xm24/?page_id=114

Traduzione in lingua italiana, ma anche formattazione del dossier in markdown.

L'originale è scaricabile qui: https://calafou.org/es/content/dossier-soberan%C3%ADa-tecnol%C3%B3gica

Mentre il libro fatto con gitbook, lo potete vedere compilato qui:

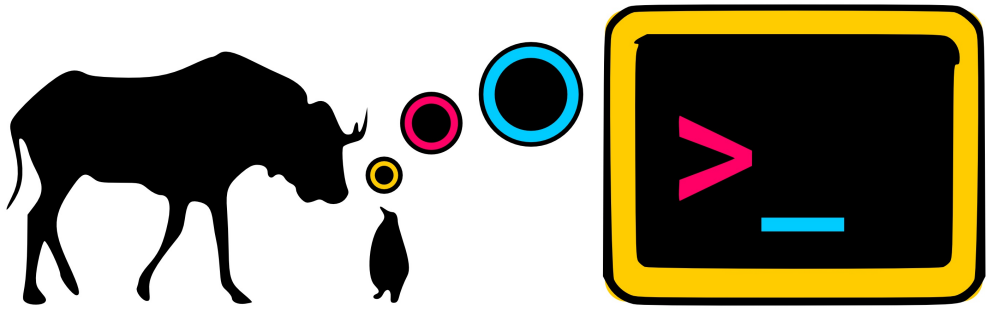
http://www.digitigrafo.it/doc/ST/

Calafou giugno 2014

Hacklabbo novembre 2016

Il software libero è ancor più necessario che mai

Richard Stallman



Una versione ridotta di questo articolo è stata pubblicata su Wired. Sono passati ormai 30 anni dalla nascita del movimento per il software libero, il cui obiettivo è quello di promuovere software che tuteli la libertà dell'utenza e della comunità. Questo software viene denominato «libero» (in riferimento alla libertà e non al prezzo[1]). Taluni programmi proprietari come Photoshop sono eccessivamente costosi, altri come Flash Player sono gratuiti; a prescindere, in entrambi i casi l'utente viene sottomesso al controllo del produttore del software.

Parecchie cose sono cambiate dalla nascita del movimento. Nei paesi sviluppati del mondo odierno chiunque possiede un computer (a volte chiamati «telefonini») con cui collegarsi a Internet. Da una parte, il software privativo continua imponendo il controllo altrui sui compiti informatici dei diversi utenti, dall'altra però, è ora possibile imporre tale controllo anche attraverso il «servizio come surrogato del software», ovvero *Service as a Software Substitute* (SaaSS), che permette a un server altrui di eseguire tali compiti.

Entrambi, software privativo e SaaSS, possono spiare, incatenare e perfino attaccare i loro utenti. I frequenti abusi nei servizi e prodotti del software proprietario sono possibili proprio perché gli utenti non hanno nessun controllo su di essi. Infatti, questa è la differenza fondamentale: tanto il software privativo come i SaaSS sono sotto il controllo altrui (spesso corporazioni oppure lo Stato). Mentre il software libero, al contrario, offre in mano a tutti i suoi utenti tale potere.

Perché il controllo è così importante? Perché la libertà implica poter assumere il controllo della propria vita. Impiegando un software per svolgere delle attività attinenti alla tua vita, la tua libertà dipenderà esclusivamente dal controllo che puoi esercitare su di esso. Meriti d'avere tutto il controllo sui programmi che utilizzi, soprattutto se vengono impiegati per realizzare dei compiti a te indispensabili.

Affinchè l'utenza possa assumere il controllo dei programmi impiegati sono indispensabili quattro libertà essenziali.

1. Libertà di eseguire il programma come si desidera, per qualsiasi scopo.
2. Libertà di studiare il codice sorgente del programma e di modificarlo in modo da adattarlo alle proprie necessità. I programmatori scrivono i programmi in un determinato linguaggio di programmazione (qualcosa di simile all'inglese combinato con l'algebra), cosa che viene denominata «codice sorgente». Chiunque sia in grado di programmare e abbia a sua disposizione il codice sorgente del programma può leggere tale codice, capire i suoi meccanismi e dunque modificarlo. Invece, quando si ha unicamente a disposizione il programma come eseguibile binario (cioè, una lista di numeri eseguibili dal computer, ma difficilmente decifrabile per noi umani), capire il programma e modificarlo a piacere diventa un compito al quanto complesso.
3. Libertà di ridistribuire copie del programma in modo da aiutare il prossimo. Questo ovviamente non è in assoluto obbligatorio. Che il programma sia libero non implica che uno è costretto a facilitare delle copie oppure che siano facilitate a noi. Mentre distribuire programmi senza le dovute libertà è un affronto verso l'utenza, la non distribuzione e l'uso privato di essi non rappresenta nessun danno altrui.
4. Libertà di migliorare il programma e distribuirne pubblicamente i miglioramenti da voi apportati.

Le due prime libertà garantiscono ad ogni utente la possibilità di esercitare individualmente il controllo sul programma. Le altre due invece, permettono a un qualunque gruppo di utenti esercitare un controllo collettivo su di esso. L'intero insieme delle libertà permettono che l'utenza assuma tutto il controllo sul programma. Se qualcuna di queste libertà manca, o non sono attendibili, il programma risulta dunque privativo/proprietario (non libero) e quindi iniquo.

In diverse ambiti pratici vengono impiegate anche opere di vario genere, tipo ricette di cucina; materiale didattico (libri di testo, manuali, dizionari ed enciclopedie); tipi di caratteri; diagrammi circuitali per la produzione hardware; oppure stampanti 3D per la manifattura di oggetti funzionali (non necessariamente ornamentali). Anche se tutte queste ed altre opere non appartengono alla categoria del software, il movimento del software libero tenta di accogliere questo vasto insieme in senso lato, cioè applicando su di esse lo stesso ragionamento di base e raggiungendo la stessa conclusione: tutte queste opere devono garantire le quattro libertà essenziali.

Il software libero permette di smanettare e aggiungere delle modifiche a un determinato programma, così da fargli realizzare quel che a noi serve (oppure di farlo smettere di fare ciò che a noi non interessa). Smanettare il software può risultare fuori luogo per chi è abituato alle scatole chiuse del software privativo, ma nel mondo del software libero è consuetudine, nonché rappresenta un ottimo modo per imparare a programmare. Persino il passatempo di aggiustare le proprie macchine, usanza nei paesi nordamericani, viene ostacolato dal fatto che ora le vetture portano all'interno del software privativo.

L'ingiustizia del privativo

Se gli utenti non controllano il programma, è il software a controllare loro. Nel caso del software privativo, esiste sempre un'entità (il «proprietario» del programma) che controlla il programma, tramite il quale usa il suo potere a discapito degli utenti. Un programma che non è libero è dunque oppressore, uno strumento di potere ingiusto.

Nei casi estremi (ormai diventati consueti), i programmi privativi sono progettati per spiare, limitare, censurare e approfittarsene dei loro utenti. Cosa che vien fatta, ad esempio, dal sistema operativo degli i-cosi[2] di Apple e anche dai dispositivi mobili Windows con processori ARM. I firmware dei telefonini, il navigatore Google Chrome per Windows e lo stesso sistema operativo, includono una backdoor universale che permette a una certa azienda di modificare programmi in modalità remota senza bisogno di permessi. Il Kindle di Amazon permette la cancellazione dei libri tramite un'apposita backdoor.

Col proposito di finire con l'ingiustizia del software privativo, il movimento per il software libero sviluppa programmi liberi così da garantire agli utenti le proprie libertà. Movimento che nasce con lo sviluppo del sistema operativo libero GNU nel 1984. Ad oggi, milioni di computer funzionano con GNU, principalmente con la combinazione GNU/Linux.

Distribuire programmi senza concederne le dovute libertà, implica un maltrattamento verso gli utenti. La non distribuzione di un programma, invece, non genera danni per nessuno. Cioè, se scrivi un software e l'usi privatamente non è un affronto per nessuno. In quel caso, sprechi la possibilità di favorire qualcun altro, cosa che però è ben diversa da fargli del male. Quando affermiamo che tutto il software deve essere libero, intendiamo che tutte le copie di un programma messe a disposizione ad altri devono concedere le quattro libertà essenziali, e non che tutti coloro che sviluppano programmi devono concedere obbligatoriamente delle copie in giro ad altre persone.

Software privativo e SaaSS

Il software privativo è stato il primo mezzo impiegato dalle aziende per prendersi il controllo dei compiti informatici delle persone. Oggi tale controllo viene anche imposto attraverso il «servizio come surrogato del software», ovvero *Service as a Software Substitute* (SaaSS), che permette a un server altrui di eseguire tali compiti.

Anche se di solito i programmi all'interno dei server fornitori di SaaSS sono proprietari, tali server possono anche includere o essere interamente progettati utilizzando software libero. Purtroppo, l'utilizzo in sé dei SaaSS provoca le stesse ingiustizie inerenti all'utilizzo del software privativo: sono due percorsi che portano alla stessa cattiva fine. Si consideri, per esempio, un SaaSS per le traduzioni: l'utente invia una o varie frasi al server, il server traduce (per esempio dall'inglese all'italiano) e poi reinvia il testo tradotto all'utente. In questo modo, il compito di traduzione è sotto il controllo dell'amministratore del server e non dell'utente.

Se usi un SaaSS, chi controlla il server controlla anche i tuoi compiti informatici. Ciò implica affidare tutti i dati necessari all'amministratore del server, che può essere costretto a fornire tale informazioni allo Stato o a terzi; quindi, a chi serve veramente tale servizio?

Ingiustizie primarie e secondarie

Impiegando programmi privativi o SaaSS si provoca un danno, poiché concedi ad altri un potere iniquo su te. Per il proprio bene si dovrebbe evitarne l'uso. Se l'utente acconsente di "non condividere" si danneggiano anche gli altri. Accettare questo tipo di compromesso è un male, smettere è meno peggio, ma per essere sinceri, la cosa giusta è non iniziare affatto.

Ci sono situazioni in cui l'uso del software privativo incoraggia altre persone a farne uso. Skype è un chiaro esempio: se qualcuno impiega il loro client, forza altre persone a farne uso a discapito delle proprie libertà. Anche Google Hangouts presenta lo stesso problema. È del tutto sbagliato proporre software di questo genere. Infatti, dobbiamo rifiutarci di utilizzare questi programmi, anche per pochi istanti, perfino nei computer di altri individui.

Riassumendo, si può dire che l'impiego di programmi privativi e SaaSS consente di: propagarli, promuovere lo sviluppo di tale programma o «servizio» e forzare sempre più persone a sottostare al dominio della azienda proprietaria. Nel caso un cui l'utente corrisponde a un ente pubblico o una scuola, i danni indiretti - in tutte le sue forme- raggiungono maggiori proporzioni.

Il software libero e lo Stato

Gli enti pubblici sono stati concepiti per i cittadini, e non come istituzioni a sé stanti. Per tanto, tutti i compiti informatici che svolgono, li svolgono facendo le veci dei cittadini. Hanno dunque il dovere di mantenere il totale controllo su tali compiti ai fini di garantire la loro corretta esecuzione in beneficio dei cittadini. È questa, infatti, la sovranità informatica dello Stato. Motivo per cui nessun ente deve mai permettere che il controllo dei compiti informatici dello Stato venga delegato a interessi privati.

Per avere un totale controllo delle mansioni informatiche svolte a favore dei cittadini, gli enti pubblici non devono impiegare software privativo (software sottoposto al controllo di entità non statali). Neppure devono delegare lo svolgimento di tali compiti a un servizio programmato ed eseguito da entità non attinenti allo Stato, poiché in questo modo farebbero uso di SaaSS. Il software privativo non offre protezione alcuna contro una minaccia fondamentale: il suo sviluppatore, che potrebbe facilitare terzi a portare a compimento un attacco. Prima di correggere gli errori di Windows, Microsoft li fornisce a alla NSA, la agenzia di spionaggio digitale del governo degli Stati Uniti (si veda a proposito www.arstechnica.com/security/2013/06/nsa-gets-early-access-to-ze-ro-day-data-from-microsoft-others/). Non abbiamo conoscenza se Apple fa lo stesso, ma è sempre sotto la stessa pressione statale di Microsoft.

Software libero e l'educazione

Le scuole (e tutte le istituzioni educative a sua volta) influiscono sul futuro della società tramite i loro insegnamenti. Nel campo informatico, per garantire che tale influenza sia positiva, queste dovrebbero insegnare unicamente software libero. Insegnare l'uso di un programma proprietario equivale ad imporne la dipendenza, azione del tutto contraria alla missione educativa. Incentivando l'uso tra gli studenti di software libero, le scuole raddrizzano il futuro della società verso la libertà, e aiuteranno alla formazione di programmatori di talento.

Inoltre, così facendo, le scuole trasmetterebbero agli studenti l'abitudine di cooperare ed aiutare agli altri. Le scuole, a cominciare dalle elementari, dovrebbero dire agli studenti: «Cari studenti, questo è un luogo dove condividere il sapere. Se porti a scuola del software devi dividerlo con gli altri bambini. Devi mostrare il codice sorgente ai compagni, se qualcuno vuole imparare. Quindi è vietato portare a scuola software proprietario se non per studiare come funziona ai fini di poterlo riprodurre».

Seguendo gli interessi degli sviluppatori di software privativo, gli studenti non potrebbero né acquisire l'abitudine di condividere il software né sviluppare le capacità per modificarli, qualora ci fosse la curiosità ed interesse tra loro. Cosa che implica una mala formazione accademica. Nella sezione http://www.gnu.org/education/ è possibile trovare informazione dettagliata riguardo l'uso del software libero nelle istituzioni educative.

Software libero: molto più che «vantaggioso»

Molto speso mi viene chiesto di descrivere i «vantaggi» associati al software libero. Il termine «vantaggi» però è del tutto insignificante quando si parla di libertà. La vita senza libertà è tirannia, cosa che si applica tanto alla informatica come a qualunque altra attività attinente alla nostra vita. Dobbiamo rifiutarci di concedere il controllo dei nostri compiti informatici ai proprietari di programmi o servizi informatici. E quel che deve essere fatto, per ragioni egoistiche o no. < uno dei motivi per cui non sono una scelta ne di destra ne di sinistra>

La libertà implica la possibilità di cooperare con altri. Negare tale libertà è sinonimo di voler dividere le persone, che porta unicamente ad opprimerle. Nella comunità del software libero siamo molto consci dell'importanza della libertà di cooperare, appunto perché il nostro lavoro corrisponde a una cooperazione organizzata. Se un qualche conoscente viene a trovarti e ti vede usare un programma nel frattempo, questa persona potrebbe chiederti una copia di esso. Qualunque programma che impedisce la sua libera distribuzione, o ti impone l'obbligo che «non devi cooperare» , è antisociale.

In informatica, la cooperazione implica la distribuzione della stessa copia di un programma fra diversi utenti. Ma a sua volta, implica anche la distribuzione delle sue versioni modificate. Il software libero promuove queste forme di cooperazione, mentre quello privativo le vieta. Anche il SaaSS impedisce di cooperare: se deleghi i tuoi compiti informatici a un servizio web custodito in un server altrui, mediante una copia di un programma altrui, non puoi nè vedere nè toccare il software impiegato per realizzarli, e quindi non puoi né distribuirlo liberamente né modificarlo.

Conclusioni

Tutti noi meritiamo di avere il controllo della nostra vita informatica. Come possiamo ottenerlo? Rifiutandoci di impiegare software privativo nei nostri computer oppure quelli di uso frequente, e anche, rifiutando i SaaSS; sviluppando software libero (per chi lavora nel campo della programmazione); rifiutando di sviluppare o promuovere software privativo o SaaSS e diffondendo queste idee.

Noi, e altri migliaia di utenti, continuiamo a farlo sin dal 1984, e grazie a questo sforzo oggi abbiamo il sistema operativo libero GNU/Linux, che tutti -programmatori e non- possono usare. Unitevi alla nostra causa, ben sia come programmatore oppure attivista. Facciamo in modo che tutti gli utenti di computer siano liberi.

Richard Matthew Stallman

Programmatore statunitense e fondatore del movimento per il software libero nel mondo. Tra i suoi meriti di programmazione all'interno del progetto GNU spiccano la realizzazione dell'editore di testo Emacs, il compilatore GCC e il debugger GDB. È principalmente conosciuto per lo sviluppo del quadro di riferimento morale, politico e legale all'interno del movimento del software libero, come alternativa di sviluppo e distribuzione al software proprietario. È stato anche l'inventore del concetto di copyleft (anche se non del termine), metodo per concedere in licenza il software garantendo che tanto il suo utilizzo, come ulteriori modifiche, rimangano libere e sempre a portata della comunità di utenti e sviluppatori.

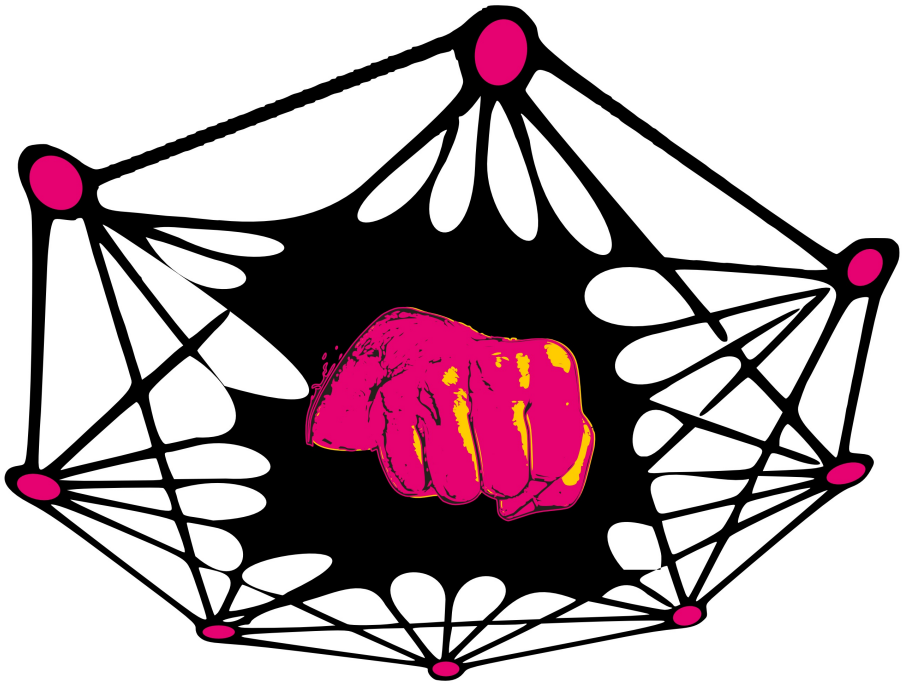
NOTE

> [1]. In inglese, il termine «free» può significare «libero» oppure «gratuito». ↩

> [2]. Presso da «iThings», termine dispregiativo per fare riferimento ad aggeggi tipo iPod, iPad, iPhone, ecc. ↩

Internet libera e reti mesh

Benjamin Cadon



La questione della sovranità tecnologica si manifesta con particolare intensità quando abbiamo a che fare con Internet e con la nostra capacità di accedervi liberamente per una serie di utilizzi, da semplici comunicazioni interpersonali allo scambio di dati, all'uso di applicazioni web di condivisione di mezzi e di organizzazione collettiva. In questo articolo tratteremo la problematica soprattutto dalla prospettiva della "rete", partendo dal globale per poi considerare le iniziative su scala locale.

Innanzi tutto, possiamo parlare della storia di Internet. Internet nasce negli Stati Uniti, avviata grazie a finanziamenti militari, ampliata da universitari e appassionati di informatica prima di estendersi in tutto il pianeta… e quindi possiamo iniziare a porci domande sulla sua gestione. Dall'ultimo Incontro Globale sulla Società dell'Informazione (WSIS, World Summit on the Information Society), che ebbe luogo in Tunisia nel 2005, Internet è regolata dall'Internet Governance Forum, sotto la sigla dell'Organizzazione delle Nazioni Unite (ONU).

Questa organizzazione mondiale non puó nascondere il fatto che, da un punto di vista tecnico, alcune istanze, al cuore della rete, sono finite sotto l'egemonia nordamericana. In particolare pensiamo all'ICANN (Internet Corporation for Assigned Names and Numbers)[1] : una società di diritto californiana senza scopi di lucro, sotto la tutela del Dipartimento del Commercio degli Stati Uniti, che gestisce i server DNS "a grappolo" (i .net, .org, .com) e attribuisce gli indirizzi "IP"[2]. Questi indirizzi identificano tutti i computer che sono presenti nella rete. Bisogna segnalare che varie iniziative per creare un sistema di DNS decentralizzato (DNS P2P), tra le quali quella di Peter Sunde, cofondatore di The Pirate Bay[3], non hanno ottenuto fino a ora un'estensione significativa. Dobbiamo anche considerare la "censura dei DNS" come per esempio l'intervento dei servizi americani per interrompere le attività di Megaupload[4], o quella del "governo attraverso la rete" come segnaló il collettivo artistico "Bureau d'etudes".[5]

Perché bisogna difendere la neutralità di Internet?

Ripassiamo rapidamente alcuni trattati e tentativi internazionali, europei e nazionali (TAFTA, CETA, ACTA, SOPA, PIPA, Regolamento dell'Unione Internazionale delle Telecomunicazioni (ITU), DAVDSI in Europa, legge Sinde in Spagna, LOPSI e Hadopi in Francia etc.) che pretendono di mettere ostacoli alla neutralità della rete per poterla "filtrare". Secondo il collettivo "La Quadrature du Net"[6] : "la neutralità della rete é un principio fondatore di Internet che garantisce che gli operatori delle telecomunicazioni non discriminino le comunicazioni dei loro utenti, e si comportino come semplici trasmettitori di informazioni. Questo principio permette a tutti gli utenti, indipendentemente dai loro mezzi, di accedere alla stessa rete nella sua totalità". Per molti e spesso discutibili motivi[7], alcuni trattati e progetti di legge provano a fabbricare strumenti legali per obbligare i fornitori di accesso o di strumenti di rete, e/o i contributori, a intervenire nell'accesso a certi contenuti per poterli filtrare, e quindi discriminare.

La possibilità di accedere liberamente e pienamente a Internet puó anche vedersi influenzata da considerazioni strategico-commerciali dei provider, i quali, con le tecnologie Deep Packet Inspection (DPI), hanno la capacità di favorire certi contenuti piuttosto che altri. La DPI consiste nell'aprire tutti i pacchetti che contengono i dati scambiati con i server e gli altri utenti per valutarne il contenuto e decidere la loro spedizione rapida o, al contrario, indirizzarli verso una strada morta o un ascoltatore prescelto. Gli interessi dei provider commerciali di accesso a Internet sono molteplici: permettono di pensare a offerte di accesso con varie velocità, per esempio, per limitare la quantità di banda dei servizi piú pesanti e meno redditizi (ad esempio YouTube) o per far pagare un accesso privilegiato a questi servizi con l'obiettivo di garantire la buona ricezione dei segnali televisivi che circolano ora via Internet, o la qualità dei servizi telefonici con IP^8. Bisogna sottolineare come queste tecnologie di "DPI" sono usate anche dai fabbricanti di armi numeriche per mettere sotto vigilanza un intero paese in rivolta (ad esempio la Libia, aiutata dai tecnici e dal software Eagle sviluppato dall'impresa francese Ameys Bull[9]).

La neutralità di Internet, un principio da difendere da un punto di vista tecno-politico

Alcuni stati puntano, ancora molto timidamente, a garantire un accesso libero e completo a Internet. Dopo il Cile[10] é il caso, per esempio, dei Paesi Bassi dove il parlamento ha adottato una legge sulla neutralità di Internet all'inizio del mese di Maggio 2012[11], mentre l'Unione Europea continua a sorvolare sul tema[12]. In alcuni paesi, le amministrazioni pubbliche hanno la possibilità giuridica di assumere il ruolo di Internet provider e proporre un servizio di qualità a prezzi piú bassi per le fasce di popolazione meno avvantaggiate (ad esempio la Régie Communale du Câble et d'Electricité de Montataire in Francia[13]) o che si trovano in zone in cui non arrivano i provider commerciali perché poco profittevoli (le "zone bianche"). Fino a ora, almeno in Francia, le amministrazioni sono state piú rapide a delegare l'ipianto delle reti di banda larga agli operatori commerciali di sempre che ad approfittare di questa opportunità per affrontare concretamente il futuro di Internet sotto il punto di vista dei beni comuni.

Alcuni attori della società civile si sono mobilizzati, da molto tempo, per difendere questo principio di fronte ai legislatori, come nel caso della "Quadrature du Net" che lo ha convertito in una delle sue priorità[14] e si presenta come una "organizzazione di difesa dei diritti e delle libertà dei cittadini di Internet. Promuove un'adattamento della legislazione francese ed europea che si mantenga fedele ai valori che hanno promosso lo sviluppo di Internet, soprattutto la libera circolazione della conoscenza. In questo senso, la Quadrature du Net interviene nei dibattiti sulla libertà di espressione, il diritto d'autore, le regolamentazioni del settore delle telecomunicazioni e anche il rispetto della vita privata. Consegna ai cittadini interessati strumenti che permettano loro di comprendere meglio i processi legislativi e partecipare efficacemente al dibattito pubblico".[15]

Comunità per una Internet accessibile, libera e aperta

Esistono varie tipologie di associazioni, ONG e comunità che militano in forma attiva e (in maniera) pratica per proporre una rete neutrale. Si possono distinguere da un punto di vista tecnico secondo il modo di accesso proposto: dal dotarsi di un router per connettersi a una rete cablata o, ancora meglio, all'installare un sistema wifi integrato in una rete mesh a sua volta interconnessa a Internet. In linguaggio tecnico, "Asymmetric digital Subscriber Line" (linea di abbonamento digitale asimmetrica, ADSL) oppure Wi-Fi, una banda libera dello spettro elettromagnetico.

Linea di abbonamento digitale asimmetrica

Possiamo citare come esempio francese la French Data Network (FDN)[16], creata nel 1992 come associazione per offrire a tutti e a minor prezzo quello che altri usavano come strumento di lavoro dall'inizio degli anni ottanta. I servizi offerti da FDN hanno incluso la posta elettronica, le notizie, l'accesso a numerosi archivi di software e documentazione e alle macchine della rete Internet.

Uno dei vantaggi di FDN è la diversità dei suoi membri, con vecchi navigatori di Internet ben preparati tecnicamente e membri interessati a temi molto differenti (musica, legge, educazione, grafica etc.). Questo permette di promuovere una Internet di qualità, sia a livelli di servizi che di contenuti che ne rispettano l'etica iniziale. Partendo da questa volontà, FDN ha avviato in Francia una federazione di provider associati per l'accesso a Internet (FFDN), che al momento comprende 23 membri[17] e che cerca di facilitare lo scambio su problematiche tecniche e politiche. La creazione di un FAI (" fournisseur d'accès a Internet ": fornitore di accesso a Internet) associativo[18] sembra relativamente sensata (vedere "come diventare il proprio FAI[19]„[20]) soprattutto quando strutture come la FFDN si profilano per accompagnare e dinamizzare questa iniziativa. Ci rimane il problema del "circuito locale", ovvero gli ultimi chilometri del cavo, e un domani della fibra ottica, che arrivano fino alla nostra casa, e che appartengono a un numero limitato di operatori con i quali bisogna giungere a un accordo. Una problematica dalla quale restano esenti le reti wireless.

Il Wi-Fi, una banda libera dello spettro elettromagnetico

Con il cambiamento della legislazione, all'inizio del 2000, in alcuni paesi, si rendeva possibile l'utilizzo di apparati di comunicazione wireless liberamente, senza dover chiedere nessun tipo di autorizzazione o licenza. Molti paesi limitarono la potenza ammessa e aprirono piú o meno "canali" in una banda di radiofrequenza che si chiama "Industriale, Scientifica e Medica" (ISM[21]) che si trova tra i 2.4 e i 2.4835 Ghz. Al tempo stesso, in alcuni paesi, esiste la possibilità di usare frequenze attorno ai 5Ghz.

A partire da qui, si sono iniziate a creare comunità Wi-Fi, tanto nelle città per essere piú autonomi, mutualisti e liberi rispetto ai fornitori di accesso, cosí come nelle campagne per coprire "zone bianche" senza connessione a Internet e considerate come "non profittevoli" per gli operatori privati e pubblici. Bisogna menzionare in Europa: Freifunk[22] in Germania, Funkefeuer[23] in Austria o Guifi.net[24] in Catalogna, tra molte altre[25]. Sono molto eterogenee, includendo da pochi utenti in zone isolate fino a decine di migliaia di "nodi" distribuiti in zone piú dense, su scala cittadina, regionale o nazionale.

In maniera schematica, i membri costituiscono un punto di accesso e un ripetitore dentro una rete mesh configurando un router Wi-Fi in maniera adeguata. Questa rete si connette a Internet tramite uno o piú accessi personali o condivisi: un'antenna fa da collegamento con zone distanti svariati chilometri dove un'altra piccola rete puó essere sviluppata. Si tratta quindi di distribuire nella maniera piú decentralizzata possibile l'accesso a Internet e a risorse informatiche "locali" (siti web, servizi di posta elettronica, strumenti di telecomunicazione etc.), cioé preposte in uno dei server direttamenti connessi a uno o piú nodi di questo intreccio elettromagnetico.

Una delle piú antiche comunità Wi-Fi in Europa, Freifunk ("radio libera"), nata nel 2002, creó un proprio sistema operativo per routers, il Firmware Freifunk, e il proprio protocollo di routing B.A.T.M.A.N.[26], oggi in uso su scala mondiale come base per costruire reti mesh e ottimizzare in queste la circolazione di pacchetti. Fece anche parte della costituzione di una rete internazionale di comunità che condividono gli stessi valori, spesso vicini a quelli del software libero, con la stessa voglia di distribuire, "decentralizzare", nella dimensione possibile, i mezzi della rete che si considerano come un bene comune al quale tutti possano accedere.

L'abbassamento dei prezzi dei router Wi-Fi (fatti nella Repubblica Popolare Cinese[27]) aiutó lo sviluppo di questa tipologia di iniziativa che alcuni vedono come il futuro di Internet: una rete decentralizzata, stabile, con una intelligenza multiforme e condivisa, che si adatta a tutto quello che puó succedere socio-tecno-ecologicamente in ogni contesto. Sicuramente esistono rivendicazioni a proposito della questione della "liberazione delle frequenze"[28], perché anche agli operatori privati fanno comodo queste onde "gratuite", sia per poter far comunicare tra di loro oggetti suppostamente intelligenti, sia per trasmettere la telefonia

mobile attravero il cavo di Internet di casa; alcune ora chiamano questa banda di frequenza la “banda bassa”. Ora quindi possiamo considerare questa risorsa elettromagnetica come un bene comune, mettendo la società al centro del processo di scambio, ben oltre l’influenza degli Stati e delle aziende sulle frequenze. Organismi come “Wireless commons” stabilirono un manifesto e una lista di punti comuni che potessero caratterizzare queste organizzazioni, e il fondatore di Guifi.net pubblica dal 2005 il Comun Sesefils[29] (Licenza Comune Wireless) < (????) >.

Artisthackers sperimentano con altre “reti”

Presentiamo alcune iniziative che contribuiscono alla problematica della sovranità tecnologica dalla questione dell’accesso a un sistema di comunicazione e di scambio aperto, accessibile e anonimo:

Workshops sul fai da te < (???) >

Negli hackerspace e in altri medialab, o per dirlo in altro modo, nei luoghi di riappropriazione della tecnologia, si realizzano workshop, piú o meno regolarmente, per essere piú autonomi di fronte alle proprie necessità informatiche: come avere i propri server web/mail in casa; come cifrare le proprie comunicazioni; aggirare possibili sistemi di filtraggio e schivare, per quanto possibile, gli ascoltatori indesiderati; come gestire i propri dati personali, la sicurezza del computer etc.

I “Battle mesh”

In questo stesso tipo di luoghi, si organizzano “wireless battle mesh”[30], riunioni di specialisti amatoriali in comunicazioni di reti wireless, che nel corso di diversi giorni e sotto forma di un gioco, di una battaglia, testano vari protocolli e provano a ottimizzare il funzionamento di una rete mesh per aquisire esperienze e abilità, interfacciandosi con altri partecipanti che condividono queste problematiche tecniche.

“Qaul.net” di Christoph Wachter e Mathias Jud

Qaul.net implementa un principio di comunicazione aperta nella quale computer e apparati mobili equipaggiati di scheda Wi-Fi possono formare in maniera spontanea una rete tra di loro, e permettere lo scambio di testi, files e chiamate vocali senza dover passare attraverso Internet o una rete di telefonia mobile. Questo progetto “artistico” è stato immaginato in reazione ai “blackout” di comunicazione imposti da regimi oggetto di rivolte all’interno del paese, o nel caso in cui catastrofi naturali distruggano le infrastrutture di rete.

“Batphone” o “Serval Mesh”

L’obiettivo di questo progetto è di trasformare ogni telefono cellulare con il Wi-Fi in un telefono Wi-Fi, cioè in un mezzo di comunicazione che, appoggiandosi alle strutture wireless esistenti, permetta la comunicazione con altre persone all’interno della rete senza passare dalla casella dell’operatore e senza aver bisogno di una scheda SIM.[31]

“Deaddrop” di Aram Barthol

Il progetto consiste nel cementare in una parete una chiave USB e condividere la sua localizzazione in una mappa apposita lanciata sulla rete dall’artista[32]. Si tratta di un’appropriazione della cassetta delle lettere usata da generazioni di spie per comunicazioni senza contatto fisico. Si tratta di un modo di creare un luogo di scambio anonimo, da persona a persona, disconnesso da Internet e impiantato nello spazio pubblico. I “deaddrops” si sono diffusi in (quasi) tutto il pianeta e dichiarano di avere al momento 7144 GB di dati salvati < storage (???) >. Incidentalmente possono prendere freddo o riempirsi di virus.

“Piratebox” di David Darts

La Piratebox[33] ripropone questo stesso princio di cassa di deposito anonima proponendo una rete Wi-Fi aperta nella quale tutte le persone che si connettono e aprono un browser Internet si vedono diretti verso una pagina che propone il caricamento dei propri file, e la consultazione e scaricamento dei file depositati precedentemente. Questa “micro-Internet” è disconnessa dalla grande Internet, non registra i “logs” e garantisce, quindi, confidenzialità. Si puó accedere al sistema in una radio che ha a che vedere con il posizionamento e la qualità dell’antenna utilizzata, si puó installare in un router Wi-Fi a basso costo come il

micro computer Raspberry Pi e aggiungerle una chiave Wi-Fi, o in un computer tradizionale, o in un telefono cellulare. Partendo da questo dispositivo, la comunità degli utilizzatori ha immaginato molte evoluzioni[34] : la “Library Box” per condividere libri liberi dal diritto d’autore in una biblioteca, il “Micro Cloud” per tenere i documenti a portata di mano, la “OpenStreetMap Box” per consultare risorse cartografiche libere “offline”, la T.A.Z. Box, la Pedago-Box, la KoKoBox, etc.

Conclusioni

Tra quello che è in gioco a livello internazionale e le disuguaglianze locali, è possibile che sia conveniente tenere a mente uno dei principi fondatori di Internet, “distribuire l’intelligenza”. Si rende necessario evitare la centralizzazione tecnica e decisionale per rivolgerci, invece, verso uno scambio aperto delle conoscenze e dei dispositivi tecnici, e la difesa collettiva dell’idea per cui Internet sia un bene comune al quale si deve poter accedere liberamente. Possiamo immaginare che ogni mattina, ognuno potrà cercare Internet nella casa della sua artigiana di reti locale, come le verdure succulente che coltiva con amore un produttore appassionato. Internet non deve essere la scatola nera chiusa poco a poco da un ristretto numero di persone, ma deve essere considerata come un oggetto tecnico di cui appropriarsi, del quale è necessario mantenere il controllo, che va coltivato collettivamente nella sua diversità e affinché ci nutra con degli ottimi bytes.

Benjamin Cadon

Artista e coordinatore di Labomedia, mediahackerfablabspace senza scopo di lucro basato a Orléans, Francia.

http://labomedia.org benjamin[at]labomedia[dot]org

NOTE

1. In italiano: https://it.wikipedia.org/wiki/ICANN

2. Un indirizzo IP chiamato “pubblico” è quello che permette a un computer di accedere a Internet e di parlare lo stesso linguaggio (il protocollo TCP/IP) per scambiare con suoi affini: server, personal computers, terminali mobili e altri oggetti chiamati “comunicanti”. I server DNS servono a trasformare questi indirizzi IP in nomi di dominio affinché i server sian piú accessibili agli umani e ai robot dei motori di ricerca.

3. “Un DNS in peer-to-peer ?” - Stéphane Bortzmeyer - http://www.bortzmeyer.org/dns-p2p.html

4. MegaUpload Shut Down by the Feds, Founder Arrested » - http://torrentfreak.com/megaupload-shut-down-120119/

5. http://bureaudetudes.org/2003/01/19/net-governement-2003/

6. http://www.laquadrature.net

7. Con “motivi discutibili” ci riferiamo al fatto di nascondere le offensive contro la neutralità della rete sotto il pretesto di voler proteggere la proprietà intellettuale e il diritto d’autore, prevenire il terrorismo e l’aumentare degli estremismi, o anche la lotta contro la pedofilia e altri comportamenti predatori nella rete. Non diciamo che questi problemi non esistono, ma provare a risolverli attraverso restrizioni della libertà in rete, dove la neutralità è un principio base, è un errore fondamentale.

8. VOIP: https://es.wikipedia.org/wiki/VOIP

9. http://reflets.info/amesys-et-la-surveillance-de-masse-du-fantasme-a-la-dure-realite/

10. http://www.camara.cl/prensa/noticias_detalle.aspx?prmid=38191

11. http://www.numerama.com/magazine/22544-la-neutralite-du-net-devient-une-obligation-legale-aux-pays-bas.html

12

12. http://www.laquadrature.net/fr/les-regulateurs-europeens-des-telecoms-sonnent-lalarme-sur-la-neutralite-du-net. Vedere anche la campagna: http://savetheinternet.eu/fr/

13. http://www.rccem.fr/tpl/accueil.php?docid=2

14. http://www.laquadrature.net/fr/neutralite_du_Net

15. http://www.laquadrature.net/fr/qui-sommes-nous

16. http://www.fdn.fr/

17. http://www.ffdn.org/fr/membres

18. Una mappa dell'evoluzione dei FAI : http://www.ffdn.org/fr/article/2014-01-03/federer-les-fai-participatifs-du-monde-entier

19. http://blog.spyou.org/wordpress-mu/2010/08/19/comment-devenir-son-propre-fai-9-cas-concret/

20. http://blog.spyou.org/wordpress-mu/?s=%22comment+devenir+son+propre+fai%22

21. https://fr.wikipedia.org/wiki/Bande_industrielle,_scientifique_et_m%C3%A9dicale y https://es.wikipedia.org/wiki/Banda_ISM

22. http://freifunk.net/

23. http://www.funkfeuer.at/

24. http://guifi.net/

25. https://en.wikipedia.org/wiki/List_of_wireless_community_networks_by_region

26. http://www.open-mesh.org/projects/open-mesh/wiki

27. Si veda il contributo di Elleflane su "Hardware Libero" in questo dossier.

28. Allegato di Félix Treguer e Jean Cattan a favore della liberazione delle frequenze « Le spectre de nos libertés » (lo spettro delle nostre libertà): http://owni.fr/2011/05/07/le-spectre-de-nos-libertes/

29. Ver https://guifi.net/ca/CXOLN

30. http://www.battlemesh.org/

31. https://github.com/servalproject/batphone

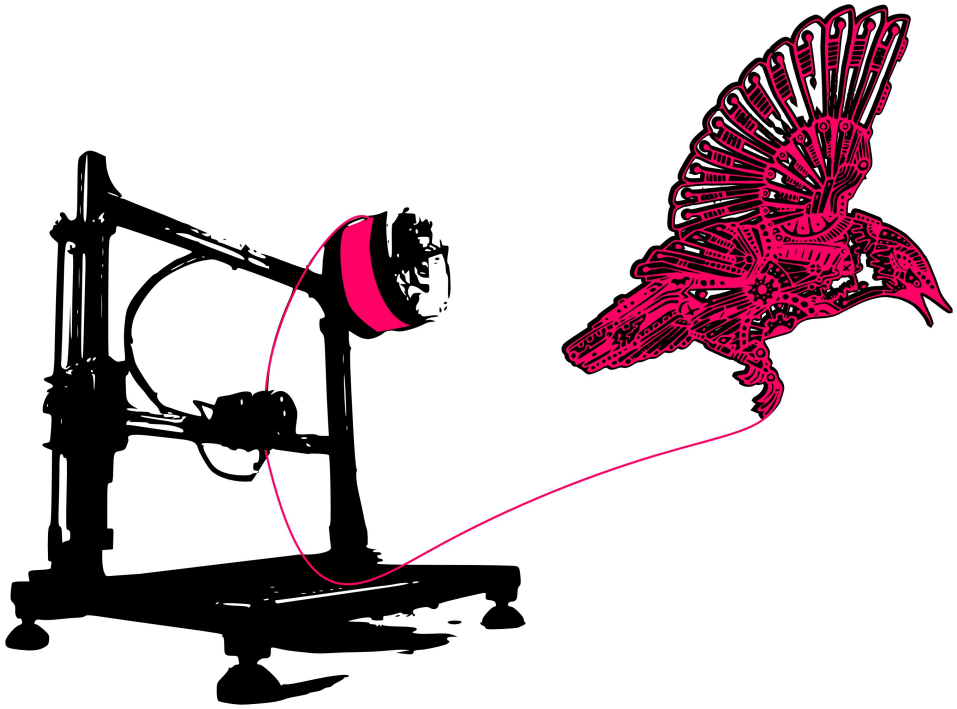
32. http://deaddrops.com/dead-drops/db-map/

33. http://daviddarts.com/piratebox/?id=PirateBox

34. http://wiki.labomedia.org/index.php/PirateBox#Projets_et_d.C3.A9tournements_de_la_PirateBox

Sull'hardware libero e il riappropriarsi della tecnologia

Elleflâne



Il concetto di hardware è abbastanza nuovo, molto ampio, in continuo rinnovamento e diametralmente diverso dal software. Vi è una vasta polemica su ciò che è e non é e grazie all'assenza di una definizione concordata ognuno lo interpreta un po' a modo suo. Ad esempio, per me, l'hardware comprende un componente elettronico, un condensatore, un transistor, un LED, un circuito integrato, un dispositivo quale un moto-aratro, la descrizione di un processo industriale, come la fabbricazione di un mattone refrattario, un computer, una stampante 3D, un meccanismo per la purificazione dell'acqua scritto in codice sorgente aperto, un processo per il riciclo della plastica, l'assemblaggio di una fresatrice CNC, un metodo di analisi dei suoli inquinati mediante sensori o il codice di un microcontrollore.

Ma se diamo una occhiata più da vicino, si può dire che la storia dell'Hardware Libero corre parallela a quella dei computer. Nel 1970, l'Homebrew Computer Club[1] si è rivelato essere un ibrido composto dal movimento studentesco radicale, imprenditori dalla comunità informatica dell'università di Berkeley e hobbysti elettronici. Appare un po' ironico vedere come molti di quei garage, prima pieni di creatività, sono ora musei, come quello di Bill Hewlett e Dave Packard, dove è stato sviluppato il primo dispositivo HP. Negli anni '90, nello stesso modo in cui programmi software venivano scambiati, l'FPGA [2] consentiva anche lo scambio elettronico di disegni liberi. La Open Design Circuits [3] lanciata da Reinoud Lamberts, è il primo sito web di una comunità di designer di hardware con lo spirito del software libero. E nonostante non ci fosse ancora un software libero adeguato per la progettazione elettronica, questo portale coinvolse molte persone ponendo le basi per una comunità più ampia. Nel 2002, l'iniziativa "Challenge to Silicon Valley" [4] promossa da Kofi Annan ha lanciato diversi progetti di sviluppo di hardware libero e reso più visibile la necessità di sviluppare tecnologie varie adeguate a realtà socioculturali ed economiche diverse. Quella linea di sviluppo della tecnologia si è anche miscelata con la lotta globale contro il divario digitale attraverso iniziative come ICT4Development. Queste erano generalmente il risultato di collaborazioni tra università e il terzo settore

per creare tecnologie adattate alle esigenze dei paesi erroneamente definiti "in via di sviluppo". Tuttavia, oggi le prospettive di produzione hardware sono principalmente caratterizzate dalle limitazioni imposte da brevetti industriali e proprietà industriale [5]. Questi sono l'insieme di diritti che pongono una persona fisica o giuridica sopra un'invenzione. Questi forniscono due tipi di diritti: il diritto di utilizzare l'invenzione, disegno o segno distintivo, e il diritto di vietare a terzi di farlo. Il diritto di vietare (Ius prohibendi) consente al titolare il diritto di richiedere il pagamento di una licenza, denominata royalty, o di canoni, avendo limiti temporali e territoriali.

Hardware Libero: Fin dove e in che modo?

Va tenuto presente che l'hardware libero richiede quasi tutte le seguenti parti: un disegno, un processo di produzione, alcune materie prime, la distribuzione, il modello di business, di manutenzione, distribuzione, replicabilità, la forza lavoro, l'accesso alla documentazione e tecnica di produzione. Partendo da questo contesto, se cerchiamo di definire ciò che è hardware libero abbiamo bisogno di vedere tutte le tappe di produzione sommate a tutti i tipi di risultati tangibili possibili che possano essere interpretati da licenze libere. Lo stesso Richard Stallman [6], presidente della Free Software Foundation [7] e creatore della GNU GPL [8] che garantisce le seguenti quattro libertà (la libertà di utilizzo, studio e modifica, la distribuzione e la redistribuzione delle versioni modificate), afferma anche che "le idee di software libero possono essere applicati ai file o agli archivi necessari per la progettazione e le specifiche (schemi, PCB, ecc), ma non al circuito fisico in sé" [9]. Va segnalato anche che c'è un hardware statico, comprendente gli elementi di sistemi materiali o tangibili elettronici, e un hardware riconfigurabile, composto da un linguaggio di descrizione hardware scritto in un file di testo che contiene il codice sorgente. Pertanto, le parole "hardware" e "progettazione hardware" sono due cose diverse. Il disegno e l'oggetto fisico non possono essere confusi anche se a volte si fondono reciprocamente. Tutti questi fattori creano confusione quando si cerca di descrivere che cos'è l'hardware libero. Se è vero che ogni componente e le fasi di produzione possono essere adatte alle quattro libertà specificate dal software libero, va detto che attualmente nessun progetto riesce a coprire l'intera catena con rigorosamente libert. Così ora usiamo il termine hardware libero/aperto, senza dover attuare le quattro libertà strettamente in tutte le aree. Ci sono molte iniziative consolidate in questo campo, anche se i modelli di utilizzo e l'approccio sono diversi a seconda delle motivazioni sociali, economici e politiche di ogni gruppo o di una comunità dietro il suo sviluppo. Di conseguenza, v'è una moltitudine di diverse licenze che cercano di chiarire questi aspetti. Ad esempio, il Free Hardware Design [10] è un disegno che può essere copiato, distribuito, modificato, e prodotto liberamente. Ciò non implica che il design non può essere venduto, o che qualsiasi pratica di progettazione hardware sia gratuita. Il Libre Hardware Design è uguale al Free Hardware Design, ma chiarisce che la parola "libre" si riferisce alla libertà, non al prezzo. L' Open Source Hardware [11] mette tutte le informazioni di progettazione a disposizione del pubblico in generale, e può essere basato su hardware di design libero, o limitato in qualche modo. L'Open Hardware [12], un marchio registrato della Open Hardware Specification Program, è una forma limitata di Open Source Hardware in quanto l'unico requisito è quello di fornire una quantità limitata di informazioni di progettazione per effettuare riparazioni. Infine, in un tentativo di sintesi, Patrick McNamara ha definito per l'Open Hardware i seguenti livelli di apertura:

1. Interfaccia aperta: l'utente ha tutta la documentazione che spiega come un pezzo di hardware svolge la funzione per cui è stato progettato.
2. Design aperto: la documentazione disponibile è sufficientemente dettagliata affinchè una terza parte possa creare un dispositivo funzionale e compatibile.
3. Fabbricazione aperta: disponibile l'elenco di tutti i materiali necessari per la costruzione del dispositivo.

Nello scenario attuale delle licenze, rispetto all'hardware libero ne esistono una grande varietà. Ci sono gruppi che usano la GNU GPL [13] come la Free Model Foundry [14] per la simulazione di modelli, componenti e testing; ESA Sparc [15] che hanno creato un CUP per 32bits o Opencores [16], una comunità che sviluppa IP core. Altri gruppi usano la licenza Open Source Initiative del MIT [17] come il Free-IP Project [18] e LART [19]; per quanto riguarda la licenza GNUBook [20], è basata sulla licenza GPL ma con aggiunte riguardanti i diritti ambientali ed umani. Esistono anche gruppi che sviluppano nuove licenze, come la Simputer GPL [21], Freedom CPU [22], OpenIPCores [23], la OHGPL [24], The Open NDA [25], la OpenPPC [26] (basata sulla Apple Public

Source License) e la Hardware Design Public License [27] del gruppo Open Collector [28]. Distinguiamo tra le altre la Licenza Hardware del CERN OHL [29] scritta originalmente per la progettazione del CERN (l'acceleratore di particelle) elecato nel Repository Open Hardware.

Modelli di business e sostenibilità derivati dall'open hardware

Secondo Wired, la Bibbia del tecnopositivismo, l'Open Hardware sta diventando una “commodity”, ovvero una merce. Anche se non esiste ancora un modello di business chiaro, si capisce che può servire mercati di nicchia che non sono stati finora coperti, applicando la logica della "long tail" coda lunga o distribuzione di beni e servizi hardware (il modello Amazon) dalle dimensioni pressoché infinite. Per quanto riguarda la commercializzazione, la progettazione in hardware libero può essere implementata da una società per promuovere il suo stesso mercato, la cui unica premessa è quella di mantenere il disegno libero. Nel 2010, Torrone e Fried [30] hanno raccolto 13 esempi di aziende che vendono Hardware Open Source fatturando tra tutti 50 milioni di dollari. Attualmente ci sono più di 200 progetti di questo tipo e si prevede che la comunità di Open Source Hardware fatturerà miliardi nel 2015. Adafruit [31], Arduino [32], Chumby [33], Liquidware [34] e Makerbot [35] hanno entrate pari a più di un milione di dollari ciascuno. Tutto questo dimostra che ci sono quindi le possibilità per generare reali guadagni economici con progetti che basano le loro attività sul far conoscere e condividere il design con la comunità.

Ora, ciò che è meno chiaro: E' possibile esercitare una vera politica anticapitalista sulla base di un progetto economico e di ri-distribuzione delle attività legate ad una logica di sostenibilità e decrescita? Un modello interessante per l'open hardware risiede nel crowdfunding [36], cioé nel raccogliere piccole quantità di individui o gruppi per avviare un progetto. Huynh e Stack hanno creato, ad esempio, la Open Source Hardware Reserve Bank [37] per coprire i costi connessi alle revisioni hardware in corso durante un progetto, stimate quasi il 40% del bilancio iniziale necessario. Il progetto mira a ridurre i rischi per i progetti di hardware libero per passare alla fase di produzione. Inoltre facilitano la sperimentazione consentendo la costruzione e la distribuzione di piccole quantità di prodotti considerati "non scalabili", perché "una cattiva idea di business" non è la stessa cosa che "una brutta idea hardware".

Un altro esempio è l'Open Source Hardware Reserve Bank che permette solo agli hackers, non agli investitori di capitali di rischio o di altre società, di investire in progetti specifici per raddoppiare il numero di pezzi prodotti e riducendo il costo unitario dal 10 al 30% circa. Da notare anche che una comunità può anche autofinanziare i suoi progetti attraverso il microcredito. Open money [38] e Metacurrency [39] propongono nuovi formati di valuta, e cercano di promuovere il legame di monete esistenti con certificati di microcredito.

E infine, l'Open Design Manifesto [40] che unisce le due tendenze. Da un lato, le persone applicano le loro competenze e il tempo in progetti per il bene comune che di solito non esistono a causa della mancanza di interesse commerciale. D'altra parte, fornisce un quadro di riferimento per lo sviluppo di progetti e tecnologie avanzate che potrebbero essere al di là delle risorse di qualsiasi azienda o paese e coinvolge la gente che senza il meccanismo del copyleft non si sentirebbe motivata a collaborare. Vediamo ora che esistono problemi per quanto riguarda la sostenibilità dell'hardware libero.

Da un lato, la mancanza di consenso sulla definizione di hardware libero è applicata anche ai possibili modelli di business. Un dispositivo aperto è diverso da ciò che esiste e domina il mercato e la cosa importante non è il prodotto finito (hardware prodotto), ma le attività immateriali, le informazioni riguardanti la progettazione dell'hardware che si apre all'uso pubblico. Inoltre, come si è visto in precedenza nell'hardware libero non i possono applicare direttamente le quattro libertà del software libero, data la sua natura diversa, uno ha una esistenza fisica, materiale, l'altro no. Pertanto, un progetto fisico è unico e la condivisione dipende dalla facilità di riproduzione.

Esiste anche una dipendenza tecnologica su componenti importati che può essere tradotto come: i chip sono disponibili? Questo è un modello di esclusione imposto e non tutti possono realizzare l'hardware a causa delle implicazioni della creazione di tutte le infrastrutture necessarie. La persona che vuole utilizzare

l'hardware che un altro ha progettato, si deve fare, acquistare i componenti necessari e ricostruire lo schema. Tutto questo ha un costo. Di conseguenza poche aziende sono in possesso di queste conoscenze e le conservano gelosamente in modo che le persone rimangano meri consumatori del prodotto.

Modelli di produzione differenziati

Abbiamo osservato due modelli convenzionali di produzione / distribuzione. Da un lato, il modello di produzione centralizzato con lo stesso prodotto disponibile in molti luoghi, con prezzo maggiorato per il consumatore. Dall'altra parte, un sistema di produzione distribuito basato su un numero di piccoli gruppi indipendenti che producono lo stesso design distribuito localmente. Per diventare sostenibile in entrambi i modelli, le iniziative di hardware libero hanno bisogno di piattaforme che mettano insieme e facilitino il contatto tra i mezzi di produzione e coloro che vogliono creare. Per quanto riguarda il modello di produzione distribuita, vediamo che al momento non ci sono molte comunità che cercano di sviluppare hardware libero alternativo senza obiettivi capitalistici. Questi gruppi di solito dovrebbero cercare di creare autonomia, facilitando l'accesso a tutti e invertire gli effetti sociali, ambientali e politici avversi legati alla produzione di hardware proprietario.

Per esempio, ci sono vari incontri promossi dai movimenti sociali, come Hackmeeting [41], Hardmeeting [42], HacktheEarth [43], Extrud_me [44], o anche come la Conferenza OSHW [45], la Chaos Computer Conference [46] o incontri Dorkbot dove si possono trovare le persone che sviluppano progetti di hardware libero. Il progetto OSWASH [47] (Lavatrici Open Source) rappresenta perfettamente quello che noi definiamo come ricerca e sviluppo di tecnologie appropriate per i quali l'unico hardware che abbia un senso è libero, che è stato ri-appropriato ovvero ripreso da licenze proprietario ed è tornato ad essere aperto. In Spagna esistono posti a livello statale come Medialab Prado [48], La Laboral [49] o Hangar [50], spesso concentrati sullo sviluppo di hardware libero. Così a Hangar (Barcellona), troviamo BeFaco [51], che sviluppa strumenti per suonare con hardware libero e FABoratory [52], specializzato nella produzione di sampanti 3d. In Calafou, possiamo di trovare la HardLab Petchblenda [53] un laboratorio di suoni, elettronica e biohacking dal punto di vista transfeminista. Infine, dal XarxaCTiT [54] (Network of Science, Engineering and Technology) della Cooperativa Integral Catalana [55] stiamo sviluppando una piattaforma per lo scambio di conoscenze ed esigenze a livello locale, promuovendo una rete di partner, produttori, prosumer e di consumatori di hardware libero e tecnologie riappropriate.

In una visione diametralmente opposta e concentrandosi su una strategia globale, mentre non esiste un completo ecosistema di produzione distribuita, Chris Anderson [56] suggerisce la produzione di progetti open hardware in Cina utilizzando Alibaba.com [57]. Questa società creata nel 1999, è diventata una società da 12 miliardi di dollari con 45 milioni di utenti registrati e 1,1 milioni di dipendenti. La produzione in Cina è un fenomeno noto come Shanzai. In origine questo termine, definiva "banditi che si sono ribellati all'autorità e impegnati in atti che per loro sono visti come giustificati." Il movimento Shanzai nel 2009 ha rappresentato il 20% dei telefoni cellulari venduti in Cina, e il 10% dei telefoni venduti nel mondo. Alcuni produttori hanno tanto successo che preferiscono promuovere i propri marchi, piuttosto che produrre prodotti di "pirateria". La cosa interessante di queste aziende è che "piratare" prodotti di marca ha creato una cultura di condivisione delle informazioni su questi prodotti e ha generato materiale di design aperto, dando credito reciprocamente in quanto ne hanno apportato miglioramenti. E' la comunità che ha auto-formulato questa politica ed esclude quelli che non la seguono. Lo Shanzai capisce e risponde alle esigenze e ai gusti locali, stabilendo e mantenenendo basi di produzione locale e della distribuzione, chiamate fabbriche locali. Tuttavia le condizioni di lavoro, in particolare nella creazione di componenti elettrici, sono deplorevoli e rappresentano un rischio per il fisico e la salute [58] e non possono essere votati a cercare la giustizia sociale per i propri lavoratori. La Open Source Hardware Work Licence (ancora da scrivere) dovrebbe integrare come un requisito fondamentale le condizioni rispettose del lavoro delle persone, la loro libertà e il loro ambiente.

Conclusioni

Utilizzare e creare hardware libero protegge e difende la sovranità tecnologica perché permette l'indipendenza tecnologica per le persone evitando ogni dipenza da un altro fornitore di risorse per il proprio sviluppo. Il riutilizzo e l'adattamento del design può innovare e migliorare, ridurre i costi e tempi di

progettazione, facilitare il trasferimento di conoscenze e prevenire l'analfabetismo digitale per motivi economici. Le persone possono smettere di essere semplici consumatori tecnologici, consentendo loro di sapere come funziona, come mantenere e riparare la tecnologia di cui hanno bisogno. Utilizzare e creare hardware libero coinvolge, e genera più ricchezza rispetto all'utilizzo di altro hardware, anche se spesso si deve prima passare attraverso un paio di delusioni durante l'apprendimento. Al di là della propria convinzione politica, la libertà rappresenta la possibilità, la capacità di imparare a costruire il proprio mondo, che non ci aliena da noi stessi e ci allontana invece dal partecipare alla struttura capitalistica. Ció che è appropriato o inappropriato non è un attributo della tecnologia stessa. Il tuo giudizio è il risultato della valutazione delle sue caratteristiche in relazione alla: (1) organizzazione dello Stato della produzione e del sistema economico; (2) i livelli e la distribuzione del reddito, e (3) lo stato di sviluppo del sistema della tecnologia in uso. Analizziamo cosa può significare in una società la desertificazione attraverso la tecnologia: l'obsolescenza programmata, la dipendenza tecnologica e l'introduzione di tecnologie inappropriate. La sua devastazione e recupero sono quasi impossibili se rimangono all'interno delle catene pesanti del sistema capitalista.

Poichè il mondo dell'hardware libero è molto complesso, e gli obblighi e gli abusi che ci sono attraverso lo sviluppo tecnologico non sembrano rispettare le libertà, sono attratta dalla riappropriazione delle tecnologie. Queste sono quelle che meglio rispondono alle situazioni ambientali, culturali ed economiche. Esse richiedono poche risorse, significano costi minori e basso impatto ambientale. Abbiamo bisogno di una vera e propria reindustrializzazione, che includa le nostre tecnologie, le tecniche e la tecnologia di tutti i giorni così come le nostre tradizioni ancestrali, che di per sé già hanno una base ambientale, sostenibile e olistica. Tecnologia riappropriata dal cieco progresso, dall'analfabetismo e dall'alienazione, dalla scienza inamovibile, dagli interessi del potere; ri-appropriata perché decentrata, organica, trasmutabile.

Opinione di Richard Stallman sull'hardware libero. Free Hardware Design - Past, Present, Future; di Graham Seaman The economics of Free Core development; di David Kessner Open-source IP could ignite system-on-chip era; di David Kessner Business Models for Open Source Hardware Design; di Gregory Pomerantz Free chips for all - The status of open hardware designs; di Jamil Khatib Open Hardware and Free Software Extending the Freedoms of Free and Open Information; di Carl Vilbrandt, progettista di GnuBook. Challenge to Silicon Valley; di Kofi Annan Liberalidad del conocimiento desde la cesión de derechos de propiedad intelectual León Rojas, J. M. Inteligencia Colectiva, la revolución invisible; di Jean-François Noubel Wikipedias versus blogs. La creación colectiva y el acceso universal al conocimiento. Casassas Canals, Xavier. Cultura libre; di Lawrence Lessig, “La industria de la música en la era digital: Participación de los consumidores en la creación de valor.”; di Chaney, D

Elleflane

Ingegnera Industriale per la UNED Universidad Nacional a Distancia; Ingegnera Tecnica in Design Industriale dell'Università Elisava Pompeu Fabra; realizza cortometraggi, poesie, quadri, fumetti, novelle fantastiche, invenzioni, +, ++, +++. Sta studiando alla ESA European Space Agency.

NOTE

1. https://es.wikipedia.org/wiki/Homebrew_Computer_Club

2. http://www.webopedia.com/TERM/F/FPGA.html

3. http://www.nationmaster.com/encyclopedia/Challenge-to-Silicon-Valley

4. http://www.opencollector.org/history/OpenDesignCircuits/index.html

5. http://www.oepm.es/es/propiedad_industrial/propiedad_industrial/

6. http://stallman.org/

7

7. http://www.fsf.org/

8. https://www.gnu.org/licenses/licenses.es.html

9. http://www.linuxtoday.com/infrastructure/1999062200505NWLF

10. http://www.opencollector.org/Whyfree/freedesign.html

11. http://www.oshwa.org/

12. http://www.openhardware.net/

13. https://www.gnu.org/copyleft/gpl.html

14. http://www.freemodelfoundry.com/

15. http://www.uv.es/leo/sparc/

16. http://opencores.org/

17. http://opensource.org/licenses/MIT

18. http://web.media.mit.edu/~rehmi/freeip.html

19. http://www.debian.org/News/2000/20001123.en.html

20. http://blog.openlibrary.org/tag/gnubook/

21. http://www.simputer.org/simputer/license/

22. http://f-cpu.seul.org/

23. http://opencores.org/

24. http://www.opencollector.org/hardlicense/msg00007.html

25. https://joinup.ec.europa.eu/software/page/ open_source_licences_and_complementary_agreements

26. http://www.opencollector.org/hardlicense/hdpl.html

27. http://www.opencollector.org/hardlicense/licenses.html

28. http://www.opencollector.org/hardlicense/hdpl.html

29. http://www.ohwr.org/projects/cernohl/wiki

30. http://www.marketwired.com/press-release/adafruits-limor-fried-phillip- torrone-featured-keynotes-for-make-conference-1649479.htm

31. https://www.adafruit.com/

32. http://www.arduino.cc/

33. http://www.chumby.com/

34. http://www.liquidware.com

35. https://www.makerbot.com/

36. http://en.wikipedia.org/wiki/Crowdfunding

37. http://p2pfoundation.net/Open_Source_Hardware_Reserve_Bank

38. http://www.openmoney.org/

39. http://metacurrency.org/

40. sociali come Hackmeeting

41. http://sindominio.net/hackmeeting/wiki/2014

42

42. http://giss.tv/dmmdb/index.php?channel=hardmeeting

43. https://calafou.org/es/contenthackthearth-2013-jornadas-autosuficiencia

44. http://xctit.cooperativa.cat/encuentros/extrud_me-2014/

45. http://2013.oshwa.org/

46. http://www.ccc.de/en/

47. http://www.oswash.org/

48. http://medialab-prado.es/

49. http://www.laboralcentrodearte.org

50. http://hangar.org

51. http://www.befaco.org

52. http://faboratory.org/

53. http://pechblenda.hotglue.me/

54. http://xctit.cooperativa.cat/

55. http://cooperativa.cat/

56. “In the Next Industrial Revolution, Atoms Are the New Bits”,

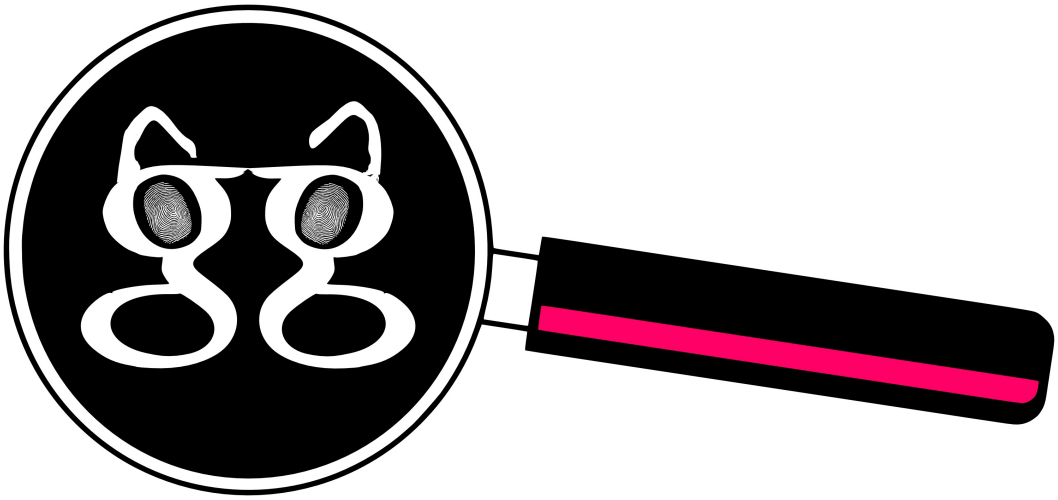
57. http://www.openhardware.net/

58. http://www.publico.es/418911/la-gente-se-sentiria-molesta-si-viera-de-donde- viene-su-iphone

Motori di ricerca

Open non significa libero, pubblicato non significa pubblico. La gratuità online è una truffa!

Ippolita



Sono passati alcuni anni da quando Ippolita ha cominciato a fare la distinzione tra l'apertura al «libero mercato», propugnata dai guru del movimento open source, e la libertà che il movimento del software libero persegue ponendola come base della propria visione dei mondi digitali. Il software libero è una questione di libertà, non di prezzo. Per un decennio si è potuto pensare che il problema riguardasse solo i geek del computer e altri smanettoni. Oggi è evidente che ci tocca tutti. I grandi intermediari digitali si sono trasformati negli occhi, nelle orecchie o, per lo meno, negli occhiali di tutti gli utenti di Internet, inclusi quelli che si connettono solo con uno smartphone.
Anche a rischio di apparire noiosi, desideriamo insistere su questo punto: l'unica vocazione dell'Open Source è quella di definire i mezzi migliori per diffondere un prodotto in una forma *open*, cioè aperta, in una prospettiva del tutto interna alla logica del mercato. L'aspetto dell'attitudine hacker che ci piace, cioè l'approccio curioso e lo scambio tra pari, è stato contaminato da una logica di lavoro e di sfruttamento del tempo finalizzata al profitto, e non al benessere personale e collettivo.
Il baccano creato dalle monete elettroniche distribuite (o cripto-monete), come Bitcoin, non fa altro che rafforzare questa affermazione. Invece di agire negli interstizi per ampliare gli spazi e i gradi di libertà e di autonomia, invece di costruire le nostre reti autogestite per soddisfare le nostre esigenze e i nostri desideri, ci adagiamo su una presunta moneta, sprechiamo energie e intelligenza in alcune molto classiche «piramidi di Ponzi», in cui i primi arrivati si arricchiscono a scapito di chi li segue.
Dal punto di vista della sovranità, siamo ancora nel quadro tracciato appositamente per la delega tecnologica della fiducia, un processo iniziato secoli fa (quanto meno con la modernità): non abbiamo alcuna fiducia negli Stati, nelle istituzioni stabilite, nelle grandi imprese e così via. Tanto meglio: *Ars longa, vita brevis*, è molto tardi e ci sono molte cose più interessanti da fare che perder tempo a riformare l'irriformabile. Sfortunatamente, invece di tessere con pazienza reti di fiducia per affinità, tendiamo a riporre

fiducia nelle Macchine[1], e sempre di più nelle Mega-macchine che si incaricano di gestire questa mancanza di fiducia con i loro algoritmi *open*: basta credere in loro. Serve solo di aver fede nei Dati, e rivelare tutto alle piattaforme sociali, confessare i nostri desideri più intimi e quelli dei nostri cari, per contribuire così alla costruzione di una rete unica (proprietà privata di alcune grandi imprese).
I Guru del Nuovo Mondo 2.0 ci hanno addestrato bene ai rituali di fiducia. Un Jobs[2], vestito tutto di nero, brandendo un oggetto del desiderio bianco e puro (per esempio un Ipod), avrebbe potuto dire una volta, sull'altare-scena degli «Apple Keynotes»: «Prendete [tecnología proprietaria], e mangiate: questo è il mio corpo offerto a tutti voi». Però se proviamo a stare attenti alla qualità e alla provenienza di quello che mangiamo, perchè non stare attenti anche agli strumenti e alle pratiche di comunicazione?

L'analisi di Google come paladino dei nuovi intermediari digitali che Ippolita ha fatto nel saggio «Il lato oscuro di Google»[3], si sviluppava nella stessa ottica. Lungi dall'essere soltanto un motore di ricerca, il gigante di Mountain View ha manifestato sin dalla sua nascita una chiara attitudine egemonica nel suo intento sempre più prossimo a realizzarsi di «organizzare tutto il sapere del mondo».
Vorremmo evidenziare come la logica *open*, aperta, combinata alla concezione di eccellenza universitaria californiana (di Stanford in particolare, culla dell'anarco-capitalismo), vedeva nel motto "Don’t be evil" [4], la scusa per lasciarsi corrompere al servizio del capitalismo dell'abbondanza, del turbo-capitalismo illusorio, della crescita illimitata (sesto punto della filosofia di Google: "è possibile guadagnar denaro senza vendere l'anima al diavolo"[5]). A loro piacerebbe farci credere che di più, più grande, più veloce (*more, bigger, faster*) sia sempre sinonimo di migliore; che essere sempre più connessi ci renda sempre più liberi; che dare a Google le nostre "intenzioni di ricerca" ci permetterà di non sentire più il peso della scelta, perché il pulsante "Mi sento fortunato" ci condurrà direttamente a una fonte alla quale saziare la nostra sete di conoscenza... Però queste promesse vengono sempre più disattese.

Abbiamo sempre più fame di informazione. La sete di novità è diventata inesauribile. La soddisfazione è tanto fugace che non riusciamo a smettere di cercare, ancora e ancora. A causa delle sue dimensioni, il re dei motori di ricerca è caduto nell'inutilità disfunzionale ed è diventato nocivo, oltre che una fonte di dipendenza. La terminologia di Ivan Illich qui risulta appropriata: a partire dal momento in cui la società industriale, perseguendo l'efficienza, istituisce un mezzo (strumento, meccanismo, organismo) per raggiungere un obiettivo, questo mezzo tende a crescere fino a oltrepassare un limite che lo rende disfunzionale e compromette l'obiettivo che originariamente perseguiva. Così come l'automobile arreca danno ai trasporti, l'istituzione scolastica all'educazione e la medicina (intesa come espressione della casta medica) alla salute, lo strumento industriale Google diventa controproducente ed nocivo per il benessere umano e sociale nel suo insieme.
È chiaro che quello che vale per Google vale anche per gli altri monopoli attualmente in attività: Amazon nella distribuzione, Facebook nella gestione delle relazioni interpersonali e così via. Inoltre ogni servizio 2.0 tende a sviluppare i propri motori e strumenti di ricerca interni dando l'impressione che il mondo, in tutta la sua complessità, sia a portata di click.
Con gli smartphone questa sovrapposizione si fa ancora più evidente: se usiamo Android, il sistema operativo made in Google, ci troviamo completamente immersi nella visione del mondo di Google. Tutto ciò che possiamo cercare e trovare viene assorbito da loro, di *default*, in maniera automatica.
In tutti i casi abbiamo a che fare con la stessa dinamica di *trasparenza radicale*. Il migliore apostolo di questa vera e propria ideologia è Facebook, con il suo mondo in cui tutto si pubblica, si condivide, si espone, ecc. Eppure niente è pubblico, è tutto privato. Abbiamo sempre meno controllo sui dati che produciamo con le nostre ricerche, tutti i «mi piace», i post, i tag, i tweet. Lungi dall'essere i padroni, né tanto meno i responsabili e gestori, siamo solo soggetti ai princìpi espressi dalla piattaforma alla quale affidiamo (letteralmente: ci affidiamo a lei, con fede) i nostri dati. Senza voler entrare in un dibattito giuridico, nel quale non ci troveremmo affatto a nostro agio [6], basterebbe ricordare che nessuno legge davvero le Condizioni Generali di Utilizzo (TOS, *Terms Of Service*) che accettiamo quando usiamo questi servizi. Come ci hanno spiegato amici giuristi, sono di fatto clausole vessatorie, che determinano asimmetrie strutturali. In questi mondi compartimentati proliferano i regolamenti sempre più prescrittivi i cui princìpi portano il politicamente corretto fino all'eccesso[7].
La moltiplicazione delle regole che nessuno conosce viene accompagnata dalla moltiplicazione delle funzionalità (*features*) che pochi usano. Ad ogni modo, nessuno è davvero in grado di spiegare come queste

funzionalità vengano adottate «in esclusiva, per tutto il mondo», o per ignoranza o pigrizia, o anche a causa di divieti derivati dalla sinergia perversa fra NDA (*Non-Disclosures Agreement*, clausole di non divulgazione dei segreti industriali, firmate normalmente dai lavoratori dell'IT), Brevetti, Trademarks, Copyrights.

Il tipo di sovranità che piace a Ippolita è l'autonomia, il fatto di «decidere le proprie regole», e in maniera condivisa. Se non si conoscono le regole, non è possibile alcuna autonomia. Abbiamo appena iniziato a comprendere come funzionano quelle che abbiamo descritto come "maliziose funzionalità" degli algoritmi, diventate note come *Filter Bubble*: la pratica della profilazione online. La bolla dei risultati personalizzati ci porta in una zona di eteronomia permanente che si espande costantemente, nella quale le scelte sono delegate agli Algoritmi Sovrani. Ovviamente non si tratta di una costrizione, siamo totalmente liberi nel nutrire la sovranità algoritmica con tutti i nostri movimenti online, e molte volte lo facciamo con entusiasmo. Sovrano è colui che decide dello stato di eccezione: per questo abbiamo sostenuto che ci troviamo immersi in uno stato di *eccezione di massa*, di matrice algoritmica privata. Questa pratica rappresenta la promessa di libertà automatizzata: pubblicità contestuale e studio dei sentimenti degli utenti, affinchè ognuno riceva un annuncio personalizzato, di prodotti su misura, per acquistarli con un clic e disfarsene, il più rapidamente possibile, per poter comprare un'altra cosa. Allora noi, gli utenti, siamo consumatori per coloro che devono conoscerci perfettamente per poter prevedere e soddisfare i nostri «vizi» con oggetti subito obsoleti. Ricordiamo che la profilazione è un prodotto della criminologia. Seguire la sua logica, anche se per scopi commerciali, è relazionarsi con l'altro come con un criminale.

In questo ambito Google è sempre stato pioniere e campione indiscusso. Il suo motore di ricerca si basa sul Page Ranking e poi anche Google Panda. All'inizio, ogni link entrante in un sito veniva considerato come l'espressione di un voto di preferenza; i risultati si basavano su quello che aveva «votato» la «maggioranza». Molto rapidamente, gli algoritmi si sono dotati di filtri contestuali [8]. Attraverso i risultati dell'algoritmo globale di top rank e a partire dai dati che provengono dalla profilazione dell'utente (ricerche precedenti, cronologia di navigazione, ecc.), è emersa un'autentica ideologia della trasparenza[9]. E questa può materializzarsi solo spogliando letteralmente gli individui e consegnando la loro interiorità (o per lo meno, quello che essi esprimono attraverso la macchina) a un sistema digitale interconnesso. Questi contenuti si accumulano con processi di *tracking*[10], vengono suddivisi in porzioni sempre più dettagliate per consegnare a ogni internauta un servizio-prodotto a misura, che risponde in tempo reale alle preferenze che ha espresso.

La questione della profilazione è diventata notizia dibattuta a livello mondiale a partire dagli «scandali» di PRISM e simili (ma qualcuno ricorda Echelon[11], tuttora in attività?). La stragrande maggioranza degli utenti dei servizi 2.0, dei quali i motori di ricerca fanno parte, accettano i loro parametri di *default*. Quando ci sono delle modifiche[12], quasi tutti gli utenti adottano la nuova configurazione. Lo chiamiamo il potere «di default»: la vita online di milioni di utenti può essere trasformata totalmente, semplicemente facendo alcune modifiche. Si possono modificare le loro abitudini, i loro comportamenti più minuti, perfezionare un addestramento che scegliamo un click dopo l'altro.

Questo è il lato oscuro dei sistemi di profilazione! È possibile che un giorno, nell'inserire il tuo nome e la tua password, trovi cambiata l'organizzazione dello spazio del tuo conto personale, un poco come se entrando a casa fosse cambiato l'arredamento e i mobili non fossero più al loro posto. Dobbiamo sempre tenere a mente questo quando parliamo di tecnologia per tutti, vale a dire per la massa: anche se nessuno vuole far parte di essa, quando usiamo questi strumenti commerciali e gratuiti siamo la massa. E ci sottomettiamo al potere "di default": questo implica che quando cambiamo il default, viene stabilita la nostra "diversità", perché la modifica che abbiamo scelto è registrata nel nostro profilo[13].
La *Pars Destruens* è ovviamente la più facile da esporre. Non è troppo difficile articolare critiche radicali. D'altro canto, il mero fatto di sentire la necessità di trovare alternative ai motori di ricerca ora disponibili non garantisce affatto un risultato soddisfacente. La navigazione il più possibile anonimizzata, che insegniamo nei nostri seminari per l'autodifesa digitale, è un buon indizio per poter giudicare la qualità delle nostre ricerche e la nostra rapporto con la rete in generale.
Potremmo riempire pagine e pagine spiegando come usare questa o quella estensione di Firefox[14] che aiuti a evitare il tracciamento, blocchi le pubblicità, o impedisca ai minori di entrare in siti «pericolosi» (così ci viene chiesto spesso da adulti-padri-educatori spesso ingannati dalla retorica reazionaria della «rete

pericolosa»). Si possono rimuovere tutti i cookies e gli LSO (Localised Shared Object), ci si può connettere in modo anonimo tramite VPN (Virtual Private Networks), criptare ogni comunicazione, usare TOR e altri strumenti anche più potenti, in modo che Google & Co non sappiano niente di noi. Sì, però... se provo a proteggermi di più, allora mi differenzio di più dalla massa ed è più facile riconoscermi. Se il mio browser è pieno di estensioni per eludere la profilazione, rendermi anonimo e criptare, e se uso soltanto un sistema operativo strettamente GNU/Linux per connettermi alla rete (Che gusto? Ubuntu, Debian, Arch, Gentoo, from scratch, ecc. Ce ne sarà sempre uno più « puro »!), paradossalmente mi riconoscono più facilmente di un qualunque internauta che usa sistemi meno complessi e più diffusi[15].
La crittografia, ottimo strumento per esercitare l'autonomia tecnologica, solleva anche tante critiche, soprattutto perché si basa sullo stesso principio di crescita illimitata (sempre più potente, sempre più veloce) del turbo-capitalismo liberista, e dell'attuale variante libertariana della Silicon Valley. Con l'aumentare della potenza di calcolo e della velocità delle reti, aumenta l'efficienza dei sistemi di crittazione più recenti; allo stesso tempo i vecchi catenacci diventano obsoleti con rapidità.
Questo meccanismo di crescita-obsolescenza fa parte di una logica militare di attacco e difesa, di spionaggio e controspionaggio. Non dimentichiamo che si tratta in generale di sistemi pensati per scopi militari, nati con lo scopo di rendere inoffensiva l'intercettazione delle comunicazioni da parte del nemico, incapace di decifrare i messaggi. La crittografia è una buona pratica, sopratutto per gli appassionati di informatica a cui piacciono i rompicapo logici, però l'approccio non è soddisfacente.
La *Pars Construens* dovrebbe iniziare dall'umile accettazione che la tecnologia non è né buona, né cattiva, né neutra, in alcun modo. L'uso delle tecnologie dipende dalle persone, ma anche da come quella tecnologia è stata architettata. Per cui una particolare tecnologia, anche la migliore del mondo (però secondo quale criterio?) non garantisce nulla di per sé. L'approccio metodologico che ci piace proporre è di valutare non il «cosa?» (che alternativa ai motori di ricerca?) bensì il «come?»: la maniera con la quale gli strumenti tecnologici si creano e si modificano attraverso il loro uso, i metodi con i quali gli individui e i gruppi si adattano e cambiano i loro modi particolari di agire.

Seconda umile accettazione: le questioni sociali sono prima di tutto questioni umane, di relazioni tra gli esseri umani, ognuno nel suo ambito. Malgrado l'alta risoluzione degli schermi touch, malgrado la velocità quasi istantanea di migliaia di milioni di risultati dei motori di ricerca quasi onnipotenti, la civiltà 2.0 è molto simile a quelle che la hanno preceduta, perchè gli esseri umani continuano a cercare l'attenzione dei loro simili. Hanno ancora bisogno di mangiare, dormire, mantenere relazioni di amicizia, dare un senso al mondo a cui appartengono. Continuano a innamorarsi e ad avere delusioni, sognano e nutrono speranze, si sbagliano, si derubano, si fanno del male, si uccidono.
In parole povere gli esseri umani devono avere coscienza della finitezza della loro esistenza, nel tempo (l'impossibilità di comprendere la morte) e nello spazio (lo scandalo dall'esistenza degli altri, e di un mondo esteriore), anche nell'era dei motori di ricerca e delle reti sociali digitali.

Come queste considerazioni possono aiutarci a cercare meglio, vale a dire, cercare in modo «diverso»?
L'egemonia dei motori di ricerca giganti si basa su una accumulazione senza limite di dati: è evidente che è una questione di dimensioni. *Size matters!* Le dimensioni contano, e parecchio! Un'informazione e tecnologia di ricerca semplice da usare che promuovano la realizzazione della libertà individuale in una società dotata di strumenti efficienti sono ancora possibili. Di fatto, la conclusione logica di una critica dell'informatica del dominio consiste nel sostenere all'opposto che *small is beautiful*, "piccolo è bello".
Le dimensioni hanno un'importanza considerevole. Superata una certa scala, è necessaria una gerarchia per gestire le relazioni tra gli esseri umani e tra gli esseri in generale, viventi e non. Fra macchine e protocolli, cavi, membrane, processi di accumulazione e ricerca. Ma chi controllerà gli intermediari? Chi controllerà i controllori? Se ci affidiamo a strumenti di intermediazione troppo grandi per le nostre ricerche, dobbiamo accettare che si instauri una gerarchia di dominio. Tutto è relativo, non nel senso che vale tutto, che ogni cosa è equipollente, ma nel senso che tutto è «in relazione con».

I saperi ammassati in quelli che chiamiamo «Big data»[16] sono una chimera perché i saperi utili per gli esseri umani non sono all'esterno dei loro corpi, individuali e collettivi, e non sono intercambiabili fra loro; se è vero che possono essere oggettivati, trasmessi, appresi, tradotti e condivisi, i saperi sono innanzi tutto un processo di immaginazione individuale, suscettibile di socializzarsi in immaginari collettivi. Al contrario della

memoria totalmente inerte degli strumenti digitali, l'identificazione è un processo nel quale perdiamo e riacquistiamo continuamente consapevolezza, nel quale perdiamo memoria per poi ricostruirla, come ci ricostruiamo nei nostri processi vitali. Se invece di avere un numero limitato di fonti tra le quali selezionare i nostri percorsi, creiamo la nostra storia che ricontrolliamo e condividiamo, avendo attinto da una fonte illimitata di dati automaticamente organizzati dai sistemi di profilazione, la relatività cede il passo all'omologazione. Così si nutrono le Megamacchine.
Queste ultime creano relazioni di causa-effetto di tipo capitalista o dispotico. Generano dipendenza, sfuttamento, impotenza degli esseri umani ridotti a essere solo consumatori sottomessi. Peggio: consumatori-produttori che desiderano asservirsi ai loro stessi desideri illimitati.

Sia detto ancora una volta per gli entusiasti sostenitori dei *commons*: è una questione di scala, non di proprietà, perché

la proprietà collettiva dei mezzi di produzione a questo livello non muta nulla, e si limita ad alimentare un'organizzazione dispotica stalinista. Perciò Illich vi oppone il diritto di ciascuno a utilizzare i mezzi di produzione in una «società conviviale», ossia desiderante e non-edipica. Ciò significa: l'utilizzazione più estesa delle macchine da parte del maggior numero di persone, la moltiplicazione delle piccole macchine e l'adattamento delle grandi macchine alle piccole unità, la vendita esclusiva di elementi macchinici che devono essere assemblati dagli stessi utilizzatori-produttori, la distruzione della specializzazione del sapere e del monopolio professionale.[17].

La domanda di sempre è: Come fare? Che intenzioni abbiamo rispetto alle tecnologie di ricerca? Vogliamo trovare ciò che cerchiamo subito, o invece ci piacerebbe percorrere un cammino? Magari desideriamo vagare con gli amici, o da soli; è possibile che abbiamo voglia di avventurarci nelle profondità sconosciute e non facilmente condivisibili con un click, un tag, un post.

Potremmo desiderare motori di ricerca «situati» che assumono una prospettiva per nulla «oggettiva» e, al contrario, esplicitamente «soggettiva», spiegando il perché e il come. La moltiplicazione dei motori di ricerca di piccola taglia ed esplicitamente dedicati, ecco una possibilità che si approfondisce poco! Un possibile criterio di giudizio potrebbe essere la loro capacità di rivolgersi a un gruppo particolare con esigenze particolari. Questa aspirazione minoritaria non implicherebbe logicamente la volontà di rifiutare in modo quasi istantaneo le ricerche di tutto il mondo, e cioè di una massa soggetta alla profilazione, ma di approfondire gli aspetti negativi di una conoscenza sempre illimitata. Questo segnerebbe la fine delle aspirazioni totalitarie, questo famoso lato oscuro dell'Illuminismo e di tutti i progetti di conoscenza globale. Ricorrere alla valutazione dei componenti della nostra «rete sociale», e non solo online, rappresenta un'altra possibilità incredibilmente efficace, se l'obbiettivo è quello di creare un riferimento affidabile su un tema particolare. Si tratterebbe allora di scegliere con attenzione a chi «dare fiducia».
L'adozione di uno stile sobrio può essere l'alternativa più potente per contrastare la proliferazione di espedienti tecnologici che non abbiamo mai chiesto, e ai quali, però, abbiamo difficoltà a sottrarci. Di fatto anche l'imposizione dell'obsolescenza programmata rientra nel campo di ricerca, iniziando dall'equivalenza «di più è meglio», frutto di un'applicazione cieca dell'ideologia del progresso a tutti i costi. Possedere una gran quantità di oggetti, nel mondo 2.0, significa anche avere accesso a un numero di risultati in crescita continua ed esponenziale, sempre più ritagliati in funzione delle nostre preferenze, ostentate più o meno esplicitamente. Seguendo la stessa logica, si dovrebbe tener in conto la durata di un risultato: una montagna di risultati validi per pochi giorni, ore, o magari minuti, dovrebbero avere meno interesse di risultati più resistenti al passare del tempo.

Sfuggire all'economismo religioso del consumo obbligatorio significherebbe, allora, avviare un percorso di decrescita, nella ricerca online, come in ogni altro ambito tecnologico. Questi processi di auto-limitazione e di scelta attenta non potranno essere in nessun caso «fortuiti», come esplicita il bottone "mi sento fortunato" della filosofia oracolare di Google, nel senso di senza sforzi o quasi automatici. Nessuna dipendenza, e ancor meno la dipendenza da una tecnologia «gratuita» dalla risposta immediata, può essere spezzata senza conseguenze. In altre parole, se desideriamo un motore «libero» che sia al 99,99% altrettanto veloce, potente e disponibile di Google, allora l'unica cosa che potrà accadere sarà di creare un altro Moloch come quello di Mountain View.

A coloro che forse potrebbero percepire come un sacrificio questa tensione che potremmo definire ecologista, risponderemo con il tono dell'allegoria tornando al cibo: perché mangiare robaccia industriale al posto di scegliere bene gli ingredienti dei tuoi pasti? Perché abbuffarsi di risultati quando potremmo sviluppare i nostri gusti personali? La vita è troppo corta per bere tutto quel vino cattivo!

Ci sono molti esperimenti autogestiti già attivi, basta aprire bene gli occhi, annusare l'aria attorno, tendere le orecchie, toccare, sporcarsi le mani e provare ad affinare il proprio gusto per le cose buone: alla fine basta mettersi alla ricerca. Aspettarsi che gli altri lo facciano al posto nostro è un'idea bislacca, come credere che i grandi motori di ricerca ci forniscano la risposta esatta immediatamente, gratuitamente e senza sforzo. Ma non esiste nessun oracolo onnisciente, solo persone nelle quali decidiamo di riporre la nostra fiducia.

Ippolita

Gruppo di ricerca indisciplinare attivo dal 2004. Conduce una riflessione ad ampio raggio sulle 'tecnologie del dominio' e i loro effetti sociali. Pratica scritture conviviali in testi a circolazione trasversale, dal sottobosco delle comunità hacker alle aule universitarie. Tra i saggi pubblicati: *Anime Elettriche*; *La Rete è libera e democratica. FALSO!*, *Nell'acquario di Facebook*, *Luci e ombre di Google*. *Open non è free. Comunità digitali tra etica hacker e mercato globale*.

Ippolita tiene formazioni teorico-pratiche di autodifesa digitale, pedagogia hacker e validazione delle fonti per accademici, giornalisti, gruppi di affinità, persone curiose.

info [at] ippolita [dot] net
http://ippolita.net

NOTE

1. Si veda Giles Slade, The Big Disconnect: The Story of Technology and Loneliness, Prometheus Books, NY, 2012, in particolare il terzo capitolo, «Trusting Machines». ↩

2. Per esempio, https://upload.wikimedia.org/wikipedia/commons/b/b9/Steve_Jobs_Headshot_2010-CROP.jpg ↩

3. Ippolita, El lado oscuro de Google: Historia y futuro de la industria de los metadatos, virus editorial ed. or. it. Luci e Ombre di Google, Feltrinelli, Milano, 2007. Free copyleft download http://ippolita.net ↩

4. Non essere malvagio ↩

5. Le dieci cose che sappiamo essere certe, http://www.google.com/intl/es/about/company/philosophy/ ↩

6. Sopratutto perché il diritto tramite leggi e giudizi sanziona chi lo infrange anche di più se non è in grado di pagare buoni avvocati. Si veda Carlo Milani,« Topologies du devenir libertaire. II – Droits ? », dans Philosophie de l'anarchie. Théories libertaires, pratiques quotidiennes et ontologie, ACL, Lyon, 2012, pp. 381-384. ↩

7. Se Google fa filosofia, Facebook annuncia princìpi: https://www.facebook.com/principles.php ↩

8. Si veda Ippolita, El lado oscuro de Google, cit., « V. Además, otras funcionalidades maliciosas » ↩

9. I lavori di danah boyd forniscono un punto di vista molto chiaro in merito, il suo sito http://www.zephoria.org/ merita una visita. Per una prospettiva più filosofica si veda Byung-Chul Han, Transparenzgesellschaft, Matthes & Seitz, Berlin, 2012. ↩

[10]. Il sito http://donttrack.us/ ci mostra molto chiaramente, con una breve presentazione, il sistema di tracciamento delle ricerche. Ci da anche l'opportunità di fare una prima allusione alle “alternative”, por esempio DuckDuckGo. Un motore di ricerca che dice di non tracciare (non fare tracking). Lo scetticismo metodologico al quale aspiriamo ci permette di osservare che è possibile: serve solo aver fiducia in DuckDuckGo... ↩

[11]. E comunque, sappiamo sin dalla publicazione del 1999 del rapporto europeo di Duncan Campbell 'Interception Capabilities' http://www.cyber-rights.org/interception/stoa/interception_capabilities_2000.htm che lo spionaggio digitale si fa su scala globale. ↩

[12]. Come successe varie volte nel 2012 e nel 2013, quando Google ridefinì i suoi parametri di confidenzialità e di scambio dei dati tra i suoi diversi servizi. ↩

[13]. Si può provarlo facilmente: chiedi ai tuoi amici e colleghi di lavoro se hanno cambiato i parametri di default di Google. Normalmente (a partire dal 2014) il filtro Safe Search che Google usa per scartare i risultati di ricerca «illeciti» è basato sulla «media», vale a dire che filtra i contenuti di carattere sessuale esplicito nei risultati di ricerca. E' sempre più difficile individuare questo tipo di parametri. La ragione è stata esposta da una fonte chiaramente corporate: la strategia di business ottimale per i giganti della profilazione online è offrire sistemi di controllo della confidenzialità difficili da usare. Si veda «Appendix: a game theoretic analysis of Facebook privacy settings», in Robert H. Sloan, Richard Warner, Unauthorized access. The Crisis in Online Privacy and Security, CRC Press, 2014, pp. 344-349. ↩

[14]. Si veda per esempio il manuale Security in a box: https://securityinabox.org/fr/firefox_principale ↩

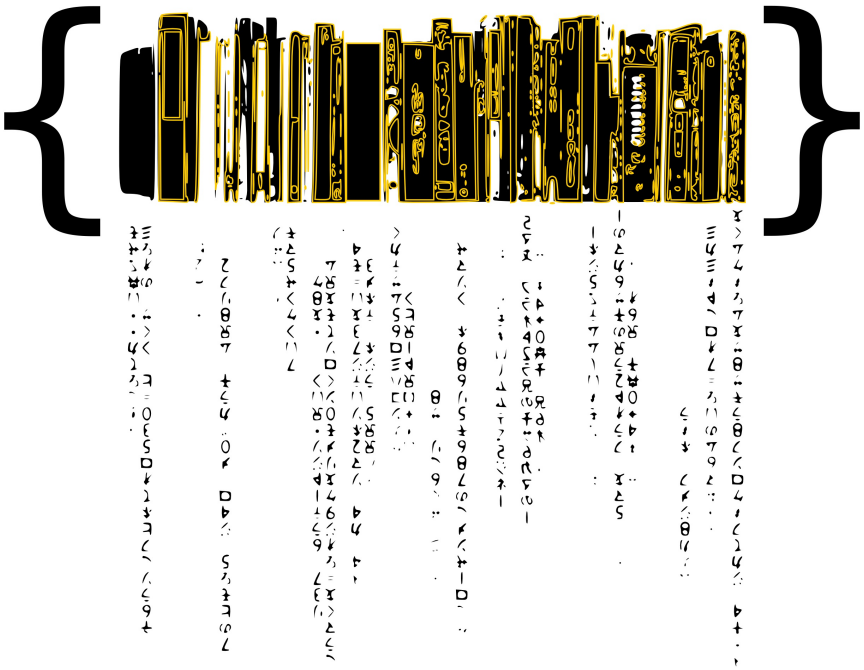
[15]. Un panorama abbozzato da Ippolita, Nell'acquario di Facebook, Ledizioni, 2012, Parte terza, le libertà della Rete, «Reazioni e antropotecniche di sopravvivenza», pp. 177-186 http://www.ippolita.net/it/libro/acquario/reazioni-e-antropotecniche-di-sopravvivenza. Si vedano anche il progetto Panopticlick della EFF: https://panopti-click.eff.org/ e Ixquick: https://www.ixquick.com/eng/ ↩

[16]. https://es.wikipedia.org/wiki/Big_data ↩

[17]. G. Deleuze, F. Guattari, Bilancio-programma per macchine desideranti, in Macchine desideranti, Ombre corte, Roma 2004, p. 114. Ed. or. Gilles Deleuze, Felix Guattari, «Appendice, Bilan-programme pour machines désirantes», L’Anti-Œdipe, Éditions de Minuit, Paris, 1975, p. 479. ↩

Biblioteca Pubblica Digitale

Marcell Mars



Nel catalogo delle grandi innovazioni storiche, la biblioteca pubblica forma parte di uno dei fenomeni per i quali ci sentiamo piu' orgogliose, sicuramente assieme all'educazione e alla salute pubblica, la dichiarazione universale dei diritti dell'uomo, il metodo scientifico, Wikipedia e il software libero.

Si tratta di una di quelle infrastrutture, quasi invisibile, che notiamo solo quando cominciano a scomparire. Per molto tempo le biblioteche pubbliche sono state considerate come il posto dove accedere alla conoscenza, anche se dipendenti dai budget sempre instabili dello "stato di benessere" o dalle risorse di alcuni ricchi proprietari.

Internet ha capovolto il senso di quello che davamo per certo e per possibile. Il sogno di poter accedere tutte a tutta la conoscenza finalmente alla nostra portata. Sembrava solo una questione di diffusione. Sapere intravedere quando le curve di distribuzione dei PC e l'accesso a Internet finivano per unirsi per fare sí che questo accesso universale alla conoscenze diventasse realtà. Senza dubbio, invece, lo sviluppo delle biblioteche pubbliche nell'era di Internet sembra andare direttamente nella direzione opposta, facendo sí che possano facilmente sparire.

Molte biblioteche pubbliche non possono ricevere, e nemmeno comprare, i libri modificati da grandi case editrici[1]. In alcuni casi, gli ebook che già fanno parte del loro catalogo devono essere distrutti dopo essere stati prestati un certo numero di volte[2]. Si sta perdendo la battaglia del mercato, dominato da nuovi attori come Amazon, Google e Apple.

Peró la rivoluzione emancipatrice forma anche parte dei fenomeni per i quali possiamo mostrarci piú orgogliose. Dare potere alle persone affinché possano contare sui mezzi necessari per raggiungere i loro sogni. Non possiamo rinunciare alle biblioteche pubbliche nell'era Internet, e tantomeno al sogno di un accesso universale a tutta la conoscenza umana. Per questo attivisti, documentaristi, cittadine, artiste, hackers e molte altre, stanno creando le circostanze necessarie per trasformare questo sogno in realtà. E, come dice Malvil Dewey: "scuole libere e biblioteche libere per ogni anima"[3].

La proposta è la seguente: facciamo un catalogo di tutti i libri che abbiamo scaricato e condividiamolo! Tanto alla fine una biblioteca pubblica consiste in:

- un accesso libero per ogni membro della società;
- alcuni cataloghi dei libri e documenti disponibili;
- una persona "bibliotecaria".

Con i libri preparati per essere condivisi e meticolosamente categorizzati, chiunque puó diventare una "persona bibliotecaria". Quando tutte le persone sono bibliotecarie, le biblioteche pubbliche si incontrano dappertutto, semplicemente cosí.

La visione che sostiene la Memoria del mondo è che il patrimonio documentale mondiale appartiene a tutte le persone e dovrebbe essere integralmente preservato e protetto, partendo da un riconoscimento delle pratiche e dei costumi culturali e rimanendo completamente accessibile a tutte le persone senza porte d'entrata. Per questo gli obiettivi specifici sono:

Facilitare la conservazione del patrimonio documentale mondiale attraverso l'uso delle tecniche piú appropriate come per esempio disseminare idee e informazioni, preparare training e workshop, essere disponibili a dare assistenza diretta, anche ponendo in relazione le persone e i collettivi con i progetti piú appropriati per loro.

Dare supporto all'accesso universale al patrimonio documentale fomentando quindi la produzione delle copie digitali cosi come la compilazione dei cataloghi accessibili su Internet, fino alla pubblicazione e distribuzione di libri, cd, dvd e altri prodotti, in forma piu ampia e ugualitaria possibile.

Tenere in conto le limitazioni esistenti proprie dei posti dove l'accesso ha implicazioni per coloro che lo custodiscono. Le legislazioni e altre contingenze relative all'accessibilita degli archivi devono essere rispettate. Le sensibilità culturali, includendo la protezione delle comunita indigene e dei suoi archivi, devono essere onorate.

Aumentare la consapevolezza a livello mondiale dell'esistenza e dell'importanza del patrimonio documentale. Gli strumenti necessari alla sua esistenza partono dallo sviluppo di registri fino alla produzione degli strumenti e di pubblicazioni promozionali e di carattere informativo. La preservazione e l'accesso non solo si complementano, ma influenzano anche la presa di coscienza del valore del patrimonio documentale, dato che che piú accesso comporta piú necessità di preservare. Per questo la produzione di copie deve essere incoraggiata per ridurre la pressione e la preservazione di materiale unico.

I temi che affiorano sono:

- lo sviluppo delle infrastrutture collettive e autonome
  - Prassi politiche sull'accesso e sulla creazione di conoscenza e documentazione
  - cultura libera e istituzioni per i beni comuni
  - Diversità culturale
  - Disobbedienza civile
  - Sovranità tecnologica

Persone e Collettivi

Davvero molto poco sarebbe stato possibile se Sean Dockray non avesse cominciato Aaaaarg, Dušan Barok Monoskop, Sebastian Luetgert e Jan Gerber Pirate Cinema & pad.ma Kenneth Goldsmith UbuWeb, Henry Warwick Alexandria project,Piratbyrån, The Pirate Bay e se gli hackers dietro Library Genesis non avessero dato l'opportunita' di scaricare il loro catalogo di quasi un milioni di libri. Queste persone sono punti di riferimento per questo progetto e lavorare con loro su questi temi ci traforma in una cumunità amichevole. Vogliamo anche sottolineare che ci manca molto Aaron Swartz.

Biblioteca pubblica (come modello di sviluppo)

La Memoria del mondo si articola nelle seguenti proposte con il fine di ottenere un'infrastruttura distribuita di biblioteche pubbliche:

- Sviluppare software per cataloghi punto a punto e per scambiare e condividere libri usando un plugin p2p per calibre che si chiama let's share books.
- Costruire scanner di libri DIY e incoraggiare la creazione di comunità sullo scanning di libri e altri materiali grafici di interesse (come per esempio a Zagreb, Belgrado, Ljubljana e in una fase iniziale in Barcelona, Berlino e Lüneburg).
- Organizzare eventi per facilitare lo sviluppo di strumenti liberi per queste biblioteche pubbliche, alimentare la sinergia e lo scambio di risorse, esperienze e conoscenze tra i gruppi lavorando su queste varie dimensioni(archivisti, documentaristi, librai, attivisti, sviluppatori, ricercatori, etc).

Un buon modo per sviluppare una biblioteca pubblica consiste nell'organizzare un evento di vari giorni in un posto e invitare persone e collettivi interessati in temi di accesso alla conoscenza, documentazione della memoria, educazione popolare, creazione di risorse pubbliche, costruzioni di scanner e amanti dei libri in generale. Molte persone e collettivi possono unire le forze per costruire e mantenere la proprio biblioteca digitale. Dentro del processo di crezione si possono incontrare i seguenti processi:

- Costruire e imparare a usare uno scanner di libri.
- Installare, configurare e imparare ad usare programmi liberi per costruire cataloghi e condividere in modo efficente collezioni di libri debitamente etichettate e documentate.
- Installare, configurare e imparare a usare i server dove si custodiranno i libri e i documenti digitalizzati e i cataloghi.
- Documentare e condividere quanto indicato sopra per permettere agli altri di avere anche loro la stessa esperienza.
- Identificare un primo gruppo di libri e altro materiale grafico di particolare interesse. Verrà presa in considerazione la rilevanza che hanno nel contesto dei collettivi presenti, dando speciale enfasi ai materiali maggiormente in pericolo (quelli che contano meno copie e sono per tanto di piú difficile accesso e condivisione).
- Scannerizzare, etichettare, e inserire i metadati necessari, etc.
- Diffondere la biblioteca pubblica e ideare meccanismi tali per cui sia possibile mantenere questi materiali nel corso del tempo.

Il tipo di materiali che si scannerizzano e documentano per primi, cosi come le metodologie che si usano per selezionarli, sono decisioni che gli stessi collettivi sviluppano per ogni biblioteca pubblica. Come parte della connotazione politica e filosofica del progetto, si vuole incoraggiare in prima istanza la creazione di biblioteche pubbliche con materiale che tratti dei movimenti sociali in tutta la loro varietà dando priorità ai materiali che rivelino trasformazioni sociali e politiche (pensiero critico, culture underground e poco documentate, lingue e temi poco presenti su Internet). Basandosi sulle esperienze precedenti, queste biblioteche funzionano meglio quando ci sono almeno un centinaio di libri.

Nenad Romić (aka Marcell Mars):

Difensore del software libero, esploratore culturale e istigatore sociale, Marcel è uno dei fondatori dell'istituto multimedia-mi2 e net.cultura mama club in Zagreb. Ha dato inizio alla GNU GPL per l'editoria e all'etichetta discografica EGOBOO.bits, oltre che al progetto Biblioteca Pubblica Memoria del Mondo. Contribuisce anche ad una serie di riunioni informali e periodiche affinché entusiasti del gruppo "mama" possano scambiarsi conoscenza, cosí come a incontri su satelliti g33koskop e incotri come "Nothing will Happen" o "The Fair of Mean Equipment".

- http://ki.ber.kom.uni.st | ki.ber[at]kom[dot]uni[dot]st

NOTE

1. http://www.digitalbookworld.com/2012/american-library-association-open-letter-to-publishers-on-e-book-library-lending/

2. http://lj.libraryjournal.com/2011/02/technology/ebooks/harpercollins-puts-26-loan-cap-on-ebook-circulations/
3. http://www.americanheritage.com/content/melvil-dewey

Anticensura

Dal niente da nascondere al niente da mostrare: sviluppare insieme pratiche più sicure in Internet

Julie Gommes

Mi piace molto quando la gente mi dice non ha niente da nascondere: "Quindi posso farti un video dentro la doccia?", sguardo esterefatto. Ma no! "Oppure, posso farti un video quando russi la notte? O almeno lasciami leggere la tua cartella medica....Ah, no?è che hai cose da nascondere?"

Ci saranno sempre aspetti della nostra vita che vogliamo mantenere intimi, per timidezza, paura, o semplicemente per il piacere di avere un giardino segreto, un mondo nostro. In più, se qualcuna non ha niente da nascondere allora nessuna le vorrà confidare un segreto. È problematico. Come fare dunque per avere amici? Questa idea di trasparenza radicale[1] che promuovono i difensori del web sociale-commerciale è una trappola per le nostre libertà individuali. Tanto più quando questo sforzo di trasparenza sembra non applicarsi ai nostri "rappresentanti" polici, né alle imprese. Quindi, perché la cittadinanza dovrebbe esporsi di forma continua per provare che non ha niente da nascondere?

La creazione attiva di spazi di sicurezza non può lasciare da parte le tecnologie digitali ed Internet. La sicurezza deve pensarsi come un congiunto di pratiche che ingloba le nostre identità fisiche ed elettroniche, le due faccie della stessa moneta. Se la sicurezza può interpretarsi come l'assenza di rischi o come la fiducia in qualcuna o qualcosa, deve essere interpretata anche come un processo multidimensionale. Questa visione significa saper proteggere il tuo corpo (del quale solo tu decidi!), il tuo diritto ad esprimerti, alla cooperazione, all'anonimato, ma anche il tuo diritto ad apprendere dagli strumenti e dalle applicazioni che ti difendono. Per questo bisogna capire che alternative esistono e come si possono usare, difenderle, appoggiarle.

La percezione di sicurezza dipende da come ci connettiamo, navighiamo e intercambiamo, ma anche del tipo di tecnologia che usiamo e con chi la usiamo. I sistemi operativi, il tipo di hardware, gli XISP, i server, i router contano. Le nostre finalità sociali e politiche influiscono nel tipo di sicurezza di cui avremo bisogno e come tenteremo scoprire, tappare o esporre le nostre traccie. A volte cercheremo l'anonimato, la autenticità, la prova di integrità delle comunicazioni, cifrare i contenuti, e altre volte cercheremo tutte queste dimensioni assieme.

Senza dubbio, il paradosso della privacy ci insegna che le persone generalmente hanno la tendenza ad affermare che si preoccupano per la loro intimità, ma quando gli si chiede che misure utilizzano per proteggerla, ci si rende rapidamente conto che non ne prendono nessuna, o quasi. Al principio di Internet, esisteva l'idea che potevamo stare li e adottare qualunque identità[2], come descriveva Steiner nel 1993: "On the Internet, nobody knows you're a dog[3]". Al giorno d'oggi questa epoca di internet è finita. Adesso ci etichettano, ci profilano, ci monitorizzano, ci analizzano. Siamo quello che il nostro grafico sociale[4] dice di noi, e coloro che non sviluppano pratiche per difendersi si incontrano totalmente esposte. Nude in Internet:"Si però ok...la sicurezza è difficile". O no, neanche tanto. Se prendi un tempo minimo per interessarti al tema, il tempo di riscrivere la tua password per impedire che si possa accedere ai tuoi dati se ti rubano il computer o lo smartphone, il tempo di alzare la testa per controllare se c'è una videocamera che guarda sulla tua tastiera. Il tempo di formulare le buone domande come, per esempio, a che rischi si è esposte e come prevenirli. O anche domandare come le tue pratiche on line espongono la vita privata delle tue amicizie o del collettivo con il quale vuoi cambiare il mondo.

Migliorare le proprie pratiche in Internet è anche essere più libere delle proprie opinioni, e poter esprimerle con sicurezza. Più libere di lavorare quando si è giornaliste, per esempio. Mi fa arrabbiare quando leggo "intervista realizzata su skype" con persone che possono morire per quella che io chiamo negligenza. Come giornalista, ed al di là di tutta la mia buona volontà e molti sforzi, mi sbagliavo anche io, per ignoranza. Oggi mi sorprende quando la persona con cui sto parlando non sa cos'è la Deep Packet Inspection[3], però, a dir la verità, neanche io lo sapevo fino ad un paio di anni fa. Quindi lo spieghiamo, lo ripetiamo una ed un'altra volta. Perchè prendersi il tempo per spiegare queste nozioni e strumenti a persone del proprio intorno -ma non solo- è un contributo fondamentale per promuovere un Internet ed una società più giuste per tutte. Imparare a proteggersi ed a non mettere le altre persone in pericolo ha bisogno di tempo ed attenzione, però conferisce automatismi che saranno salvifici nel quotidiano.

Presa di coscienza Al giorno d'oggi non si può ignorare lo spionaggio on line. Che si tratti delle rivelazioni di Edward Snowden rispetto alla NSA o delle detenzioni ripetute di oppositrici politiche, prima e dopo le rivoluzioni del 2011, non possiamo più ignorare che potenzialmente potremmo essere tutte sotto vigilaza. Questa situazione succede anche offline con la videovigilanza. Se sto in una grande via di negozi con delle amiche, ci sarà sicuramente una videoregistrazione di quel momento anche se la mia immagine, il mio sorriso, un momento di intimità o confidenza che non hanno niente a che fare in un dabase. È la mia vita.

Sdrammatizzare

La protezione della vita privata non è riservata ad un'elite di appassionate alla tecnica, e passa molte volte attraverso piccoli gesti quotidiani e, prima di tutto, per una presa di posizione. Tutte abbiamo rilevato, inclusa (e sopratutto) io, pezzi della nostra vita nel web, per mancanza di conoscenza delle consequenze. Tutte abbiamo parlato della vita privata delle nostre amiche, prima di renderci conto del danno che stavamo causando. Probabilmente abbiamo caricato foto nostre, perchè avevamo travestimenti fighi, perchè eravamo felici, perchè ci amavamo e non pensavamo che questi momenti sarebbero finito nell'ufficio di un agenzia di marketing o in un dossier dei servizi segreti.

Scegliere

Non siamo apostoli del fare bene, vivere meglio, nè le messaggiere della sacra protezione di dati. Vogliamo solo, con la tecnica che conosciamo, arricchita dagli errori commessi, darvi alcuni consigli basici per aiutarvi a proteggervi, o per lo meno, farvi riflettere su quello che (non) dovreste insegnare. Presto ci si renderà conto che bisognerà scegliere tra comodità e libertà, però, come diceva Benjamin Franklin "Un popolo pronto a sacrificare poca della sua libertà in cambio di poca sicurezza non merità né una cosa nell'altra, e

finisce per perdere entrambe." Quindi al lavoro! Per scappare dalla vigilanza in maniera semplice e senza dolore, bisogna solo rimpiazzare i vostri strumenti quotidiani con strumenti sicuri. PrismBreak[6], non importa il sistema operativo usato (si, anche windows, anche se ne sconsigliamo vivamente l'uso n.d.t.), propone strumenti che permettono schivare la vigilanza elettronica. E per evitare la videovigilanza il progetto "sotto vigilanza"[7], lanciato da persone francesi, permette consultare le mappe delle città dove ci si trova: Minsk, Mosca, Seattle, Parigi, etc, e così darsi appuntamento con le proprie fonti, amicizie, compagne di azione dove non ci sono videocamere e quindi evitare il pesante sguardo del Grande Fratello.

Dell'importanza della riappropiazione degli strumenti A ciascuna pratica/persona/necessità corrisponte uno strumento. Non ci si anonimizza nella stessa maniera se si è una docente-investigatrice che vuole recuperare delle lezioni o se si è un'adolescente che vuole scaricare la musica preferita. Interessarsi per il proprio compiuter, per capire come funziona è anche capire che non c'è una soluzione miracolosa o uno strumento rivoluzionario. Iteressarsi vuol dire anche domandarsi quali sono i programmi che possono essere malevoli. Per esempio, perché un'applicazione di disegno in uno smartphone chiede i permessi per avere accesso alla mia rubrica o al mio archivio di SMS? Perché un'applicazione di note ha bisogno di localizzarmi? Possiamo renderci conto molto facilmente di come i creatori di alcune applicazioni si danno permessi sui nostri dispositivi. Bisogna solamente leggere le caratteristiche prima di fare click su "Installa". Un'altra volta non si hanno bisogno di competenze tecniche per proteggersi, solamente curiosità verso gli strumenti che si usano.

Disciplina Possiamo imparare a lanciare e usare questo o quel software, creare partizioni crittate con Truecrypt[8], però se non siamo coscienti dei rischi che facciamo correre alle altre persone quando le chiamiamo al telefono o le mandiamo una email senza cifrarla, la tecnologia non serve a niente. Oltre il difficile apprendimento degli strumenti, è una disciplina che bisogna imparare, essere coscienti di quello che facciamo o di quello che non facciamo e delle conseguenze che possono portare. È una presa di coscienza quotidiana. È importante creare momenti di apprendimento collettivo, momenti di interscambio, per poter pensare la sicurezza in una rete personale dove anche le amicizie e i parenti adottano queste pratiche per creare un circolo virtuoso dove ognuna stimola le altre. Scambiarsi email cifrate, scegliere un'indirizzo email che non dipenda da un'impresa commerciale, o lavorare insieme a tutorial e manuali sono buone pratiche di appoggio mutuo.

Anonimato, perché? Come? Oltre le soluzioni tecniche, l'anonimato e l'uso di pseudonimi possono constituire soluzioni semplici alla vigilanza. L'uso di pseudonimi è mostrare un'altra identità in Internet, che sia di corta o lunga durata, che serva per una chat di alcuni minuti o per identificarsi in un forum nel quale si parteciperà per anni. L'anonimato è non lasciare nessuna traccia che permetta il riconoscimento. Alcuni strumenti semplici lo permettono. Tor[9], per esempio, fa compiere dei salti da un server ad un altro alla vostra richiesta [di pagina web?]. Il risultato? È l'indirizzo IP di uno dei server che se la salverà e non della vostra connessione.

Crittare, un gioco da ragazze Inviare una mail "transparente" è lo stesso che inviare una cartolina. Il postino la può leggere nel cammino, vedere la foto, può scherzarci su, etc. La vostra cartolina viaggia senza protezione né contro la pioggia né contro occhiate indiscrete. Con le vostre email succede lo stesso. Tranne se, come nel sistema di posta, si mette il messaggio in una busta. La busta digitale si ottiene crittando. Quando eravamo bambine, lo facevamo in piccola scala inviandoci messaggi segreti con le amiche. Allo scegliere un codice tipo "saltare di tre lettere", "Ti voglio bene" si trasforma in "zo brlonr ehqh ". Adesso che siamo adulte non è molto più complicato. La differenza è che i computer lavorano per noi e fanno sì che crittare sia ancora più complesso, più difficile da rompere, con caratteri speciali, algoritmi che crittano un messaggio senza nessuna corrispondenza con il prossimo che critteranno.

Della servitù volontarie Nel caso delle e-mail, quando facciamo click su "inviare" il messaggio questo viene imagazzinato in quattro copie:

1. Il primo nella cartella di invio della mittente, si trova facilmente andando sulla cartella "posta inviata".
2. Il secondo, nella cartella in entrata della destinataria. Fino ad ora niente di anormale, tranne che...
3. La terza copia viene imagazzinata in un server del signore Google, della signora Yahoo, l'impresa della email della mittente. Bisogna aggiungere che chiunque abbia accesso a questi server, che lavori o meno

per questa compagnia, può avere accesso a queste email.
4. E non finisce qui, visto che la quarta copia la conserva la signora Google, il signor Yahoo, l'impresa della email della destinataria. Quindi, ancora una volta, chiunque abbia accesso a questi server, che lavori o meno per questa compagnia, può avere accesso a queste email.

Cancellare i messaggi dalla cartella in arrivo o di uscita dell'interfaccia non li cancella dai server, li stanno imagazzanati e li rimangono. Anche se tutto questo sia detestabile rispetto la vita privata, siamo noi che permettiamo che si possa fare.

Conclusioni Proteggere la propria vita privata, quella delle persone che si relazionano a noi, delle nostre amicizie, non si improvvisa, però non è una sfida insuperabile. A volte basta riflettere prima di cliccare, prima di installare un'applicazione. Il resto è solo tecnica e sta alla portata di tutto il mondo, basta solo volerla apprendere.

ALcune guide e tutorial per iniziare Security in a box: una guida che spiega che strumenti usare a seconda della situazione concreta. Esiste in 13 lingue: https://securityinabox.org/

How to bypass Internet censorship: La spiegazione passo passo dell'installazione della maggior parte degli strumenti di sicurezza, attraverso screenshot esplicativi. Esiste in 9 lingue: http://howtobypassinternetcensorship.org/

Prism Break: proteggersi sul cellulare e sul computer sostituendo i prori strumenti con strumenti sicuri: https://prism-break.org/

Cryptocat: un software di chat sicuro attraverso il proprio navigatore: https://crypto.cat/

Julie Gommes Analista in cybersicurezza e giornalista che scrive codice e parla con il suo computer con linee di comandi. Ha vissuto e lavorato in Medio Oriente enel sud-est asiatico. Partecipa in diversi collettivi per difendere la neutralità della rete e lottare contro la società della vigilanza.

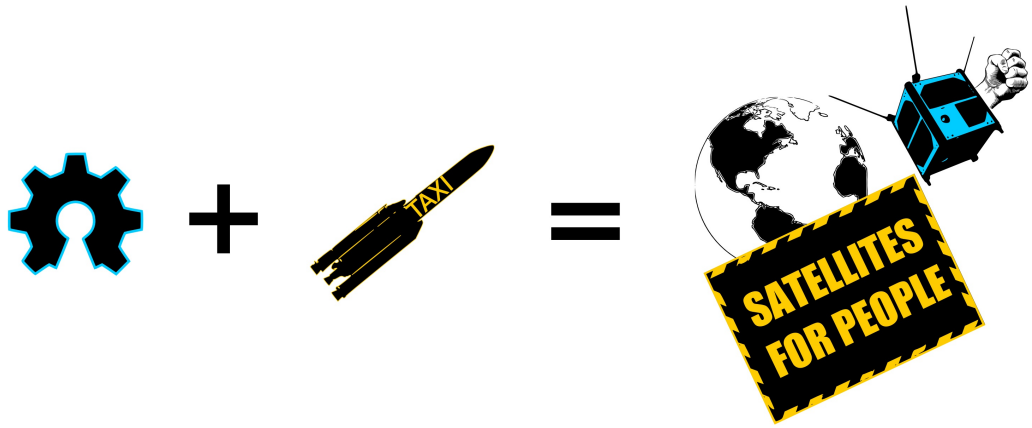
Il suo blog in francese: http://seteici.ondule.fr jujusete[at]riseup[point]net PGP D7484F3C e @jujusete su twitter.

NOTE

> [1]. http://www.ippolita.net/fr/libro/la-confidentialit%C3%A9-n%E2%80%99est-plus-l%E2%80%99id%C3%A9ologie-de-la-transparence-radicale ↩
>
> [2]. Vedere la famosa immagine del New Yorker. https://upload.wikimedia.org/wikipedia/en/f/f8/Internet_dog.jpg ↩
>
> [3]. https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog ↩
>
> [4]. http://es.wikipedia.org/wiki/Grafo_social ↩
>
> [5]. Ver https://es.wikipedia.org/wiki/Inspección_profunda_de_paquete ↩
>
> [6]. In 26 lingue, PrimBreak propone come proteggersi usando cellulare o computer sostituendo gli strumenti con strumenti protetti: https://prism-break.org/en/ ↩
>
> [7]. Cartografia collaborativa della videosorveglianza: www.sous-surveillance.net ↩
>
> [8]. http://www.truecrypt.org/ ↩
>
> [9]. https://www.torproject.org/ ↩

Una odissea spaziale autogestita

Marta G. Franco & Spideralex



Nei racconti di fantascienza venne sviluppata l'idea di un futuro tecnologico, in cui lo spazio sarebbe stato sfruttato per facilitare le comunicazioni terrestri attraverso onde elettromagnetiche. I satelliti artificiali furono teorizzati dal specialista di radar e ufficiale militare Sir Arthur C. Clarke, poi internazionalmente riconosciuto come l'autore di "2001, odissea nello spazio". Nel suo articolo, pubblicato nel 1945 sul Wireless World, egli stabilì le fondamenta per la creazione dei satelliti geostazionari, oggi messi -in suo onore- sull'orbita di Clarke al di sopra sopra dell'equatore terrestre.

Negli anni 50, nel pieno della guerra fredda e della corsa allo spazio, l'esercito statunitense realizzò i primi sperimenti per lo sfruttamento dello spazio nella propagazione di radiocomunicazioni impiegando la luna come riflettore passivo. In questo contesto storico, il principale argomento di riviste pulp come "Satellite Science Fiction"[1] era la minaccia di pericolosi alieni filocomunisti. Nel 1957, l'Unione Sovietica lancia il primo satellite artificiale Sputnik, cui segnali radio -sotto forma di segnali acustici- possono essere ancora ascoltate qui[2]. Evento scatenante d'una isteria di massa negli Stati Uniti finché, nel 1962, riuscirono a lanciare in orbita il Telstart I, permettendo la creazione del primo collegamento televisivo internazionale e, dunque, l'espansione del raggio di diffusione della cultura nordamericana.

Paradossalmente, l'avveramento e realizzazione della corsa allo spazio risultò più noiosa di quanto la cultura popolare avesse previsto. Motivo per cui l'Associazione di Astronauti Autonomi, coalizione neo-situazionista di esploratrici anonime, mise in luce che le élite tecnologiche *tentano soltanto di riempire il paesaggio mentale della nostra memoria con la loro versione dei viaggi spaziali, la quale potrebbe essere più o meno "Tu non devi andare da nessuna parte. Soltanto devi restare seduto e guardare come noi viaggiamo verso le stelle"*[3]. Anche se al suo tempo pareva si parlasse di fantascienza, nei due decenni successivi alla pubblicazione del loro manifesto, e in risposta alla militarizzazione e privatizzazione delle tecnologie spaziali, sono sorte diverse iniziative che mirano e lottano per **l'esplorazione spaziale "dal basso"**.

Un traguardo importante verso l'uso libero di satelliti miniaturizzati nell'ambito delle telecomunicazioni è stato raggiunto nel 1961 col lancio di OSCAR (Orbiting Satellite Carrying Amateur Radio) da un collettivo di radioamatori. I satelliti miniaturizzati si distinguono per la dimensione ridotta e per pesare solamente mezza tonnellata, caratteristiche che li rendono più economici rispetto ai satelliti convenzionali, anche perché possono essere messi in orbita da razzi più leggeri. Questi satelliti si muovono in orbite medie o basse emettendo segnali direttamente a dispositivi mobili sulla terra.

Nel 2008, Kristian von Bengtson e Peter Madsen danno vita al progetto senza scopo di lucro Copenhagen Suborbitals[5], il cui obiettivo è la costruzione ed il lancio di razzi sviluppati al di fuori dei programmi spaziali dei governi e delle multinazionali. Attualmente il progetto se la cava piuttosto bene e riceve una crescente collaborazione volontaria di ingegneri aerospaziali.

Un'altro aspetto fondamentale riguardante i satelliti artificiali è circoscritto nell'ambito della sovranità nazionale. Motivo per cui il governo venezuelano[6] prende la decisione **nel 2008 di lanciare il satellite Simón Bolívar**, permettendo a delle regioni isolate del Venezuela l'accesso a diversi servizi di telecomunicazioni nonché a programmi educativi e di sanità a distanza. Il Simón Bolívar si trova in un'orbita geostazionaria appartenente all'Uruguay, che può fare uso fino al 10% della sua capacità di comunicazione.

Considerando l'aumento esponenziale nella produzione di contenuti audiovisivi, nel traffico d'internet e gli innumerevoli tentativi di regolazione, controllo e censura di questi spazi, risulta evidente che la dipendenza nelle comunicazioni satellitari cresce ogni giorno di più. Per esempio, dopo che l'11 giugno 2013 la televisione pubblica greca ERT viene chiusa su decisione del governo, i suoi dipendenti portarono avanti una forte mobilizzazione per continuare a trasmettere dei contenuti tramite radio e internet e, tra le diverse azioni intraprese, lo scorso 28 agosto pubblicarono un'appello internazionale chiedendo il supporto della loro lotta attraverso la cessione di banda satellitare per la trasmissione della loro programmazione.

È per questa dipendenza che diversi collettivi si sono posti l'obiettivo di lanciare dei propri satelliti in orbita, assicurando così la loro presenza nello spazio interstellare. Satelliti il cui scopo potrebbe essere di assicurare l'afflusso libero dell'informazione anche nei momenti in cui si pretenda chiudere il rubinetto di internet, come successe d'altronde a Tunisia ed Egitto durante la primavera araba. Nel corso dell'ultimo Chaos Computer Camp, celebrato nell'estate del 2011 e organizzato dal Chaos Computer Club[8], Nick Farr feci un'appello[9] per far si che la comunità hacker iniziasse a lavorare assieme in un progetto per il lancio di satelliti e, più in là, di hacker sulla luna. In risposta, nacque il Hackerspace Global Grid[10], proggetto sviluppato dai membri del hacklab tedesco Shackspace[11], assieme a Constellation[12], progetto di calcolo parallelo[13] specializzato nell'ambito aerospaziale.

Al momento, i loro obiettivi principali sono focalizzati nello sviluppo di una rete distribuita di sensori capaci di rintracciare e comunicare con i satelliti amatoriali localizzati nelle orbite basse. Come sottolineato da Farr, il primo scopo è di creare una conoscenza libera riguardante lo sviluppo di dispositivi elettronici in grado di restare in orbita. È di particolare rilievo osservare che nella diffusione mediatica il progetto viene descritto in modo succinto come il satellite che permetterà di evadere la censura internet. Nonostante ciò, nelle domande frequenti del progetto, vien chiarito che attualmente gli obiettivi sono altri. Ciò non implica però che in un futuro l'HGG non possa coprire tale aspetto, poiché rispetto allo stato attuale c'è ancora molto lavoro da fare prima di raggiungere tale meta.

Infine, occorre menzionare che si trova già nello spazio l'OSSI-1 (iniziativa di satellite open source -1), dispositivo amatoriale lanciato lo scorso 19 aprile 2013, uno dei sei piccoli satelliti lanciati assieme al Bion-M No.1 dell'Accademia russa delle scienze, disegnato dall'artista e radioamatore coreano Hojun Song impiegando la tecnologia arduino. A discapito delle aspettative, l'apparecchio casereccio non è stato in grado di comunicare con la Terra. Le istruzioni dell'assemblaggio si trovano liberamente disponibile sulla pagina web opensat.cc, per essere consultate e migliorate.

Mentre la comunità hacker si prepara, potrebbe essere nel tuo interesse scoprire come si occupano satelliti militari in disuso o in semi-attività. I satelliti comunemente conosciuti come Bolinhas in Brasile corrispondono a satelliti militari SATCOM statunitensi. La maggioranza delle trasmissioni nella loro frequenza si produce nella Amazzonia brasiliana e colombiana. Per cui camionisti, commercianti, segherie, professori e

trafficanti possono comunicare a basso costo. L'impiego di questa banda e illegale e le autorità statunitensi si dedicano alla geolocalizzazione degli 'okupa' attraverso la triangolazione dei segnali. Con la collaborazione delle autorità brasiliane, 39 sospettati sono stati accusati nel 2009 dell'uso illegale di tali infrastrutture militari, per cui sono state confiscate le loro apparecchiature e sanzionati con multe severe. Un video[14] realizzato da Bruno Vianna introduce questa realtà, mettendo in evidenza l'utilizzo di questa banda come strumento di disobbedienza civile, come indicato da Alejo Duque, membro del Movimento Dos Sem Satélite[15] il cui manifesto dice: "Che ruolo noi, al riparo e ben alimentati, possiamo giocare nella creazione di una sovranità delocalizzata? E nella generazione e diffusione di conoscenza che permetta ribaltare la tendenza autodistruttiva dell'umanità? L'ipotesi di questo manifesto è un'equazione diretta verso una scintilla che si affaccia sul'orizzonte: realizzeremmo il nostro primo satellite fatto a mano e l'invieremmo allo spazio siderale tra orde di satelliti industriali, aziendali e governativi"[16].

RIFERIMENTI

http://www.larazon.es/detalle_movil/noticias/LA_RAZON_424968/5924-los-hackers-ya-tienen-satelite#.UhN3ptdDT6n

Hacker Space Global Grid: http://en.wikipedia.org/wiki/Hackerspace_Global_Grid

---

Marta G. Franco

Giornalista e attivista. Lavora e milita nel giornale Diagonal. Partecipa in diverse iniziative di hacktivismo, tanto digitali come analogiche, associate alla comunicazione, femminismo, cultura libera e autonomia.

Spideralex

Hacktivista e cyberfemminista, Spideralex abita all'interno della rete e partecipa attivamente nelle iniziative di sovranità tecnologica portando avanti diverse ricerche di rilievo. spideralex[at]riseup[dot]net

---

NOTE

1. http://www.philsp.com/mags/sf_s.html#satellite_science_fiction ↩

2. http://es.wikipedia.org/wiki/Archivo:Possible_PDM_signal_labeled_as_Sputnik_by_NASA.ogg ↩

3. http://www.ain23.com/topy.net/kiaosfera/contracultura/aaa/info_guerra.htm ↩

4. I satelliti possono essere caratterizzati in basse all'orbita che percorrono (geostazionaria, bassa, media, polare oppure equatoriale) e anche in funzione della loro applicazione (per telecomunicazioni, meteorologici, per la navigazione, militari, per telerilevamento oppure scientifici). ↩

5. Si invita al lettore ad approfondire nella apposita documentazione: http://www.copenhagensuborbitals.com/ ↩

6. Secondo María Eugenia Salazar Furiati, il progetto è stato concepito nel 1977 da 5 nazioni andine (Bolivia, Colombia, Ecuador, Perù e Venezuela), partendo dagli studi tecnici necessari per fondare l'uso di determinate posizioni orbitali, posizioni di seguito assegnatagli dall'Unione Internazionale delle Telecomunicazioni (ITU), entità internazionale che regola tali attribuzioni. Presso da: http://www.gumilla.org/biblioteca/bases/biblo/texto/COM2009146_53-64.pdf ↩

7. http://www.ertopen.com/news-in-4-languges/english/item/3849#.UiOnVNdDT6k ↩

8. https://es.wikipedia.org/wiki/Chaos_Computer_Club ↩

9. http://events.ccc.de/camp/2011/wiki/Space_program_of_the_Hacker_Scene:_For_our_future ↩

10. http://en.wikipedia.org/wiki/Hackerspace_Global_Grid ↩

11. http://shackspace.de/ ↩

12

12. Il calcolo distribuito è un paradigma computazionale un cui i compiti informatici vengono risolti impiegando un elevato numero di computer autonomi collegati, in base a una gerarchia data, attraverso un'infrastruttura di rete. ↩

13. http://aerospaceresearch.net/constellation/ ↩

14. Satelites Bolinhas (Brasil) http://www.youtube.com/watch?v=veDZfejpbs8 ↩

15. MSST: Movimento Sem Satelites http://devolts.org/msst/ ↩

16. http://devolts.org/msst/?page_id=2 ↩

Contributi

Editrice: Alex Hache

Coordinatrice: Erika Campelo

Disegno grafico ed editing: Foockinfoo, Elle Flâne

HTML e markup: Tatiana de la O

Traduzione in castigliano: Bruno Lakmeche

Traduzione in francese: Elisabeth Teixeira

Traduzione in catalano: Xavier Borràs i Deliris

Traduzione in italiano: HacklabB0

Revisione del castigliano e catalano: Aarón Fortuño

Ringraziamenti

Patrice Riemens, Richard Matthew Stallman, Benjamin Cadon, Elle Flâne, Tatiana de la O, Karlessi, Ippolita, Marcell Mars, Hellekin, Julie Gommes, Jorge Timon,Marta G. Franco, Maxigas, Ursula Gastfall, Thomas Fourmond, Paula Pin.

Margarita Padilla, Erika, Justine, Javier de Rivera, Antonio, WaiWai, Lilith, Michael, Tripta, Ank.