Un luddista si dondolava sopra un filo di ragnatela

riflessioni su open source, creative commons e sul capitalismo della sorveglianza

-[jolek78]-

Un Luddista
si dondolava sopra un filo di ragnatela

Riflessioni su open source, creative commons
e sul capitalismo della sorveglianza

jolek78

Prima bozza completata: 13/02/2021
Seconda bozza completata: 25/04/21
Terza bozza completata: 13/01/2022

A dibbì
perché senza di lui tutto questo non sarebbe mai successo

Ma poi quassù ritorno
Lo so che verrà un giorno in cui saremo un po' di più
Perché ci credo che in fondo dietro ogni galera c'è una scala che va su
Sul tetto - Rein

Indice

Cronologia

- 1960: Prime ricerche del DARPA
- 1964: Nasce il BASIC
- 1969: Nasce la rete ARPANET
- 1975: Primi test di connessione
- 1976: Lettera di Bill Gates agli hobbysti
- 1977: Apple produce Apple II
- 1978: Prima connessione dial-up di una BBS
- 1983: ARPANET adotta il protocollo TCP/IP
- 1985: Richard Stallman fonda la Free Software Foundation
- 1989: Cade il muro di Berlino
- 1989: ARPANET si demilitarizza - Nasce Internet
- 1991: Lettera di Linus Torvalds - Nasce Linux
- 1992: Nasce la Internet Society
- 1993: Prima release di Mosaic
- 1995: Prima release di Netscape
- 1998: Nasce il ICANN
- 1998: Eric Raymond fonda la open source Initiative
- 1999: Nasce Indymedia
- 1999: La battaglia di Seattle
- 1999: Nasce Freenet
- 1999: Prima release di Ajax
- 2001: Lawrence Lessing fonda la Creative Commons
- 2001: 11/9 e Patriot Act

- 2003: Nascita di Tor
- 2003: Anti-war protest
- 2004: Facebook esce dalla sua fase di beta
- 2006: Chiusura di PirateBay
- 2006: Nasce PlosOne
- 2006: Nasce il Pirate Party
- 2006: Julian Assange fonda Wikileaks
- 2008: Crisi dei subprime
- 2008: Satoshi Nakamoto crea Bitcoin
- 2008: Google lancia Android
- 2009: Iran e la Twitter Revolution
- 2010: Scoppia la Primavera Araba
- 2012: Obama - Primo mandato
- 2012: Steve Bannon rileva Breitbart News
- 2013: Edward Snowden contatta Glenn Greenwald
- 2015: Obama - Secondo mandato
- 2016: Referendum sulla Brexit
- 2016: Nasce Mastodon
- 2017: Elezione Donald Trump
- 2017: Wikileaks pubblica Vault7
- 2018: Scandalo Cambridge Analytica
- 2018: Nasce il protocollo ActivityPub
- 2019: Prima release della Hippocratic License
- 2020: Pandemia Covid-19
- 2020: Attacco a Capitol-Hill

Excusatio non petita, accusatio manifesta

Questo non è un lavoro scientifico.
Sebbene faccia spesso uso di dati, citazioni, parametri e statistiche, l'analisi realizzata è frutto, e forse altro non potrebbe essere, dei miei bias culturali ed ideologici. La mia naturale ritrosia ad esprimere pareri personali deriva dal fatto che ho passato troppo tempo a raccontare dati scientifici, ad investigare e risolvere problemi informatici.

Ho sempre pensato che il buon argomentare sia un'arma potenzialmente a doppio taglio e che solo i numeri possano restituire ordine laddove ordine non c'è.

Ma il mio passato giornalistico mi ha insegnato una cosa: il mito dell'informazione imparziale va assolutamente ridimensionato. Tutte le volte che guardiamo alla realtà, o tutte le volte che la raccontiamo, lo facciamo con i nostri occhi, con le nostre paure, i nostri dubbi, le nostre speranze. E questo libro non è da meno.

Ho una confessione da fare: si, anch'io sono affetto da bias cognitivi. E si, anch'io quando analizzo il mondo che mi circonda lo faccio con i miei occhi e non con gli occhi di un ipotetico e imparziale algoritmo. Quindi è altamente probabile che io abbia utilizzato del "cherry picking" nel selezionare le fonti e nell'analizzare i dati, ma sono un partigiano e odio gli indifferenti, come avrebbe detto Gramsci. E come partigiano prendo parte, parteggio per una visione del mondo libera, indipendente, e avulsa da controlli esterni e catene.

I miei occhi sono importanti.

Introduzione

Il tizio che scrive sono io, jolek78, uno dei tanti non-più ragazzi che, per voglia, curiosità o disperazione sono scappati via dall'Italia. La mia vita in sostanza si può riassumere in poche parole: da piccolo giocavo con i lego, da adolescente con i circuiti elettrici, diventando grande ho cominciato a giocare con i computer.

Combatto contro la depressione da quando ne ho memoria e di certo questo periodo di lockdown (con tanti ringraziamenti alla zoonosi) non è stato di aiuto. Ma qualcosa è successo: il silenzio, l'isolamento dal mondo circostante e la solitudine mi hanno forzatamente costretto a riflettere su molte cose.

Lavoro nel mondo dell'Information Technology ormai da più di 6 anni ma la mia passione, quella vera, è da ricondursi al giornalismo, sopratutto quello scientifico. Ho fondato, tanti anni fa, con un gruppo di amici, un sito che diventò il portale italiano per l'astronomia (per chi se lo ricorda ancora si chiamava Astrofili.org). E poi, pochi anni dopo, grazie a una serie di eventi che preferisco non esplorare in questa sede, mi imbarcai in un progetto che portai avanti per 5 anni. Era un podcast scientifico, si chiamava Caccia al Fotone, e lì, a mie spese, imparai l'importanza della comunicazione e il ruolo che il buon giornalismo può avere su un pubblico attento.

Ecco perché scrivo questo libro.
Perché le mie riflessioni, quello che ho imparato, quello che ho vissuto e studiato nel corso di questi anni, spero possano essere utili a qualcuno, anche soltanto per fornire dei piccoli spunti di riflessione. I tempi che viviamo non sono semplici e i problemi che ci troveremo ad affrontare si potranno risolvere soltanto con l'aiuto di tutti. Questo è semplicemente il mio minuscolo pezzo di codice.

Capitolo 0 - Il cyber partigiano

Prologo

C'era una volta Caitlin Decter, una ragazza non vedente che, grazie a uno strumento tecnologico chiamato eyePod, riusciva a "vedere" il Word Wide Web e comunicare con Webmind, una entità profonda che viveva al suo interno. Quando lessi questa storia nella trilogia WWW[(#1)] di Robert J. Sawyer fu amore a prima vista. In qualche modo sembrava toccare alcuni punti chiave che mi avevano "tenuto in vita" - passatemi l'espressione - fino ad allora. In un'intervista l'autore dichiarò che il suo lavoro di scrittura cominciò grazie a un articolo pubblicato su New Scientist in cui si leggeva che "il word wide web, nel suo complesso, aveva lo stesso numero di sinapsi di un cervello umano". Idea affascinante, e spaventosa allo stesso tempo.

La relazione fra Caitlin Decter e Webmind mi disse una cosa: il web poteva essere non soltanto un individuo super-intelligente, ma anche un individuo pensante ed empatico da tutelare. Una nuova versione del Robbie dei racconti di Asimov in cui ci si domanda da quando si possa trattare un robot sullo stesso piano di un essere umano.

Salvate il soldato Internet

Capitolo 1 - Una mattina mi son svegliato

Chi (non) vuol essere individualista

Quella che oggi si chiama "citizen science" nacque grazie a un piccolo sogno: la ricerca di intelligenze extraterrestri. Il progetto SETI, acronimo di "Search for Extra-Terrestrial Intelligence", è noto al pubblico per essere quel tipo di ricerca astronomica che scandaglia il cielo in banda radio, analizza i dati e cerca d'individuare se, nell'oscurità del cosmo, qualche lontana civiltà extraterrestre sta cercando di comunicare con noi. Questo lavoro lo fa utilizzando i tempi morti delle antenne radio sparse per il mondo. Una serie di pionieri della radioastronomia si domandarono come fare ad aumentare la potenza di calcolo: bisognava distribuire un software, installabile dagli utenti sui propri personal computer, che permettesse di elaborare pochi dati alla volta ma in un tempo rapido. Quel pacchetto si chiamava "Seti@Home" e il suo compito era di scaricare i dati, analizzarli con la FFT - trasformata veloce di Furier - e restituirli indietro al centro radioastronomico di Arecibo. La risposta fu immediata: quasi due milioni di appassionati scaricarono il programma in tutto in mondo e fu letteralmente un successo planetario.(*1)

Analogamente nel 2006 la dottoressa Ilaria Capua, che si trovava a lavorare sul virus H5N1 - la meglio nota influenza aviaria - prese una decisione storica: decise di pubblicare l'intera sequenza genica di cui era in possesso su un database "open access" chiamato GenBank. Questa decisione, presa in polemica con buona parte dell'accademia, si rivelò provvidenziale. Rendendo pubblici i dati, si rese partecipe di un estremo atto di fiducia verso la comunità scientifica. Anche qui la risposta fu immediata: quasi un anno dopo l'azienda medica Sanofi Pasteur produsse il primo vaccino contro l'aviaria e si poté cominciare a combattere una influenza che, a memoria d'uomo, non aveva mai avuto una mortalità cosi alta.(*2)

Questi sono soltanto due piccoli, ma importanti, esempi che ci dicono qualcosa di fondamentale: l'individualismo, mantra dei nostri tempi, è dannoso per l'intera umanità. La collaborazione fra esseri umani liberi e indipendenti è capace di accelerare lo sviluppo e portare ad un progresso. Mettere un blocco - che sia esso sociale, politico o economico - è sconveniente per tutti, rallenta la diffusione delle idee e impedisce la loro rapida evoluzione.

Sediamoci a capotavola

Nel libro del 2019 "Talking to my Daughter"[(#2)], Yanis Yarufakis - economista greco ed ex-ministro delle finanze nel governo Siriza - spiega:

"In questo periodo storico, siamo nel mezzo di un processo di meccanizzazione e automazione, di digitalizzazione e intelligenza artificiale. Sfortunatamente però, questo processo ci porterà nella direzione opposta a una soluzione, poiché il suo presupposto non è quello di conciliare gli uomini con le macchine ma di rimpiazzare i primi con le seconde".

L'esperienza di Yarufakis è piuttosto significativa, considerando che politicamente tocca con mano la crisi post-2008 e accademicamente è un esperto di "game theory", disciplina tramite la quale si studia l'evoluzione di sistemi complessi come quelli economici. Ma in che modo l'economia interseca i processi tecnologici che stiamo vivendo? Dobbiamo a questo punto fare un salto indietro nel tempo, e andare al 1998 quando Larry Page e Sergey Brin, giusto due anni dopo l'uscita del browser web Netscape[(*4)], fondarono una azienda che di lì a poco sarebbe diventata un colosso mondiale. Si chiamava Google, era un motore di ricerca e incorporava al suo interno una semplice idea: assegnare un valore a ogni sito web a seconda del numero di link da cui veniva richiamato. Questo famoso algoritmo si chiamava "page-rank" e Google diventò, nel deserto quasi caotico di quegli anni (Yahoo - Altavista etc…), il motore di ricerca sul web più utilizzato al mondo. Fondato però da due geek che si rifiutavano, con tutte le forze, di introdurre le inserzioni pubblicitarie, Google stava rischiando di diventare rapidamente una magnifica idea che sarebbe morta nel giro di pochi anni[(*5)].

All'apparire dei cookies - piccoli oggetti che tracciavano la navigazione di un utente su ogni sito web - quindi Google ebbe l'idea: cominciare a sviluppare una sorta di IA - intelligenza artificiale - che creasse una esperienza personale e privata - quella che oggi chiamiamo filter-bubble - da poter vendere sul mercato degli inserzionisti[(*4)]. Nella prima fase i fruitori di Google non avrebbero visto inserzioni

pubblicitarie ma avrebbero avuto una esperienza di ricerca "personalizzata" per le loro esigenze. Successivamente, quando arrivarono le inserzioni, discrete e ben identificabili, con i metadati degli utenti già presenti nei database, Google potè cominciare ad indirizzare i "consigli per gli acquisti" a chi ne era potenzialmente interessato. Come possiamo leggere nel monumentale libro "The Age of Surveillance Capitalism"[(#3)] scritto dalla sociologa e filosofa Shoshana Zuboff:

"Quando un capitalista assume dei lavoratori, li integra nella produzione e provvede a un salario. Ma non qui, dove i lavoratori non sono pagati per il loro lavoro, e non sono integrati nella produzione. [...] Spesso si sente dire che gli utenti sono il prodotto. Non è esatto. Il prodotto del capitalismo della sorveglianza è quello di prevedere le nostre azioni"

E aggiunge:

"Gli utenti sono usati come oggetti di un non-mercato, in modo da sviluppare la missione di Google che è quella di classificare coerentemente le informazioni disponibili sul web, e renderle accessibili e utili a tutti".

È così che cominciò tutto: un semplice metodo creato per poter sopravvivere sul mercato, e per impedire a un'idea, oggettivamente migliore delle altre, di scomparire nell'universo dei motori di ricerca. Fu nel 2001, all'indomani degli attacchi dell'11 settembre, che i metadati divennero letteralmente oro digitale per i governi di tutto il mondo. Possederli diventava priorità nazionale, da realizzare a tutti i costi, privacy inclusa. Da allora, cercando di tutelare la sicurezza internazionale, cominciammo lentamente a perdere la sicurezza personale, trasformando lo "stato di eccezione" in "stato di normalità".

Homebrew Computer Club e Goedel

Nel 1975, sulle pagine della newsletter del Homebrew Computer Club, apparve una lettera scritta da Bill Gates[(*6)], che faceva pressappoco cosi:

"Come la maggior parte degli hobbisti sa, molti di voi hanno rubato il mio software. Per voi poco importa se chi ha scritto il codice non abbia ricevuto compenso per il suo lavoro. Questo secondo voi è giusto?"

Negli anni '70 l'informatica, come la conosciamo oggi, stava letteralmente esplodendo. Da lì a poco si sarebbe passati dagli amplificatori a valvole ai transistor(*7) e i computer, tanto grandi da riempire stanze intere, si sarebbero rimpiccioliti fino al punto da diventare "personal". Ma a quei tempi c'era anche una guerra di idee in corso. In questa battaglia, che correva sul filo delle tastiere, si confrontavano due fazioni: la prima lottava per la libertà di programmazione, il codice sorgente aperto e la condivisione delle idee(*8), mentre la seconda sosteneva la necessità di tutelare il lavoro informatico, sosteneva il software proprietario, e scoraggiava così la pirateria e la condivisione delle fonti.

L'evento storico che scatenò la diatriba fu la vendita, da parte della MITS - Micro Instrumentation and Telemetry Systems - di un nuovo gioiello tecnologico basato su processori Intel. Questo primo personal computer, denominato Altair-8800, veniva venduto fornito di un interprete, l'Altair-BASIC(*9), creato da una neonata azienda fondata da un giovane fino ad allora sconosciuto: l'azienda si chiamava Micro-Soft(*10) e il giovane era un certo Bill Gates. Durante la presentazione del progetto, un piccolo - e storico - gruppo di appassionati di informatica, l'Homebrew Computer Club, si presentò a Palo Alto per assistere all'evento. Fu qui che Steve Dompier, uno dei membri del club, trafugò una copia del BASIC rendendola disponile anche agli altri iscritti.

Ma c'è dell'altro. Le due schede di memoria fornite con il computer non erano le migliori sul commercio, erano difettose e avevano problemi di progettazione. Fu così che Robert Mash, un altro membro del Club, lavorò sui sorgenti e produsse nuove e migliorate memorie a 4k, compatibili con l'Altair e con il BASIC. In breve tempo, molti appassionati cominciarono a comprare l'Altair-8800 dalla MITS insieme alle schede di memoria compatibili. Per quanto riguarda il BASIC, beh per quello si poteva sempre averne una copia di straforo da qualcuno...

La pirateria ebbe i suoi effetti: in due anni il BASIC divenne l'interprete più popolare per macchine con processori Intel e un suo porting, sviluppato da una altra neonata azienda - la Apple - cominciò a girare sul celeberrimo personal computer Apple II(*11). Avrebbe detto Kurt Gödel: "se un sistema assiomatico può dimostrare la sua stessa coerenza, allora deve essere incoerente"(*12). L'assioma del "io produco software, io devo essere pagato" stava così lentamente crollando su se stesso.

Just for Fun

Mentre negli Stati Uniti si sviluppava la battaglia fra "hobbisti" e "professionisti", in un altro continente un giovane ragazzo finlandese, Linus Benedict Torvalds(#6), riceveva in regalo il suo primo computer. Era Un Commodore Vic20(*13) - uno dei primi personal computer "popolari" - e fu amore a prima vista. Il ragazzo, inesperto e goffo, - come siamo tutti a quell'età - si appassionò così tanto a quella strana diavoleria che decise di imparare il suo primo linguaggio di programmazione. Era il BASIC, oggetto della diatriba che stava occupando le cronache oltreoceano. Il giovane decise di trasformare quella passione in una professione e cominciò a studiare informatica all'università di Helsinki. Decise di specializzarsi sui sistemi operativi, rivolgendo l'attenzione verso un microkernel in licenza BSD chiamato MINIX(*14). Nei suoi esperimenti però, Torvalds si accorse quasi subito di non esserne completamente soddisfatto e cosi, just for fun, come ebbe a dire lui stesso, cominciò a sviluppare un nuovo kernel monolitico basato sulle linee di codice che aveva potuto leggere nei sorgenti di MINIX. Il suo sistema era ancora in fase di test quando, nel 1991, decise di superare quella naturale timidezza che lo affliggeva da tempo. Indirizzò così una e-mail(*15) al newsgroup comp.os.minix:

"Salve a tutti gli utilizzatori di MINIX. Sto sviluppando per hobby un sistema operativo per macchine AT-386. Il mio sistema ha qualche somiglianza con MINIX - in particolare il file system per ragioni pratiche [...] Sto attualmente lavorando per inserire sia l'interprete bash che il compilatore gcc, e quindi credo che il sistema operativo sarà pronto entro pochi mesi"

In pochissimo tempo quel sistema operativo "per hacker fatto da hacker" riscosse una certa popolarità e numerosi collaboratori si aggiunsero al progetto. Nacque git, un sistema strutturato per tenere "in bolla" gli aggiornamenti del software, e lentamente si aggiunsero nuove applicazioni fino a includere tutto il pacchetto sviluppato dalla Free Software Foundation. Cambiò la licenza d'uso in GPL - Gnu Public License -, il sistema passò da essere un semplice emulatore di terminale a un kernel vero e proprio, e cominciò a implementare il sistema Xwindow per integrare una interfaccia grafica. Tre anni dopo, dopo tanto lavoro, si era arrivati alla prima versione stabile e Linus Torvalds, in un'aula magna gremita, la presentò presso l'università di Helsinki dove era studente. Il ragazzo era cresciuto. Ed era nato Linux(*16).

Hacker lo è chi hacker lo fa

Nell'universo Open Source ci sono due figure che, più di altre, brillano come fossero i punti cardinali.

La prima è quella di Richard Stallman[(#7)], fondatore nel 1985 della Free Software Foundation[(*17)], che letteralmente ha fornito l'architettura software al sistema operativo oggi più utilizzato al mondo. Le fondamenta che stanno alla base della FSF sono semplici e quasi elementari: vi deve essere la libertà di scrivere software, di leggere come è stato realizzato e la libertà di re-distribuirlo modificato. Nella popolare licenza GPL - oggi arrivata alla terza versione - si chiarisce infatti come si possa modificare e distribuire il codice sotto forma di nuovo software ma solo e soltanto attribuendone la fonte. Questo principio è noto come copyleft e permette al programmatore di vedere il suo lavoro riconosciuto, senza però interrompere lo sviluppo del software stesso da parte di altri soggetti.

La seconda è quella di Eric S. Raymond - meglio noto come ESR, programmatore, evangelista informatico, e fondatore della open source initiative (OSI)[(*18)] - che ha contribuito a diffondere ad un pubblico di non specialisti il movimento hacker. Lo jargon file[(*19)], da lui scritto, è semplicemente diventato un pezzo di storia dell'informatica. Nel suo "The Cathedral and the Bazaar"[(#4)] Raymond descrive alcune cose fondamentali. La prima: hacker è un approccio mentale. Non si è hacker perché si sa programmare in Perl, Lisp, C o Python. Si è hacker se si riconosce che il mondo è pieno di problemi straordinari che attendono di essere risolti. La seconda: hacker è una comunità. Partendo dal presupposto che nessun hacker dovrebbe risolvere i problemi due volte, vi è l'obbligo morale di diffondere le soluzioni - ammesso che ci siano - nel miglior modo possibile. Lo scopo: rendere il mondo un posto con meno problemi irrisolti. La terza, e forse la più importante: l'attitudine ad essere hacker non è un sostituto alla competenza, motivo per cui è incoraggiato un costante e assiduo apprendimento.

In un mondo così complesso, pieno di problemi e affamato di soluzioni, il bazaar informale raffigurato graficamente dalla comunità open source, si contrapponeva alla cattedrale raffigurata dai grandi monopoli dell'informatica che agivano solo per interessi economici e non per pura e genuina curiosità. Secondo la famosa "legge di Linus"[(*20)] - denominata così in onore di Linus Torvalds -:

"dato un campione abbastanza ampio di programmatori, tutti i problemi forniti saranno analizzati rapidamente e pertanto la soluzione sarà ovvia per almeno alcuni di loro"

La cultura hacker è una cultura libertaria, quasi anarchica oserei dire che, durante il passare degli anni, ha sviluppato un approccio pragmatico ai problemi. È questo in sostanza l'open source: un modello

collaborativo, che integra al suo interno la necessità di sopravvivere in un mondo capitalista e, allo stesso tempo, di lavorare insieme per uno scopo comune. Da qui all'idea che Internet, il sistema operativo Gnu/Linux, l'open source e il free - as a beer - software(*21),fossero adatti a integrarsi nel sogno mai interrotto di avere una società migliore, il passo fu assolutamente breve.

Indymedia

La World Trade Organization (WTO) nacque nel 1995, come una sorta di seguito e "miglioramento" a quello che era il General Agreement on Tariffs and Trade (GATT). Nacque con l'intento preciso di favorire lo scambio delle merci a livello internazionale, di incentivare i commerci, di ridurre al massimo i dazi commerciali e per stimolare gli accordi multilaterali. In questo gioco complicato delle parti, dove il denaro e le merci si spostano da un posto all'altro e i grandi Paesi e/o le grandi multinazionali prendono accordi, non tutti erano trattati allo stesso modo. In particolare, i Paesi del cosiddetto Terzo Mondo erano tenuti fuori dai giochi. Una delle tante cose che fece gridare allo scandalo fu la cosiddetta "green room", un organismo interno al WTO dove soltanto alcune nazioni - le più ricche, ça va sans dire - prendevano le decisioni più importanti. Quando tutto ciò avveniva, un movimento nato dal basso, spontaneo e organizzatosi tramite internet, cominciò a riversarsi nelle strade con lo scopo preciso di rappresentare una massa critica silente che, per anni, aveva subìto le decisioni economiche e sociali delle grandi multinazionali, dei Paesi più ricchi del mondo e delle organizzazioni create a loro tutela.

Così nel novembre 1999, durante l'ultimo convegno del millennio, quel movimento manifestò lungo le strade di Seattle(*22) per protestare e impedire la realizzazione della riunione del WTO. Fu l'evento in cui ci fu la prima apparizione di quello che da allora venne riconosciuto come il "blocco nero" - i black block - cioè teppisti organizzati che vedevano la protesta come un momento per distruggere quelli che si ritenevano "i simboli del capitalismo": banche, fast food, uffici di multinazionali e non solo. La protesta e la repressione furono feroci: vennero sparati sui manifestanti proiettili di gomma, lacrimogeni e molti dei manifestanti - anche e sopratutto pacifisti - vennero malmenati. Fu il battesimo di fuoco del movimento. L'evento venne ricordato successivamente dai media come "la battaglia di Seattle".

Il G8 di Genova(*23) nel luglio 2001, gli eventi della Diaz, Bolzaneto e la morte di Carlo Giuliani furono soltanto l'escalation di quella prima e scomposta repressione.

E l'open publishing

Durante quell'enorme disastro però era avvenuto un miracolo. Un piccolo pacchetto software, distribuito attraverso internet, aveva permesso a milioni di persone di partecipare e manifestare in piazza. Il movimento alla base di tutto si chiamava Indymedia(*24) e la sua sezione australiana aveva creato il cosiddetto "active software"(*25), un blocco basato su piattaforma LAMP (Linux Apache Mysql Php) che, sulla base di un template univoco a tre colonne, permetteva di riprodurre un identico sito web in ogni parte del mondo. Questa piattaforma fu poi modificata, in seguito, dai vari "nodi" di Indymedia sparsi per il mondo - alcuni sostituirono, per esempio, il database Mysql con Postgresql - e diventò rapidamente il primo esempio di social network "decentralizzato". Nacquero così i "media center", gruppi organizzati di attivisti che mantenevano aggiornato il software diffondendo, attraverso il news feed, le notizie non rilanciate dai media tradizionali. Attraverso le chat IRC ci si coordinava e si organizzavano nuovi eventi di protesta. Nascevano web radio composte da giovani giornalisti. Nascevano esperienze come RadioGAP, coordinamenti che univano i nuovi media sotto un cappello unico. E, attraverso questa esperienza, avvenne qualcosa di ancora più affascinante: nacque l'open publishing(*26).

Fu Matthew Arnison, uno dei programmatori che avevano lavorato alla stesura del "active software", a definirlo così nel giugno 2001. I princìpi che stavano alla base di questa idea erano semplici. Come per il free software, se uno parlava di libertà delle idee, l'altro parlava della libertà di codice, ma entrambi erano una risposta alla privatizzazione delle informazioni realizzata da parte dei monopoli internazionali. Citando lo stesso Arnison:

"Il prodotto è liberamente disponibile e il processo di produzione è libero e trasparente. Se a qualcuno non piace, lo può prendere, modificare e redistribuire. L'unica cosa che non si può modificare è la sua libertà"

Quel movimento stava cambiando il mondo. E qualcuno stava cominciando ad accorgersene.

Per un pugno di MP3

C'era un tempo, tanti anni fa, che la musica si ascoltava soltanto attraverso supporti fisici. Prima i vinili, poi i minidisk, poi le audiocassette, poi i cd. Ma i supporti prendono spazio, si rovinano e non si

possono trasportare agilmente. Fino agli anni '90 si poteva (e lo si faceva) convertire una traccia audio in un file digitale ma era un processo dispendioso in termini di risorse e il file finale occupava molto spazio su disco. La storia vuole che, lavorando sulla decodifica di un brano di Suzanne Vega, un team internazionale coordinato dall'ingegnere Leonardo Chiariglione(*27), riuscisse a creare l'algoritmo di compressione mpeg. Il nuovo formato musicale mp3 - mpeg layer III - aveva un vantaggio rispetto agli altri: era estremamente compatto e nella compressione quello che rimaneva nel file finale erano soltanto le frequenze acustiche udibili dall'orecchio umano(*28). Con la disponibilità di file musicali rippati da audio cd si diffuse, in una internet ancora in fase di definizione, la pirateria audio e nacquero in poco tempo siti web che rendevano possibile il download di album interi per artisti di ogni genere. Era il periodo delle connessioni a 24/56k(*29), c'erano i forum e le newsletter, e stava emergendo lentamente quell'idea dell'internet come "territorio di nessuno". Lo scandalo della dotcom sarebbe arrivato soltanto pochi anni dopo.

In quell'innovativo humus culturale, due amici, Sean Parker e Shawn Fanning, crearono un piccolo software che avrebbe rivoluzionato l'intera industria musicale. Si chiamava Napster(*30), era un programma di file sharing P2P e aveva un funzionamento che poi, in seguito, avrebbe mostrato le sue vulnerabilità. Permetteva in sostanza agli utenti di ricercare file mp3 contenuti nelle macchine degli altri utilizzatori del network. In questo sistema, Napster fungeva soltanto da indicizzatore delle risorse, mentre i computer locali degli utenti fungevano da archivio fisico. Il sistema purtroppo aveva una falla: quando l'industria musicale cominciò ad accorgersi del danno ricevuto, bastò buttare giù il server centrale per risolvere il problema. Fu soltanto con Gnutella e sopratutto con BitTorrent, due migliorati sistemi di P2P, che il processo non poté più essere interrotto.

BitTorrent in particolare, oltre all'assenza di un nodo centrale, aveva introdotto una interessante novità: gli utenti erano diventati essi stessi nodi del network e, attraverso il sistema del "segmented file tranfer", si potevano scaricare pezzi di file da diversi nodi allo stesso tempo, accelerando così di molto la velocità totale del download. Inoltre, il protocollo utilizzava un algoritmo crittografico che rendeva virtualmente impossibile risalire a chi stava condividendo il file. Questo fu essenzialmente motivo per cui l'unica cosa che, legalmente, si riuscì a fare, fu di chiudere siti come PirateBay(*31) che indicizzavano le risorse. Ma chiuso un indice ne nasceva un altro e un altro ancora. E inoltre BitTorrent era soltanto un protocollo di scambio file, non un'azienda da poter chiudere.

Nella realizzazione di una internet libera e indipendente andava dunque aggiunto un altro tassello fondamentale: la decentralizzazione.

Il Creative Commons

Erano passati appena 30 anni dalla definizione del protocollo TCP/IP che aveva reso possibile identificare e far comunicare i computer all'interno di un network, e giusto 10 anni dalla definizione del web come luogo dove i contenuti potevano essere condivisi attraverso il protocollo HTTP (HyperText Transfer Protocol). La "information superhighway"(*32) era giusto dietro le spalle e si stava creando nuovo terreno in cui internet sarebbe stata la piattaforma del futuro. In un universo come quello cyberpunk, dove la tecnologia stava ri-definendo regole e cancellando confini geografici, serviva un'idea, qualcosa di nuovo che delimitasse cosa e come, al pari del software, fosse appropriato condividere oppure no. Mentre sulle strade scoppiava la protesta e negli zainetti degli adolescenti circolava "No Logo"(#8) di Naomi Klein, in questo nuovo universo virtuale stava per nascere un'entità che avremmo avuto difficoltà a dimenticare.

Era il gennaio 2001 e un giurista statunitense di nome Lawrence Lessing fondò l'organizzazione no profit Creative Commons(*33). L'idea che stava alla base dell'organizzazione era semplice ma ambiziosa: la ridefinizione del concetto di copyright. Era necessario creare un nuovo standard di regole in un mondo dove, virtualmente, le regole erano diventate assenti. Pochi anni dopo, nel dicembre 2002, la CC rilasciò le 6 licenze che cambiarono il corso della storia:

*Attribution // **cc by***
Questa licenza permette di utilizzare, modificare e distribuire, anche a scopo commerciale, l'opera originale a patto di citarne la fonte.

*Attribution Share Alike // **cc by-sa***
Questa licenza permette di utilizzare, modificare e distribuire, anche a scopo commerciale, l'opera originale a patto di citare la fonte. L'unica differenza con "cc by" è che il nuovo lavoro deve equipaggiarsi della stessa licenza dell'originale.

*Attribution No-Commercial // **cc by-nc***
Questa licenza permette di utilizzare, modificare e distribuire l'opera originale a patto di citarne la

fonte. L'unica differenza con "cc by" è che il nuovo lavoro non può essere utilizzato per scopi commerciali.

*Attribution No-Derivatives // **cc by-nd***
Questa licenza permette di utilizzare e distribuire, anche a scopo commerciale, l'opera originale a patto di citarne la fonte. L'unica differenza con "cc by" è che il nuovo lavoro non può presentare modifiche rispetto alla versione originale.

*Attribution No-Derivatives No-Commercial // **cc by-nc-nd***
Questa licenza permette di utilizzare e distribuire l'opera originale a patto di citarne la fonte. L'unica differenza con "cc by-nd" è che il nuovo lavoro non può essere utilizzato per scopi commerciali.

*Attribution No-Commercial Share-Alike // **cc by-nc-sa***
Questa licenza permette di utilizzare, modificare e distribuire l'opera originale a patto di citarne la fonte. L'unica differenza con "cc by-nc" è che il nuovo lavoro deve equipaggiarsi della stessa licenza dell'originale.

Queste licenze fornirono a quelli che oggi chiamiamo i "creatori di contenuti" uno strumento importante per decidere se diffondere o no, se permettere di modificare o no, se condividere o no, un lavoro di cui erano gli autori. Era apparso quel fenomeno che avremmo chiamato "web 2.0", dallo standard RDF stava per nascere il suo figlio illegittimo RSS(*34) e stava letteralmente per esplodere la condivisione dei contenuti. E, dalla storia, arrivò un altro piccolo regalo. Nel gennaio 2001, praticamente in contemporanea alla nascita della Creative Commons, un imprenditore statunitense di nome Jimmy Wales ideò una piattaforma aperta editabile dai suoi iscritti per creare una "sorta" di enciclopedia on-line. Si sta parlando ovviamente di Wikipedia(*35) e, già dalle prime release, cominciò ad utilizzare, al suo interno, una piattaforma open source chiamata MediaWiki. Wikipedia è attualmente editata in 313 lingue, ha più di 55 milioni di voci pubblicate, ed è letteralmente uno dei siti più popolari del mondo.

Passeranno pochi mesi e, nel numero #36 di Amazing Spiderman(*36), l'amichevole ragno di quartiere si staglierà fra le rovine dei grattacieli di New York mentre Doctor Doom, nella nona tavola, verserà le sue lacrime sulle vittime degli attentati. Nei testi di Straczynski e nei disegni di John Romita jr. si

rappresenterà visivamente tutta l'angoscia di chi avrebbe potuto fare e non aveva fatto, di chi avrebbe potuto vedere e non aveva visto. Una tragedia che avrebbe ridefinito il mondo. Era arrivato l'11 settembre 2001(*37).

Riferimenti

(*1) https://www.engadget.com/2020-03-04-seti-home-stops-for-now.html

(*2) https://www.wsj.com/news/articles/SB114221407089396217

(*3) https://www.screamingfrog.co.uk/adwords-history/

(*4) https://web.archive.org/web/20090216175708/http://browser.netscape.com/history

(*5) https://arxiv.org/abs/cs/0105018

(*6) https://web.archive.org/web/20120323162213/http://startup.nmnaturalhistory.org/gallery/notesViewer.php?ii=76_2&p=3

(*7) https://www.101computing.net/from-transistors-to-micro-processors/

(*8) https://learn.canvas.net/courses/4/pages/history-of-free-and-open source-software

(*9) http://altairbasic.org/

(*10) https://news.microsoft.com/2000/05/09/microsoft-fast-facts-1975/

(*11) https://apple2history.org/history/ah04/

(*12) http://www.ams.org/notices/200604/fea-davis.pdf

(*13) http://www.computinghistory.org.uk/det/2535/Commodore-VIC-20/

(*14) https://www.cs.vu.nl/~ast/reliable-os/

(*15) https://www.cs.cmu.edu/~awb/linux.history.html

(*16) https://www.linuxfoundation.org/

(*17) https://www.fsf.org/

(*18) https://open source.org/

(*19) http://www.catb.org/jargon/html/

(*20) https://arxiv.org/abs/1608.03445

(*21) https://www.gnu.org/philosophy/free-sw.en.html

(*22) https://www.democracynow.org/1999/12/2/the_battle_in_seattle_hundreds_arrested

(*23) https://www.amnesty.org/en/latest/news/2010/03/convictions-abuse-during-genoa-g8-protests-upheld/

(*24) https://journals.sagepub.com/doi/full/10.1177/0163443720926039

(*25) http://purplebark.net/maffew/cat/imc-rave.html

(*26) https://wiki.p2pfoundation.net/Open_Publishing

(*27) https://www.scientificamerican.com/article/digital-revolutionary-int/

(*28)
https://www.researchgate.net/publication/323969962_Compression_history_detection_for_MP3_audio

(*29) http://www.windytan.com/2012/11/the-sound-of-dialup-pictured.html

(*30) https://www.jstor.org/stable/1600355?seq=1

(*31) https://torrentfreak.com/the-piratebay-is-down-raided-by-the-swedish-police/

(*32) http://www.netvalley.com/cgi-bin/intval/net_history.pl

(*33) https://creativecommons.org/2005/10/12/ccinreviewlawrencelessigonhowitallbegan/

(*34) http://www.aaronsw.com/weblog/000574

(*35) https://history-computer.com/wikipedia-history-of-wikipedia-by-jimmy-wales-larry-sanger/

(*36) https://imgur.com/gallery/83xZp

(*37) https://www.theguardian.com/world/2001/sep/12/september11-usa

Capitolo 2 - E ho trovato l'invasore

La mia capretta

"Il capo del gabinetto della Casa Bianca entrò nell'aula e disse a Bush 'la nazione è stata attaccata'. Non sapendo cosa fare, non essendoci nessuno che gli suggerisse cosa fare, e visto che gli uomini dei servizi segreti non lo stavano prelevando di peso per trasferirlo in un luogo sicuro, Bush non si scompose, e continuò a leggere 'la mia capretta' insieme ai bambini"

Così Michael Moore, regista del film "Fahrenheit 9/11", descrive la reazione(*1) dell'allora presidente degli Stati Uniti George W. Bush nel momento in cui, quell'11 settembre del 2001, ricevette la notizia dell'attacco alle Torri Gemelle. Per ironia della storia, i 19 attentatori appartenevano ad un movimento fondamentalista islamico conosciuto col nome di Al Quaeda(*2) che, nel 1988, era stato finanziato direttamente dal governo degli Stati Uniti per contrastare l'invasione sovietica in Afghanistan. In una intervista rilasciata al National Geographic(*3) 10 anni dopo, Bush dichiarò di non aver immediatamente lasciato la scuola per evitare reazioni di panico nei bambini e per mostrare che la nazione rimaneva forte anche in situazione di pericolo. Criticabile, giusto, ma noi al suo posto cosa avremmo fatto? Come avremmo reagito in una situazione simile?

Se la risposta rimane aperta per molti cittadini rimasti esterrefatti dagli errori compiuti in quel tragico giorno, di certo non rimane aperta quella che diedero i servizi segreti statunitensi all'indomani dell'11/9. Grazie all'introduzione di una nuova legge federale denominata Patriot Act(*4), CIA ed FBI ebbero l'autorizzazione ad intensificare i controlli di massa allo scopo di prevenire un nuovo attacco terroristico. Questa legge infatti espandeva i poteri in mano al governo degli Stati Uniti per intercettare chiamate nazionali e internazionali, traffico e comunicazioni tramite internet ed aumentare le pene verso i soggetti sospettati di collusioni col terrorismo. Le norme diventarono così assurde e restrittive

che i controlli si estesero a tappeto. Uno degli esempi più celebri avvenne nei confronti del Linux Journal(*5), rivista popolare fra gli appassionati di informatica. Si scoprì che la National Security Agency infatti, secondo un leak pubblicato da Tagesschau - giornale online tedesco - tracciava tutti i suoi lettori poiché la rivista era identificata come una sorta di "forum estremista". La sua colpa? Aver trattato in un articolo la tecnologia Tor - ne parleremo dopo - e Tails, una distribuzione linux anonima e, appunto, basata su Tor.

Di contro Osama Bin Laden, nell'immenso deserto afgano, scappava a bordo di una motocicletta(*6) insieme al suo compagno d'armi il mullah Omar. E l'esercito statunitense, impotente nell'affrontare una così avanzata tecnologia a due ruote, invece di tagliare le radici di Al Quaeda, si dirigeva verso l'Iraq(*7) dove lo aspettava il presidente iracheno Saddam Hussein, un tempo finanziato dagli stessi Stati Uniti, ora accusato di possedere armi di distruzione di massa. Lui, non l'esercito USA. Ma nella smania di estirpare alla base la minaccia terroristica, per l'intelligence statunitense il dark web, evidentemente, faceva più paura dei due leader di Al Quaeda. Nota dell'autore: si capisce l'ironia o la devo anche spiegare?

Si stava meglio quando si stava peggio

"Vieni nel mio salotto, disse la macchina allo specialista"

Questo è il modo con cui Marshall McLuhan descrive, nel celeberrimo libro "The Medium is the Massage"(#9), lo stato che avrebbe assunto la tecnologia nei confronti dell'essere umano. Uno stato non di subalternità dunque ma di superiorità che, successivamente, il potere politico avrebbe cercato di controllare. C'è un evento in particolare che descrive come le compagnie high-tech del nuovo boom della Silicon Valley si siano piegate al potere politico. Era il febbraio del 2000 e Marc Knobel, un francese di origine ebrea, si imbatteva in un sito web sotto il dominio di Yahoo.com nel quale l'azienda statunitense concedeva spazio per vendere memorabilia(*8) del periodo nazista. Secondo la legge francese vendere un qualsiasi oggetto che richiamasse l'ideologia nazista era semplicemente illegale. Ma il sito era ospitato negli Stati Uniti dove la stessa regola non si applicava. Cosa fare dunque? Marc Knobel decise di denunciare Yahoo per aver permesso di diffondere propaganda nazista in territorio francese. La questione era certamente molto delicata perché non coinvolgeva soltanto legislazioni differenti in territori differenti ma riguardava sopratutto il principio della libertà di espressione che, per l'internet di allora, era qualcosa di prezioso da tutelare. Jerry Yang, il co-founder di Yahoo, dopo esser

stato condannato a filtrare i contenuti del suddetto sito, pronunciò una dichiarazione di guerra che, nei fatti, sarebbe stato costretto a ritirare:

"noi non modificheremo il contenuto dei siti negli Stati Uniti soltanto perché una corte francese ci chiede di farlo"(#12)

Arriviamo al 2005. Sulla scena era apparsa Google, Yahoo aveva cominciato a perdere quote di mercato e cominciava a guardare alla Cina come un luogo dove potersi espandere. Come noto, la Cina è lontana dall'essere una democrazia compiuta e per entrare nel suo mercato Yahoo siglò un patto col diavolo: il governo cinese avrebbe permesso al gigante della dotcom di entrare nel suo territorio solo a patto di poter ispezionare, a richiesta, la navigazione di tutti gli utenti. Fu così che il giornalista cinese Shi Tao(*9), nel tentativo di diffondere un meeting per commemorare la tragedia di Piazza Tienanmen, commise l'errore di utilizzare la sua email sotto il dominio Yahoo. Il giornalista venne trovato, indagato, processato e incarcerato per 10 anni. La coerenza, purtroppo, conserva sempre un senso del ridicolo.

Ajax. E il Web 2.0

Si era in un momento di transizione: la programmazione web stava evolvendo a tal punto che le pagine da statiche cominciano a diventare dinamiche. Con la nascita della tecnologia Ajax(*10) - acronimo che sta per "asynchronous javaScript and xml" - le pagine web stavano diventando non solo luoghi dove inserire contenuti, ma anche luoghi dove inserire applicazioni intere. Integrati in una pagina web cominciammo a vedere editor di testo, presentazioni, fogli di calcolo, chat online e così via. Era la rivoluzione del cosiddetto "web 2.0". Internet non era più un luogo da vivere passivamente, ma - grazie alle aumentate velocità di connessione e le nuove web-app - un luogo dove si poteva partecipare ed essere protagonisti.

Molti libri hanno esplorato questa transizione: in "Wikinomics"(#10) di Don Tapscott, per esempio, si descrive la nuova figura del "prosumer", utente capace di fruire di contenuti e contemporaneamente fornire contenuti. Col nuovo web semantico(*11) si poteva interagire con internet in un modo creativo, senza dover necessariamente avere conoscenze di programmazione: bastava un browser, una gui e una interfaccia web. Internet era diventato di tutti e per tutti.

Bloggo ergo sum

Una delle manifestazioni più evidenti di questa voglia di comunicare furono i blog, contrazione di web-log(*12), ovvero diari personali online che venivano utilizzati nei modi più disparati. C'era chi li utilizzava semplicemente per comunicare i propri pensieri, poesie, scritti personali, altri che cominciavano già ad usarli come sistema per fare un primo ed amatoriale giornalismo online. Fra le piattaforme, Livejournal forniva una interfaccia piuttosto intuitiva e presentava al suo interno, oltre che ad un editor di testo, anche la possibilità per gli utenti più smaliziati di scrivere direttamente in html. Piattaforme come Wordpress invece permettevano l'integrazione di vari plugin esterni che interagivano con altri servizi sociali, mentre Blogger, una volta acquisita da Google, si integrò con tutta la suite fornita dall'azienda di Mountain View. Di certo però, in questo caotico esperimento, cominciò a generarsi molto rumore online, tanto che, a un certo punto, diventò addirittura difficile distinguere i dati dalle opinioni. Si arriverà a dire addirittura che "uno vale uno"(*13), come se internet fosse avulso dalla necessità di avere competenze.

Molto interessante è il parere sviluppato da Andrew Keen nel suo libro "The Cult of the Amateur: How Today's Internet Is Killing Our Culture"(#11). Keen sostiene infatti che l'abitudine a condividere senza controllare, il cut & paste da Wikipedia, il crosslink, non genera talenti ma genera il culto della personalità senza controbilanciare il culto della competenza. Narcisismo 2.0 insomma. Analogo pensiero fu sviluppato un anno dopo da Nicholas Carr, autore di molti libri, ma famoso sopratutto per il suo articolo sul giornale The Atlantic intitolato "Is Google making us stupid?"(*14) in cui si sosteneva la pericolosità che un uso continuato di Internet avrebbe, a dir suo, ridotto la capacità di attenzione e di approfondimento. Senza dubbio c'era del vero in entrambe le analisi, ma oltre a questo c'era anche dell'altro: stava cominciando il profiling, ovvero quel sistema con cui i dati degli utenti venivano prima incamerati e poi gestiti dalle varie piattaforme sul web. Oro digitale insomma che, nelle mani sbagliate, avrebbe potuto ostacolare lo sviluppo della democrazia.

La privacy. Qualche anno fa.

Era il 1995 e io, in una notte di settembre, mi connettevo ad uno dei primi "bulletin board system". Le cosiddette BBS erano computer connessi in rete(*15) che permettevano alcuni embrionali servizi come l'email, l'ftp per lo scambio di file e sopratutto, il sistema irc che consentiva di chattare online con persone di tutto il mondo. Ci si connetteva attraverso telnet, si navigava da terminale attraverso gopher e il mondo sembrava finalmente bello e pieno di risorse. A quei tempi a me sembrava davvero

fantascienza. Eppure non era una tecnologia particolarmente nuova. Era fin dagli anni '80 che circolavano server di quel genere e io ero uno degli ultimi utenti a scoprire l'esistenza di quelle meraviglie. Mi sentivo in forte imbarazzo e quando entrai in chat per la prima volta mi presentai sperando di poter comunicare con qualcuno. Quando però scrissi:

"Salve a tutti, mi chiamo Fabio, abito a Lecce e sono appassionato di astronomia"

l'amministratore della chat mi redarguì rispondendo:

"Benvenuto. Non fornire le tue generalità in chat, è contro la policy del canale. Potresti essere bannato per questo"

Policy? Bannare? Di cosa stava parlando l'amministratore? Stava parlando banalmente di privacy o meglio ancora del minimo sindacale di privacy che si dovrebbe avere quando si accede a servizi online e si comunica con persone che non si conoscono. Imparai soltanto dopo che l'anonimato in rete, a quei tempi, era qualcosa di assolutamente fondamentale, tanto che si comunicava fornendo soltanto nickname e non nomi di battesimo. Come avrebbe poi scritto Kevin Mitnik, uno dei più famosi hacker al mondo, in "The Art of Invisibility"[(#13)] per andare online bisogna seguire sempre 3 importanti e basilari regole:

- Rimuovere il proprio indirizzo IP originale
- Oscurare hardware e software utilizzati durante la navigazione
- Difendere il proprio anonimato durante le comunicazioni

Qualche anno dopo il prof. Luciano Floridi, professore di filosofia ed etica presso l'università di Oxford, analizzò questa costante migrazione della vita dal offline/online al nuovo concetto del "onlife", un termine coniato[(*16)] per descrivere come siano cambiati i comportamenti umani dopo l'arrivo di internet disponibile 24 ore su 24 e di come la nostra privacy si sia radicalmente ridotta. Questo apre radicalmente nuovi scenari, centrati in particolar modo su una società costruita per macchine e non per esseri umani. Ma ci arriveremo dopo, un passo alla volta.

Il Guerrilla Manifesto

Aaron Swartz(*17) è una delle figure più importanti e purtroppo meno conosciute dei nostri tempi. Morto suicida a 26 anni(*18), era uno degli sviluppatori più brillanti della sua epoca. Forte sostenitore della necessità che le informazioni fruissero liberamente e senza limiti all'interno di internet, partecipò e contribuì fortemente allo sviluppo dello standard RSS che permise al web di essere esteso e condiviso come lo possiamo vedere oggi. Fondò il sito watchdog.net per aggregare i dati e le proposte dei politici statunitensi e si impegnò nella campagna contro la "online piracy act"(*). Convinto della necessità che i dati scientifici posseduti dai giornali accademici dovessero essere distribuiti in rete per la loro fruizione gratuita, trafugò, utilizzando la rete del MIT(*20), più di 300 lavori dalla biblioteca chiusa Jstor(*19), con il chiaro intento di distribuirli in rete.

Nota(*): nell'ottobre del 2011 il deputato repubblicano Lamar Smith presentò, presso la camera dei deputati statunitense, una proposta di legge che avrebbe permesso di procedere legalmente contro la ricondivisione dei contenuti coperti da copyright. Questo, in sostanza, avrebbe obbligato agli internet service provider ad oscurare i siti incriminati operando sul filtraggio dei dns.

Per farlo utilizzò uno script che scaricava in automatico i paper dentro un hard disk esterno collegato ad un laptop. Nottetempo, appena riempito l'hard disk, tornava nel dipartimento per cambiarlo, fare un backup e ricominciare il lavoro. Arrestato nel 2011(*21), passò gli ultimi due anni della sua vita a difendersi dalle accuse della Corte federale, la quale dichiarò pubblicamente il rischio a cui Swartz stava per andare incontro: 30 anni di prigione senza condizionale. Si spesero per lui personaggi come Lawrence Lessing, il fondatore della Creative Commons, Tim Berners Lee, il fondatore del consorzio W3C, e una intera comunità di utenti che riconosceva in lui una figura importante sopratutto per le battaglie che, sulla sua pelle, aveva portato avanti. Uno dei suoi post più importanti - presente ancora oggi online - è senza dubbio il "guerrilla open access manifesto"(*22). Scritto nel 2008 durante una breve permanenza in Italia, recita:

"L'informazione è potere. Ma come ogni tipo di potere, ci sono quelli che se ne vogliono impadronire. L'intero patrimonio scientifico e culturale, pubblicato nel corso dei secoli in libri e riviste, è sempre più digitalizzato e tenuto sotto chiave da una manciata di società private [...] Non c'è giustizia nel rispettare leggi ingiuste. [...] Dobbiamo acquisire le informazioni, ovunque siano archiviate, farne copie e condividerle con il mondo. Dobbiamo prendere ciò che è fuori dal diritto d'autore e caricarlo

sul web. Dobbiamo acquistare banche dati segrete e metterle sul web. Dobbiamo scaricare riviste scientifiche e caricarle sul web. Dobbiamo lottare per un guerrilla open access"

Una metafora: il gioco della vita

Quando parliamo di scienza parliamo di modelli di rappresentazione del mondo. E quando parliamo di modelli di rappresentazione del mondo parliamo di strumenti matematici. Il motivo per cui oggi abbiamo la possibilità di scrivere, lavorare e interagire coi computer, ci arriva grazie ad una idea di un matematico inglese che, nel tentativo di risolvere il entscheidungsproblem(*23) - il problema della decisione - di David Hilbert, si diresse verso la teorizzazione di un processo risolutore che fosse universale. Questa, chiamata "teoria della computabilità", venne sviluppata Alan Turing nel tentativo di creare un modello di calcolo per le funzioni ricorsive. Da qui nacque l'idea della cosiddetta "macchina di Turing"(*24), antesignana dei personal computer che oggi abbiamo sulle nostre scrivanie.

Una cosa che ci ha insegnato la scienza - da Newton in poi - è il principio di *azione e reazione*. Così come il raggiungimento della massa limite in una stella genera la formazione di un buco nero, così anche in informatica una differenza di condizioni iniziali genera una differenza di condizioni finali. Anche la vita in fondo è un algoritmo, di certo più complesso a causa degli innumerevoli parametri in gioco, ma pur sempre un algoritmo. Nel tentativo di rappresentare l'evoluzione temporale di un sistema, il matematico John Conway inventò un gioco del tutto particolare che chiamò "il gioco della vita"(*25). Richiedendo pochissime regole - e zero giocatori - questa semplicissima macchina di Turing poteva rappresentare l'evoluzione di un intero sistema complesso a patto di fornire un semplice stato iniziale. Il gioco si sviluppa in due assi cartesiani, dove la configurazione iniziale è banalmente un grumo di punti collegati fra loro, e la sua evoluzione invece avviene dall'alto verso il basso, lungo una matrice virtualmente infinita.

Se per pura ipotesi potessimo sostituire alle condizioni iniziali quelle fornite dall'open source, dal creative commons e dall'open access, e se per pura ipotesi potessimo sostituire alla matrice di punti il sistema nel quale esse si sono evolute, capiremmo perché sia tanto importante fornire i parametri giusti al momento giusto. Ecco il motivo per cui figure come Raymond, Stallman, Torvalds, Lessing, Lee e Swartz sono state cosi importanti per fornire e ispirare una direzione.

Più data che meta

Piccolo aneddoto personale: mio padre, all'inizio della carriera, aveva cominciato a lavorare su macchine a controllo numerico. Una delle prime innovazioni di cui si occupò fu un sistema che permetteva di identificare i veicoli in autostrada attraverso un sistema a radio frequenza, creando successivamente un report che riportasse quanti chilometri avevano percorso da casello a casello. Era una sorta di identificativo che serviva a quella neonata tecnologia per mettere un "timbro virtuale" a ogni veicolo. Si chiamava "telepass"(*26), ed ogni italiano che abbia transitato in autostrada ci ha avuto a che fare prima o poi. Se ci pensiamo non è tanto diverso da quello che succede col codice a barre, che identifica ogni informazione relativa a un prodotto. Oppure agli exif all'interno di una immagine digitale, che permettono di risalire alla camera che ha effettuato la foto, la risoluzione e, spesso, anche alla sua geolocalizzazione. In sostanza, dove esiste una macchina, un computer o un elaboratore, esistono dati scritti da qualche parte e quei dati, utilizzati in modo sapiente, permettono di effettuare analisi e previsioni per migliorare o implementare nuovi servizi.

I metadati dunque altro non sono che questo: una serie di elementi utili per classificare le informazioni di un prodotto all'interno di un archivio dati. Chiarito ciò, non sorprende che - in un mondo in cui i computer passavano da schede perforate a circuiti integrati - una delle prime a preoccuparsi di categorizzare i dati in maniera coerente sia stata la CIA - Central Intelligence Agency - la quale nel 1977 comprò, dalla neonata azienda Software Development Laboratories, un database che fece storia(*27): l'Oracle-DB. Adesso fate un salto di 30 anni e arrivate alla internet di oggi. Vi stupirebbe sapere che i dati della vostra navigazione siano inseriti in qualche database? E vi stupirebbe davvero sapere che, durante la vostra navigazione, viene registrato il vostro IP, il posto da dove navigate, le vostre preferenze, quali siti visitate più spesso e con quali persone parlate? Benvenuti dunque nell'era dei cookies, dei metadati e del loro figlio illegittimo, il dataismo.

Se una chiave non basta

Immaginate di essere davanti alla vostra porta di casa e di doverla aprire. Cosa fate? Normalmente le azioni che eseguite in successione sono: estraete il portachiavi dal vostro taschino, selezionate la chiave di casa, ed aprite la porta. Immaginate ora di essere davanti alla porta di casa di un vostro amico. Per aprire la porta vi si presentano ora due alternative. La prima: il vostro amico è con voi, prende la sua chiave di casa ed apre la porta. La seconda: il vostro amico vi ha fatto una copia della sua chiave e vi ha dato l'autorizzazione per entrare. In informatica non è molto diverso. Uno dei metodi più noti per

connettersi via console ad un computer di cui non siete i possessori, è attraverso il protocollo SSH(*28). È, diciamo così, uno standard che permette, attraverso l'immissione di un IP, della porta attraverso la quale comunica il protocollo e di una password, di connettersi ad una macchina remota. C'è però un piccolo problema: noi non siamo in possesso della chiave originale. Come si è ovviato a questa mancanza?

Facciamo un passo indietro. Siamo alla fase iniziale del processo, abbiamo appena installato il nostro server e stiamo configurando SSH. Dopo l'installazione del pacchetto base, dobbiamo eseguire un'altra operazione importante per il suo funzionamento. Essa è la *generazione delle chiavi*. Si, ho parlato al plurale e non al singolare perché il processo genererà una coppia di chiavi e non una singola. Una *privata*, in possesso del proprietario del server, ed una *pubblica* che sarà letteralmente un pezzo generato a partire dalla vostra chiave privata. Per permettere a qualunque vostro amico di accedere alla vostra macchina, a questo punto voi avrete bisogno di condividere con lui non la vostra chiave privata, che rimane soltanto nel vostro portachiavi, ma la vostra chiave pubblica che sarà quel pezzo di fiducia di cui ha lui ha bisogno per accedere nel vostro territorio. Questo principio in informatica viene detto "crittografia asimmetrica", e tendenzialmente funziona allo stesso modo per vari sistemi. Uno di quelli che val la pena menzionare qui è, per esempio, il gnu privacy guard, meglio noto come GPG(*29). Questo è un sistema per poter criptare un pacchetto dati, e per renderlo interpretabile soltanto da chi sia in possesso della vostra chiave pubblica.

Tutta questa sicurezza fornita dai sistemi crittografici è effettiva grazie al fatto che noi e soltanto noi siamo in possesso delle chiavi originali. Se però qualcuno è *in possesso della matrice delle chiavi originali, potrà sempre generare una chiave pubblica* ed accedere al nostro sistema anche in assenza di nostra autorizzazione.

Questo è un concetto importante poiché tutte le volte che sentiamo parlare di cose come *crittografia end-to-end*, cioè di messaggi leggibili soltanto da mittente e destinatario, tutto perde senso se la chiave originale non è in possesso del creatore della chiave pubblica. Se, per esempio, si utilizzano sistemi esterni che non risiedono a casa nostra, ci dovremo essenzialmente fidare di chi fornisce quel servizio. Nel mondo hacker si ripete spesso che la paranoia sia una virtù(*30). E voi, le dareste le vostre chiavi di casa a qualcuno che ha già dimostrato di non essere affidabile?

Nuvole in cielo e in terra

Ho sempre amato la posta elettronica. Nasceva come un sistema decentralizzato, era assolutamente immediato da utilizzare e permetteva un tipo di comunicazione lunga, pensata e senza la brevità tipica dei sistemi di messaggistica. E quando nel 2004 ricevetti l'invito per partecipare alla prima beta di Gmail(*31) ricordo che ne fui letteralmente entusiasta.

Migliorava alla base un servizio che purtroppo, con l'aumento degli utenti connessi ad internet e l'incremento esponenziale dello spam, era fortemente peggiorato. Forniva inoltre, al suo interno, un primo e rudimentale sistema di chat attraverso il protocollo XMPP che rispettava tutti gli open standard del web. Paul Buchheit, il suo creatore, fece partire il servizio come un progetto pilota che provvedesse a gestire le comunicazioni interne dell'azienda. Pochi anni dopo, Google decise di rilasciare una beta pubblica, e fu immediatamente un successo straordinario. In termini informatici, Gmail, e tutta la piattaforma delle Google-Apps - Drive, Docs, Hangouts, Calendar... - si definisce come Saas, ovvero Software As A Service. Una intera piattaforma sotto il cappello di Google che permetteva, tramite un semplice browser, di avere un centro di controllo unico da cui far partire tutte le varie applicazioni. È il famoso cloud di cui sentiamo parlare ogni giorno: ci semplifica la vita, rende i nostri dati accessibili da ogni parte del mondo, permette alle aziende di ridurre drasticamente i costi.

Ma la centralizzazione ha un costo in termini di sicurezza informatica ed indipendenza dei dati. Lo stesso Buchheit nel 2006, una volta lasciata Google, ebbe a dichiarare(*32)

"Son molto scettico per quanto riguarda la produzione di sistemi centralizzati, o di sistemi che, per esempio, provvedano a fornire un ecosistema unico e universale per tutti. Penso invece che la risposta debba venire dalla comunità"

Google ovviamente non è l'unico. Amazon per esempio ha un ruolo fondamentale nel mercato del cloud. Col suo Aws - Amazon Web Services - fornisce una piattaforma ideata per la creazione e la gestione di numerose macchine virtuali, database, storage, load balancer e non solo. È quello che per gli amministratori di sistema funziona come una Iaas - Interface as a service - e per gli sviluppatori come Paas - Platform as a service. È importante però chiarire una cosa: cloud non è soltanto sinonimo di Google, Amazon, o Apple. Il cloud può - e dovrebbe sempre essere - un private cloud, ovvero un sistema costruito internamente, magari attraverso un software open source, che permetta di avere un

sistema dove io e solo io sono il padrone dei miei dati. Esistono alternative software come nextcloud per gestire un cloud interno, openstack per gestire le macchine virtuali, oppure come docker e kubernetes per i containers. Tutto open source ovviamente. Ma ci torneremo nell'ultimo capitolo.

Internet fatto a strati

Era il 1967 e Leonard Kleinrock, allora dottorando presso il Massachusset Institute of Technology, capì che la formulazione matematica con cui i dati potevano fluire da una macchina all'altra non era adeguata a trasferire pacchetti in maniera discreta. Ne sviluppò un'altra(*33) che riuscisse a superare, a livello teorico, quell'impasse. Fu così, quasi per caso, che si gettarono le basi per quella struttura che sotto il dipartimento militare statunitense divenne ARPAnet e che, una volta demilitarizzata nel 1989, produsse la internet che conosciamo oggi. Nella sua prima formulazione, quella rete non includeva una indicizzazione. Essendo una rete sperimentale, in cui i pacchetti scambiati erano pochi e viaggiavano molto spesso in maniera lineare da un computer all'altro, strutture come i motori di ricerca non erano né previste né richieste.

Quando Tim Berners Lee diede vita al Word Wide Web(*34), si cominciarono però a distinguere alcuni livelli. Il primo, quello più evidente, era il "*surface web*", quello che si poteva navigare in superficie, quello con cui potevamo interagire a un livello base. C'era però una parte più ingente che non veniva indicizzata dai motori di ricerca e che includeva le nostre email, le chat private, i nostri scambi dati, i nostri accessi con user e password, i nostri profili sui social e via discorrendo. Questa venne definita "*deep web*", ovvero quel web inaccessibile ai motori di ricerca che generava però la maggior parte di tutto il traffico.

Era un po' come avere un enorme iceberg. La parte esterna più ridotta, che potevano vedere tutti in superficie, corrispondeva al "surface web", mentre la parte più ingente, quella sotto il livello dell'acqua e nascosta alla nostra vista, corrispondeva al "deep web". Due strati e due facce della stessa medaglia. Da qui, qualche tempo dopo, ne nascerà una terza. Una talmente nascosta che verrà definita oscura: il cosidetto "*dark web*". E il sistema Tor, in questo terzo universo parallelo, la farà da padrone.

Riferimenti

(*1) https://www.washingtonpost.com/entertainment/books/bushs-911-school-visit-pushed-pet-goat-into-spotlight/2011/09/08/gIQAYpXtFK_story.html

(*2) https://www.history.com/topics/21st-century/al-qaeda
(*3) https://www.npr.org/sections/thetwo-way/2011/07/29/138814060/in-interview-president-bush-explains-his-initial-sept-11-reaction?t=1615549442537
(*4) https://www.aclu.org/issues/national-security/privacy-and-surveillance/surveillance-under-patriot-act
(*5) https://www.linuxjournal.com/content/nsa-linux-journal-extremist-forum-and-its-readers-get-flagged-extra-surveillance
(*6) https://www.theguardian.com/world/2002/jan/06/afghanistan.rorycarroll
(*7) https://www.e-ir.info/2013/06/06/iraq-invasion-a-just-war-or-just-a-war/
(*8) https://www.nytimes.com/2000/04/12/technology/antiracism-group-sues-yahoo-for-hosting-auctions-of-nazirelated.html
(*9) https://www.nytimes.com/2005/09/08/business/worldbusiness/yahoo-helped-chinese-to-prosecute-journalist.html
(*10) https://techtracer.com/2007/03/12/the-birth-of-ajax-an-amazing-story/
(*11) https://www.w3.org/RDF/Metalog/docs/sw-easy
(*12) https://blog.hubspot.com/marketing/history-of-blogging
(*13) https://link.springer.com/article/10.1007/s12290-016-0412-8
(*14) https://www.theatlantic.com/magazine/archive/2008/07/is-google-making-us-stupid/306868/
(*15) https://www.theatlantic.com/technology/archive/2016/11/the-lost-civilization-of-dial-up-bulletin-board-systems/506465/
(*16) https://library.oapen.org/handle/20.500.12657/28025
(*17) https://www.internethalloffame.org/inductees/aaron-swartz
(*18) https://www.rollingstone.com/culture/culture-news/the-brilliant-life-and-tragic-death-of-aaron-swartz-177191/
(*19) https://docs.jstor.org/summary.html
(*20) https://news.mit.edu/2013/mit-releases-swartz-report-0730
(*21) https://www.theatlantic.com/national/archive/2013/12/mit-undercover-video-caught-aaron-swartz-act/355793/
(*22) https://gist.githubusercontent.com/ksinkar/4552726/raw/74458d1932510e2b93d8ebde9ac387f842afbc0f/Aaron%2520Swartz:%2520Guerilla%2520Open%2520Access%2520Manifesto
(*23) https://www.cambridge.org/core/journals/journal-of-symbolic-logic/article/abs/note-on-the-

entscheidungsproblem/9461BEAD94BB16D56EC78933D7D67DEF
(*24) https://www.cl.cam.ac.uk/projects/raspberrypi/tutorials/turing-machine/one.html
(*25) https://web.stanford.edu/class/sts145/Library/life.pdf
(*26) https://worddisk.com/wiki/Electronic_toll_collection/
(*27) https://paleofuture.gizmodo.com/larry-ellisons-oracle-started-as-a-cia-project-1636592238
(*28) https://www.openssh.com/history.html
(*29) https://gnupg.org/download/release_notes.html
(*30) https://theconversation.com/internet-of-things-between-panacea-and-paranoia-80286
(*31) https://time.com/43263/gmail-10th-anniversary/
(*32) http://paulbuchheit.blogspot.com/2010/10/serendipity-finds-you.html
(*33) https://theconversation.com/how-the-internet-was-born-a-stuttered-hello-67903
(*34) https://www.dw.com/en/hyperlink-when-tim-berners-lee-invented-the-world-wide-web-not-the-internet/a-19448729

Capitolo 3 - Partigiano portami via

Lyle e le sue biciclette

Nel 2037 Lyle vive nei sobborghi di Chattanooga, una piccola città degli Stati Uniti. In un futuro distopico pieno di intelligenze artificiali, corpi modificati artificialmente e droghe sintetiche, Lyle decide di rimanere ai confini della città. Vivendo in modo anarchico e utilizzando ormoni inibitori per placare la sua libido, campa di espedienti. Ripara biciclette e affitta un piccolo bilocale nel grattacielo diroccato proprio sopra al suo laboratorio. Un giorno però la sua quiete viene interrotta dalla visita di una ragazza, Kitty Casadey, che si rivelerà essere un inviato del NAFTA, l'organizzazione che serbava in sé un tremendo segreto. A quel punto Lyle dovrà scegliere: scoprire "quanto fosse profonda la tana del bianconiglio"(*1), oppure tornare alla sua vita di sempre.

Questo piccolo racconto, presente nell'antologia "A good old fashioned future"(#14) di Bruce Sterling presenta il bivio in cui a volte ci troviamo nella nostra vita. Rispetto al dark web per me fu lo stesso: mi dissero che era meglio tenersi alla larga. Ma perché?

Cipolle e Dark-web (1)

Il terzo livello della rete è più un concetto che una tecnologia. È, in parole semplici, quella minuscola parte del deep web che ha bisogno di un software specifico per essere visitata. Una rete nella rete, anonima, sicura, che si presenta come un terreno fertile dove far crescere quella originale idea di "anarchia cyberpunk" propria delle origini di internet. Il primo tentativo di crearne una, completa e funzionante, avvenne nel 1999, prima addirittura degli attacchi dell'11 settembre. Quella tecnologia, attiva e in sviluppo ancora oggi, fu denominata Freenet e venne ideata grazie ad un lavoro dell'allora studente di informatica Ian Clarke presso l'università di Edimburgo. Clarke scriveva:(*2)

"È curioso notare come molte invenzioni realizzate dall'essere umano seguano uno schema alieno allo sviluppo dei processi biologici. Nonostante l'evoluzione abbia mostrato come i sistemi decentralizzati siano gli unici con un evidente vantaggio evolutivo, i sistemi creati dall'uomo tendono invece verso architetture fortemente centralizzate"

Freenet(*3) è una rete P2P strutturalmente anonima, in cui sono gli utenti stessi a fare da nodi della rete. Questa è una caratteristica non di poca importanza, poiché rende la rete completamente decentralizzata e non dipendente da nessun nodo specifico. Inoltre, al suo interno le comunicazioni e le connessioni - sia in tcp che in udp - sono completamente criptate di modo che dall'esterno nessuno possa intercettare uno scambio di qualsivoglia pacchetto fra due utenti. Queste caratteristiche la rendono sicura e solida, anche se, nel corso del tempo, sono state riscontrate alcune piccole vulnerabilità dovute al motore java sul quale gira tutta la piattaforma. Un tentativo di migliorare Freenet fu fatto nel 2003 con la creazione di I2P(*4), una dark net molto simile, con molti più livelli di sicurezza ma con molte meno funzionalità.

Nel 2003 successe però anche qualcos'altro. Venne pubblicato un lavoro elaborato da due crittografi del Massachusetts Institute of Technology che lavoravano per il progetto FreeHeaven(*5) e da un ricercatore che lavorava per il Naval Research Lab.

Cipolle e Dark-web (2)

Il lavoro si chiamava "The Second-Generation Onion Router"(*6) ed era letteralmente un modo nuovo di vedere la dark net. Modificando sostanzialmente la prima versione dell'onion routing - in italiano suonerebbe "connessione a cipolla" - proposta dal DARPA(*7) statunitense, i tre ricercatori crearono quella struttura teorica per ciò che sarebbe diventato noto al grande pubblico col nome di Tor(*8).

Lavoriamo di astrazione. Immaginate di essere sul surface web e di dover inviare un pacchetto dati da un punto A a un punto B. Nell'immaginario collettivo c'è l'idea che quel pacchetto viaggerà senza interruzioni di sorta, quasi come stesse seguendo una linea continua senza mai fermarsi. Ma la realtà è un po' diversa. Quello che avviene è che il pacchetto passa da parte a parte per poi, non linearmente, approdare a destinazione. Questo viaggio è fatto seguendo alcuni criteri, attraverso determinati protocolli, e utilizzando particolari metodi di trasmissione dati. Alla partenza, durante il tragitto o alla destinazione, noi lasciamo traccia delle nostre azioni, e questo ormai non dovrebbe essere un segreto per nessuno. Spesso si sente dire che, per mettere un filtro fra noi e il server che vogliamo raggiungere,

un buon metodo sia utilizzare una cosiddetta VPN - virtual private network - ma si sa, la sicurezza, specialmente quando siamo in situazioni particolari, non è mai abbastanza.

Immaginate ora un sistema a più strati, a cipolla appunto, dove invece che avere un solo strato protettivo ne abbiamo vari. Questi strati intermedi sono capaci di prendere il pacchetto in arrivo, criptarlo, e inviarlo al livello successivo. Abbiamo, nello specifico, un punto d'ingresso, tre punti di transizione e uno di uscita. In un sistema come questo, l'amministratore del server che vogliamo visitare non riceverà la richiesta dal punto iniziale, bensì da un punto intermedio, rendendo virtualmente difficile - se non spesso impossibile - risalire a quale sia davvero il punto di partenza. Questo è in poche parole tor: un sistema di sicurezza a più livelli creato per tutelare la privacy(*9) nel cyberspazio. C'è però anche qualcos'altro da dire. Questi livelli intermedi, chiamati *relay node*, forniscono non solo gli strati anonimi della cipolla, ma anche e potenzialmente dei luoghi dove poter attivare un server web accessibile solo e soltanto sulla dark net. Questi nodi sono tecnicamente macchine mantenute da volontari e, ad oggi, ce ne sono più di seimila attive(*10) in tutto il mondo.

Se pensate che quelli descritti precedentemente siano solo tecnicismi da hacker che mai potrebbero avere un impatto nella vita reale, siete in errore. La Wikileaks di Julian Assange, o il rilascio dei dati da parte di Edward Snowden, sono eventi avvenuti solo e soltanto grazie all'esistenza della rete Tor. E se non sapete di cosa stiamo parlando, non vi preoccupate: ci arriveremo fra qualche capitolo.

Il migliore dei web possibili

Col termine semantico si intende, prendendo direttamente la definizione che ne fa l'enciclopedia Treccani, qualcosa che "concorre a determinare il significato del discorso"(*11). Se trasliamo questo concetto in informatica, associandolo alla parola web, assume il significato di una internet prodotta attraverso sistemi, standard e protocolli che rendono semplice ed immediata l'estrazione e l'analisi dei suoi contenuti. Se torniamo per un attimo a più di 20 anni fa, Tim Berners Lee in "Weaving the Web"(#15) descriveva così i suoi sogni di futuro:

"Ho un sogno che si sviluppa in due parti. [...] La prima parte è che il web diventi un strumento ancora più importante per la collaborazione fra persone. Ho sempre immaginato il web come un qualcosa non solo da esplorare, ma anche dove ognuno sia capace di creare contenuti. […] Nella seconda parte, la collaborazione si estende ai computer, dove le macchine stesse siano capaci di

analizzare il contenuto dei link e aiutare l'interazione fra gli esseri umani. Questo sogno si chiama web semantico"

Il web, a quei tempi, era in pieno sviluppo. Wikipedia cominciava a imporsi come un nuovo modello collaborativo - in pochi anni diventò più affidabile della storica Enciclopedia Britannica(*12) - e il termine "wikipediano" diventò simbolo di "mi interesso", un nuovo modo di fare attivismo culturale ed essere utili alla comunità. I forum e le mailing list erano nella loro fase calante e cominciavano ad affacciarsi sul web i primi blog. Ma fu la rivoluzione degli RSS che cambiò tutto. Nel 1997 Netscape, allora leader indiscusso fra i browser web, produsse un nuovo standard(*13) all'interno del quale si potevano inserire i metadati principali per ogni sito. Questo strumento era un semplice file di testo chiamato RDF, acronimo che stava per "resource description framework". Fu un importante passaggio nella storia del web tanto che, nel 1999, il consorzio W3C lo inserì tra gli standard consigliati.

Figlio illegittimo del RDF fu l'RSS(*14), un formato nato quasi per caso che fece però transitare rapidamente il web ad un nuovo livello evolutivo. Esso permetteva, ad ogni creatore di contenuti, di distribuire gli aggiornamenti provenienti dal proprio sito attraverso un file unico e coerente a cui il lettore si poteva iscrivere. In sostanza, per il fruitore di contenuti, diventava possibile sapere in tempo reale se il proprio blogger di fiducia aveva prodotto un nuovo articolo senza dover, necessariamente, visitare il sito da cui proveniva la notifica. Nacquero così programmi chiamati "aggregatori" che permettevano di unire, come in una sorta di cartella bookmark, tutti gli RSS dei siti e dei propri podcast preferiti. Lasciando da parte le incompatibilità fra le varie versioni - la migliore è sempre risultata la 1.0(*15) a cui lavorò Aaron Swartz - per ovvi motivi questo formato cominciò a essere utilizzato estensivamente da tutta quella nuova famiglia del web 2.0 che stava cominciando a popolare la "blogosfera". Da quel punto in poi arrivò letteralmente l'esplosione del web decentralizzato. Milioni e milioni di blogger cominciarono a pubblicare contenuti sulle varie piattaforme, differenti CMS cominciarono a diffondersi on-line - Drupal Joomla e Worpress i più famosi - e quel sogno di Tim Berners Lee cominciò lentamente a realizzarsi. Internet era diventato uno strumento per persone fatto da persone(*16), come Linux era diventato un sistema per hacker fatto da hacker.

A new dream on the block

Fra gli anni '80 ed oggi abbiamo avuto una transizione tecnologica straordinaria. Alcuni intellettuali e filosofi della nuova era hanno definito questa fase storica come l'età della "post-informazione" dove i

bit e le persone si sono incontrati in un corpo unico per creare nuovi stili e modelli di vita. Siamo passati, per dirla con parole semplici, da una età dove macchine ed umani erano concetti separati ad un modello di società senza tempo e spazio che tende ad integrare le due entità su uno stesso piano. Con il piccolo problema che, in una economia a sviluppo infinito dove i pochi parametri che contano sono l'efficienza e l'aggiornamento permanente, le macchine vincono a mani basse senza neanche avere la necessità di chiedere il permesso. Nicholas Negroponte, nel corso degli anni '80, è stata una figura chiave nello sviluppo della rete che conosciamo oggi. Fondatore del Media Lab presso il Massachusetts Institute of Technology, è stato uno dei teorizzatori della tecno-utopia odierna dove, usando le parole del filosofo Umberto Galimberti, il passato è male, il presente è redenzione e il futuro è salvezza. In "Being Digital" Negroponte scriveva:

"L'informatica non è più soltanto relativa ai computer. L'informatica è relativa al modo in cui viviamo le nostre vite ogni giorno. La sfida per la prossima decade sarà non soltanto fornire le persone di migliori devices, ma sopratutto di oggetti che comprendano comportamenti verbali e non verbali"

e ancora:

"I computer non possiedono attributi morali, non possono risolvere problemi complessi come il diritto di vita o di morte, ma l'epoca digitale non può essere per questo né rallentata né interrotta"

Nel corso di queste pagine stiamo vedendo come molti visionari abbiano previsto e auspicato il futuro che viviamo oggi. Devices interconnessi, intelligenze artificiali, internet come frontiera per un mondo nuovo, libero e aperto. La domanda è: che prezzo stiamo pagando per questo? È il mondo davvero un posto migliore oggi di quanto lo fosse un tempo? E se non lo è, cosa è andato storto?

Umano, troppo umano

La risoluzione 1441(*17) fu una iniziativa richiesta dal consiglio di sicurezza delle Nazioni Unite nel novembre 2002 per imporre all'Iraq la rimozione completa dei suoi armamenti militari. La posizione strategica del Iraq nel medio oriente, vicino all'Arabia Saudita, al Pakistan e all'Afghanistan dove si pensava fosse la sede del comando centrale di Al Quaeda, lo rendeva drammaticamente pericoloso. In più, l'allora presidente Saddam Hussein, aveva dimostrato nel corso degli ultimi anni una certa ritrosia nell'avallare le indagini degli osservatori delle Nazioni Unite, e questo lo aveva reso una minaccia

aggiuntiva all'interno del quadro generale innescatosi nel dopo 11 settembre. L'Iraq però, e l'intero partito Baatista che lo guidava, non aveva mai dimostrato né di avallare né di supportare il terrorismo religioso intrapreso da Osama Bin Laden e dai suoi pari.

Nel lontano 5 Febbraio del 2003, Colin Powell, segretario di Stato degli Stati Uniti d'America, si presentò presso il consiglio di sicurezza delle Nazioni Unite(*18) affermando:

"Attraverso le informazioni arrivate dalle immagini satellitari e dai nostri servizi segreti, siamo a conoscenza che Saddam Hussein possiede armi di distruzione di massa ed è determinato a fabbricarne altre. [...] Non possiamo dirvi tutto ciò di cui siamo a conoscenza [...] Conosciamo le sue manie di grandezza, la sua storia di aggressioni militari, i suoi legami con le organizzazioni terroristiche. È questo consiglio pronto ad accettare il rischio di rimandare una azione militare? [...] Lasciare Saddam in possesso delle armi di distruzione di massa non è una opzione accettabile, non all'indomani dell'11 settembre"

Si diceva fosse in ballo una sorta di guerra di civiltà, il mondo libero contro il terrorismo islamico, ma era diventato chiaro quasi da subito che lo scopo principale fosse un altro: il controllo del "vicino oriente" - i francesi, a giusta ragione, lo chiamano così - e delle sue risorse petrolifere. L'Iraq, da questo punto di vista, rappresentava una occasione ghiotta che non ci si poteva lasciar sfuggire essendo, già nel 2003, in possesso di ben 112 miliardi di barili di petrolio(*19). Da quella consapevolezza, nacque un movimento pacifista che attraversò tutte le nazioni. In Italia, l'European Social Forum, coordinatosi a Firenze nel 2002 presso Fortezza da Basso(*20), ebbe un ruolo fondamentale nella protesta che avvenne pochi mesi dopo. Un intero movimento globale, coordinatosi ancora attraverso Indymedia, scese in piazza nel febbraio 2003(*21). La guerra contro l'Iraq sarebbe scoppiata un mese dopo, ma il web avrebbe dimostrato una capacità di aggregazione piuttosto potente. Quella guerra fu definita come un "secondo Vietnam" per l'impatto che ebbe sui media, e dai balconi di tutto il mondo spuntarono bandiere arcobaleno che mostrarono la contrarietà da parte di molti ad una azione militare realizzata per motivi di controllo e dominio.

Nel mondo quasi dieci milioni di persone scesero in piazza fra il 15 e il 16 febbraio 2003, e quel movimento, formatosi a partire dal web e dal Social Forum di Porto Alegre, cominciava a dimostrare di esser capace di far massa critica. Sembrava che i sogni dei pionieri stessero cominciando a realizzarsi:

internet avrebbe permesso di sviluppare i confini di un mondo migliore. Ma stava per arrivare sulla scena qualcosa di inatteso. Erano i social network centralizzati - o meglio controllati - che avrebbero dissolto, lentamente, la decentralizzazione che aveva rappresentato il web 2.0 fino ad allora. Purtroppo, ci saremmo accorti degli innumerevoli danni soltanto in seguito.

A cosa stai pensando?

Quando nel 1999 il CEO della Sun Microsystem dichiarò alla stampa che la privacy era morta scoppiò uno scandalo(*22). Scott McNealy - questo il suo nome - stava presentando al pubblico una nuova piattaforma in Java denominata Jini - Jini Is Not Initials(*23). L'affermazione era grave per due motivi. Il primo: il sistema, nella costruzione di un network scalabile e distribuito, richiedeva agli utenti di condividere le loro risorse. E sapere che la privacy per Sun non era importante non era certo un buon inizio. Il secondo: Scott McNealy era membro della Online Privacy Alliance, e come si può immaginare, quel pensiero espresso non era esattamente in linea con l'operato dell'organizzazione. A cinque anni di distanza fu però un ragazzo 25enne a dire più o meno le stesse cose(*24). Era Mark Zuckerberg, CEO di Facebook, social network appena uscito dalla sua fase sperimentale:

"La privacy non è più una norma sociale, e la maggior parte degli utenti che usano i social media non si attendono alcuna norma che tuteli il loro anonimato [...]"

Facebook dava la possibilità a ogni utente di crearsi un profilo personale che includesse un avatar, le proprie preferenze artistiche, musicali, politiche e sessuali, le proprie foto, aveva un messenger interno, e permetteva di aggiornare il proprio "stato" rispondendo alla famosa domanda "a cosa stai pensando?"(*25). In quel modo il network forniva una internet dentro internet, esclusiva e personale - nel primo periodo infatti fu accessibile solo per invito - per potersi connettere con i propri amici e per estendere la propria rete di relazioni. Fu letteralmente un successo.

Il social network blu non fu il primo tentativo di creare qualcosa di simile. Prima di Facebook, MySpace aveva letteralmente spopolato sul web(*26). Ma era un social disomogeneo, poco pulito, e soprattutto, come il Yahoo di quei tempi, pieno zeppo di pubblicità. Arrivò successivamente Twitter: social per il microblogging; Instagram: social per condividere foto; Youtube: social per condividere video; Anobii: social per condividere passioni letterarie; Last.fm: social per condividere gusti musicali; Foursquare: social per la geo-localizzazione, e molti molti altri. In sostanza, fra il 2004 e il 2006,

internet fu letteralmente invaso dalle piattaforme social al grido di "condividi se vuoi rimanere connesso". Il mondo del web stava passando rapidamente dalla decentralizzazione alla centralizzazione. Anche i feed RSS, simbolo della selezione personale delle informazioni, cominciarono ad essere aggregati da molti utenti sulla piattaforma Google Reader. In questo modo, anche le fonti provenienti da blog personali, entravano nel grande file delle nostre preferenze. Era arrivata, col nostro silenzio/assenso, l'era del profiling.

C'è un dataismo di troppo

Con l'avanzare delle politiche dei metadati e del personal profiling, siamo entrati direttamente nell'epoca del dataismo, termine presentato per la prima volta dal giornalista David Brooks sul New York Times(*27) all'indomani dell'elezione di Barak Obama. Brooks lo definisce come una sorta di filosofia religiosa, nata con l'assunto di poter predire, con un certo grado di accuratezza, i nostri pensieri e le nostre azioni. Ma cosa ne è dei nostri sentimenti e delle nostre intuizioni? Un insegnante, per esempio, sa riconoscere se un alunno abbia o meno una mente razionale, o se sia portato per una determinata materia. E non certo facendo una media statistica dei suoi risultati scolastici, ma estrapolando piccoli dettagli che la sua professione e la sua esperienza hanno permesso di cogliere. Dov'è dunque, nella religione dataista, l'interazione fra cervello destro e cervello sinistro? Dov'è l'immedesimazione con l'altro? Dove sono tutte le emozioni che derivano dalla disposizione dei neuroni specchio? Di una cosa possiamo essere certi: dai metadati non si può ancora estrarre il campo "empatia". Come ben descrive Noah Arari nel suo monumentale "Homo Deus"(#17):

"Il lavoro di processamento dei dati deve essere affidato agli algoritmi informatici che superano di gran lunga la capacità di processare informazione [...] ma il dataismo è scettico nei riguardi della conoscenza umana, e preferisce trasformare tutto in dati da analizzare"

L'economia dei dati, nell'epoca del libero mercato, è così fiorente che sono addirittura nate aziende chiamate data broker(*28) che acquistano, conservano e rivendono metadati al miglior offerente: Acxiom, Epsilon e Experian, per esempio, sono soltanto alcune di esse. Ed in questa economia, le potenze di calcolo per processare questi dati devono essere strutturalmente infinite. In un bellissimo libro del 1970 chiamato "Future Shock"(#18), il futurologo Alvin Toffler predisse, con una trentina di anni di anticipo, il periodo che saremmo arrivati ad affrontare. Diceva:

"Se la sovrastimolazione dei livelli sensoriali continuerà ad aumentare, arriverà un momento in cui tutto ciò interferirà con la nostra capacità di prendere decisioni. Ognuno di noi sarà costretto a processare l'immensa mole di informazioni con difficoltà per attuare scelte razionali"

La chiamò "information overload"(*29), un processo che nel corso del tempo avrebbe potuto portare, come argomentava lo psichiatra James Miller, a problemi psicopatologici mai affrontati prima. E allora forse, siccome il nostro cervello è così complesso e nella sua complessità cosi imperfetto, qualcuno avrà pensato: perché non delegare tutto alle macchine, che sono performanti, programmabili e per giunta senza empatia? Lascio al lettore trovare la fallacia logica in questo ragionamento.

Evviva l'illuminismo

Il Cubo di Rubik fu inventato nel 1974 dal professore di architettura ungherese Ernő Rubik con l'intento di spiegare ai suoi studenti gli spazi in tre dimensioni. L'originale cubo, il 3x3x3, è sostenuto da un blocco centrale che lo regge internamente mentre ogni lato è rappresentato da sei piccoli cubi capaci di permutare fra loro. Quando, nel 1977, il cubo fece il debutto sul mercato fu un successo straordinario(*30). Diventò quasi subito uno dei simboli degli anni '80 e generò una interessante gara fra matematici per studiarne struttura e proprietà. Risolvere il cubo voleva dire, banalmente, riportarlo in uno stato di ordine, con un solo colore per lato, con meno mosse possibili. Nacquero allora molti metodi di risoluzione. Il primo e il più famoso fu il metodo a strati che aveva una risoluzione media, calcolandola in una curva gaussiana, fra le 85 e le 205 mosse. Non male certo, ma non era abbastanza. Fu soltanto col metodo CFOP(*31), scoperto nel 1997 dalla professoressa di elettronica Jessica Fridrich, che la curva a campana si restrinse drasticamente(*32) e si arrivò ad una media statistica che andava fra le 40 e le 70 mosse. Questo permise ad una attività fino ad ad allora amatoriale chiamata "speedcubing" - l'arte di risolvere rapidamente il cubo di rubik - di diventare una disciplina professionale che raggiunge oggi migliaia di partecipanti in tutto il mondo. La scienza funziona esattamente cosi: fornisce uno schema di rappresentazione(*32) e cerca di risolvere i problemi in maniera sempre più efficiente.

Proviamo ora a descrivere la nostra società. Leggendo i dati e le statistiche, dovremmo essere estremamente positivi. Numeri alla mano infatti, sappiamo che, lentamente ma inesorabilmente, la fame nel mondo sta diminuendo, le guerre nel mondo si stanno riducendo(*33) e che l'aspettativa di vita sta aumentando. Ma nonostante questo, abbiamo la percezione - me incluso - che non sia così. Steven

Pinker, uno dei pochi intellettuali che si è preso la briga di analizzare i dati, ha definito questa paura nel progresso con un termine: progresso-fobia. Nel suo libro "Enlightenment Now"[(#19)] scrive:

"Ho scoperto che gli intellettuali che amano definirsi "progressisti" odiano il progresso. Non che odino davvero i frutti del progresso: molti di loro preferiscono avere un intervento chirurgico con anestesia piuttosto che senza. È l'idea stessa di progresso che li irrita, o meglio l'idea che l'illuminismo possa portare verso un miglioramento delle condizioni di vita"

Questo però non ci può rendere ciechi di fronte ai difetti del mondo che ci circonda. Se fosse così, negheremmo il principio stesso del progresso scientifico, che ha come suo obbiettivo il miglioramento dell'intero, non di una sua parte. Tornando per un attimo al nostro cubo, cosa sarebbe successo se la dottoressa Fridrich non si fosse posta l'obiettivo di creare un algoritmo più efficiente degli altri? Saremmo arrivati, oggi, a risoluzioni al di sotto dei cinque secondi? Come vedete, tutto si tiene insomma, anche parlando di cose apparentemente frivole.

Dal tavolo del ricercatore

La scienza non esiste. Quello che esiste davvero è la comunità scientifica. Ma come funziona esattamente la fase di pubblicazione?

Immaginate di essere in un laboratorio di ricerca e dopo aver letto più di un centinaio di lavori scientifici, vi rendete conto che c'è un aspetto non ancora investigato dai vostri colleghi e, potenzialmente, rivoluzionario. Vi presentate quindi timidi e insicuri davanti al vostro PI - "principal investigator" - per chiedergli se il gruppo col quale lavorate ha le risorse professionali ed economiche per portare avanti la vostra idea. Dopo alcuni - noiosissimi - passaggi burocratici, la vostra idea viene accettata e cominciate, voi da soli o insieme al vostro team, a raccogliere i dati che confermino o smentiscano quello che avete in mente. Immaginiamo ora che la ricerca vada a buon fine, e che siate arrivati al risultato sperato. La soddisfazione è grande ed ora, con pazienza, vi mettete a scrivere quello che in gergo tecnico si chiama "paper scientifico".

Questo paper è diviso in quattro parti. La prima si chiama "abstract", ed è un insieme di parole che descrivono, tramite una forma più semplice possibile, i risultati ai quali siete arrivati. Poi ne abbiamo un'altra introduttiva che analizza lo stato della ricerca fino a quella data. E poi una successiva, la più

importante, che descrive la ricerca vera e propria con calcoli, grafici, citazioni e riferimenti. La parte conclusiva fa soltanto da corollario finale e serve a fornire al lettore nuovi spunti per ricerche successive. Bene, se questo vi sembra un processo lungo e pedante, non avete idea di cosa venga dopo.

Una volta scritto questo paper, voi o il vostro dipartimento vi occupate di scegliere alcune riviste scientifiche a cui inviarlo. Se il vostro lavoro tratta un argomento astronomico lo si invierà al "astrophysical journal", se è inerente ad un argomento medico lo si invierà al "british medical journal" e così via. Ogni giornale si classifica attraverso un parametro chiamato "impact factor". Più è elevato questo parametro, più il giornale acquista credibilità all'interno della comunità scientifica.

Dopo decine e decine di rimpalli fra voi e i "peer reviewer" - revisori fra pari, anonimi e chiamati in causa dal giornale stesso per fare le pulci al vostro paper - ammettiamo che il vostro lavoro venga accettato. C'è a questo punto un piccolo problema: i costi. Così come è dispendioso realizzare una ricerca scientifica, così è anche dispendioso pubblicarla, stamparla e diffonderla. Come è stato risolto questo problema nel modello tradizionale? Banalmente facendo ricadere i costi delle pubblicazioni sui lettori. I centri accademici quindi, per poter accedere al vostro lavoro, devono fornirsi di una sottoscrizione, a volte piuttosto costosa, che permetta di accedere alla banca dati del giornale. Ciò non è sorprendente, ma ha un terribile risvolto della medaglia: le ricerche possono essere lette soltanto da chi ha la possibilità economica di pagare un abbonamento. Questo, per esempio, impedisce a centri di ricerca situati nel terzo mondo di accedere a quei risultati. Ergo, il dibattito scientifico, che da lì in poi si innescherà, sarà un dibattito elitario, realizzato soltanto da chi può permetterselo. Ma è l'economia bellezza, nulla è gratis. O forse in questo caso dovremmo avere altre prerogative?

Fino alla scienza in Open Access

Ora immaginate un modello diverso, in cui i costi non ricadano sui lettori ma direttamente sul centro scientifico che ha portato avanti la ricerca. Immaginate ora che in questo modello tutti i lavori pubblicati, dopo aver passato una fase di "peer review", esattamente come nel modello tradizionale, siano disponibili gratuitamente sul web, liberamente accessibili e addirittura commentabili dai colleghi come fossero articoli di un blog. Voi, come ricercatori, quale modello sceglliereste? Quale modello pensate sia migliore per diffondere rapidamente la vostra ricerca? Se ricordate, abbiamo cominciato dicendo che la scienza non esiste ma che, al contrario, esiste la comunità scientifica. Ed è infatti attraverso l'analisi del vostro lavoro che quei risultati acquisteranno credibilità. Più il lavoro è citato - in

gergo tecnico si chiama “cross-refence” - più il lavoro acquisterà valore. Più i vostri risultati sono validati e confermati dai vostri colleghi, più quei risultati acquisteranno autorevolezza. Questo modello esiste e si chiama "open access" - ad accesso aperto -.

PlosOne(*35) nel 2006 - e tutte le riviste open access in generale - hanno completamente cambiato le carte in tavola della pubblicazione scientifica in due aspetti. Il primo: un giornale online ha decisamente più spazio, e potendo pubblicare più materiale, si riserva di analizzare l'accuratezza scientifica e non l'impatto politico, sociale o economico che potrebbe avere la vostra ricerca per la rivista in questione. Il secondo: i costi non ricadono più sui lettori, che hanno la possibilità di leggere e valutare gratuitamente, ma sui ricercatori, che possono a questo punto espandere l'audience della propria ricerca diffondendola attraverso un modello aperto.

In epoca di Covid-19 per esempio la stessa biblioteca Jstor(*36) ha rilasciato parte delle sue risorse in open access in modo da facilitare pubblico, studenti e istituzioni accademiche nella migliore comprensione della pandemia generata dal Sars-Cov-2(*37). Questo vuol dire semplicemente una cosa: diffondere l'informazione liberamente è un modello vincente. Non ci soffermeremo qui sui problemi interni - come il "publish or perish" o il "predatory publishing" - ma di certo l'open access scientifico è uno degli esempi più evidenti di come non fermarsi allo status quo, sollevare critiche, innovare, creare una alternativa e guardare oltre.

Riferimenti

(*1) https://www.cs.cmu.edu/~rgs/alice-I.html
(*2) https://freenetproject.org/assets/papers/ddisrs.pdf
(*3) https://freenetproject.org/
(*4) https://geti2p.net/
(*5) https://geti2p.net/en/faq
(*6) https://www.onion-router.net/Publications/tor-design.pdf
(*7) https://www.darpa.mil/about-us/about-darpa
(*8) https://www.torproject.org/about/history/
(*9) https://www.freehaven.net/anonbib/
(*10) https://metrics.torproject.org/relays-ipv6.html
(*11) https://www.treccani.it/vocabolario/semantico/

(*12) https://www.cnet.com/news/study-wikipedia-as-accurate-as-britannica/
(*13) https://www-archive.mozilla.org/rdf/doc/
(*14) https://www.rssboard.org/rss-0-9-1-netscape
(*15) https://edition.cnn.com/2013/01/15/tech/web/aaron-swartz-internet/index.html
(*16) https://cs.stanford.edu/people/eroberts/cs181/projects/personal-lives/debate.html
(*17) https://www.un.org/Depts/unmovic/documents/1441.pdf
(*18) https://www.americanrhetoric.com/speeches/wariniraq/colinpowellunsecuritycouncil.htm
(*19) https://www.worldometers.info/oil/oil-reserves-by-country/
(*20) https://www.opendemocracy.net/en/article_736jsp/
(*21) https://www.huckmag.com/perspectives/activism-2/italy-iraq-unlike-britain-u-s-stop-war-movement-succeeded/
(*22) https://www.wired.com/1999/01/sun-on-privacy-get-over-it/
(*23) http://sunsite.uakom.sk/sunworldonline/swol-08-1998/swol-08-jini.html
(*24) https://www.crn.com/news/security/222300279/facebooks-zuckerberg-face-it-no-one-wants-online-privacy-anymore.htm
(*25) https://www.history.com/this-day-in-history/facebook-launches-mark-zuckerberg
(*26) https://www.theatlantic.com/technology/archive/2011/01/the-rise-and-fall-of-myspace/69444/
(*27) https://www.nytimes.com/2013/02/05/opinion/brooks-the-philosophy-of-data.html
(*28) https://yourdigitalrights.org/data-brokers
(*29) https://www.bbc.com/future/article/20120306-information-overload-fears
(*30) https://ruwix.com/the-rubiks-cube/history-rubiks-cube/important-dates-timeline/
(*31) https://www.nytimes.com/2008/12/16/science/16prof.html?_r=1&em
(*32) http://www.diva-portal.org/smash/get/diva2:812006/FULLTEXT01.pdf
(*33) https://plato.stanford.edu/entries/scientific-method/
(*34) https://ourworldindata.org/war-and-peace
(*35) https://undsci.berkeley.edu/article/howscienceworks_16
(*36) https://www.sciencemag.org/news/2014/06/output-drops-worlds-largest-open-access-journal
(*37) https://about.jstor.org/covid19/

Capitolo 4 - Che mi sento di morir

La crisi dei sub-prime...

Il periodo che va fra il 2007 e il 2009 è stato uno dei peggiori che abbia attraversato l'intera economia mondiale. Tutto cominciò negli Stati Uniti(*1) durante l'amministrazione Clinton, quando vennero erogati numerosi mutui "sub-prime" a creditori che precedentemente si erano dimostrati insolventi. Lo scopo, quasi ingenuamente, era uno solo: permettere a molti statunitensi di essere proprietari di una casa. In questo sistema, Fannie Mae e Freddie Mac - aziende leader nei mutui abitativi - cominciarono a incrementare il numero dei contratti da loro erogati, contribuendo così a creare una bolla speculativa. Favorite dalla deregolamentazione degli strumenti derivati di investimento, per banche e assicurazioni diventò pertanto possibile fornire fondi ai mutuatari con minor rischio. Il sistema di "cartolarizzazione" era appena iniziato, ma stava già per generare i primi danni. Si capì ben presto che la maggior parte dei mutui erogati non sarebbero stati mai ripagati. Questo generò a cascata prima la crisi dei mutui, poi una discesa repentina dei prezzi delle case e poi il crollo della bolla speculativa. Il 15 settembre 2008 la banca di investimenti Lehman Brothers dichiarò bancarotta(*2) e l'effetto domino cominciò. Andrew Sorkin, giornalista economico presso il New York Times, nell'introduzione di "Too big to fail"(#20) scrisse:

"In un qualche modo, Wall Street fu buttata giù dai suoi uomini più brillanti, poiché, data la complessità degli strumenti derivati, nessuno era davvero in grado di definire il prezzo in un mercato in declino. Senza un prezzo il mercato si paralizzò, e senza accesso ai capitali Wall Street non poteva funzionare"

Non c'è algoritmo che tenga: anche ammesso e non concesso che il neoliberismo sia il migliore dei mondi possibili, l'errore umano è sempre dietro l'angolo. E se l'errore non viene aggiunto come

parametro aleatorio all'interno dell'algoritmo, rischia costantemente di evidenziare ed espandere drammaticamente le vulnerabilità di un sistema centrale e verticistico.

...e la rivoluzione della Blockchain

La risposta da parte della comunità cyberpunk - o meglio la sua estensione, il cypherpunk - non si fece attendere. Nessuno sa davvero come sia andata la storia, ma la leggenda vuole che verso la fine del 2008 un gruppo formato da economisti, crittografi, programmatori, matematici e sviluppatori si riunisse in una stanza cercando di analizzare cosa fosse andato storto e cosa avesse generato la seconda crisi economica in meno di cento anni. Si identificarono così alcuni punti. Il primo: il sistema era in mano a grandi monopoli, o in termini informatici, era un sistema fortemente centralizzato. L'esperienza storica, a partire da bittorrent fino alla stessa rete internet, ci aveva dimostrato invece che i sistemi vincenti erano sempre stati quelli decentralizzati. Il secondo: tutto si basava sulla fiducia fra utente e ente bancario. Serviva invece un qualcosa che riportasse le transazioni alla loro naturale essenza, fra utente e utente dunque, bypassando il sistema centrale delle banche e rompendo in questo modo il loro monopolio. Il 31 ottobre 2008, a meno di un mese dal fallimento della Lehman Brothers, il team si diede il nome fittizio di Satoshi Nakamoto, e con quello pseudonimo pubblicò un paper che fece storia: "Bitcoin: A Peer-to-Peer Electronic Cash System"(*3):

"Quello di cui abbiamo bisogno è un sistema di pagamento basato su prova crittografica, che permetta alle due parti di transare direttamente senza il bisogno di doversi interfacciare con una terza parte. In questo lavoro, proponiamo una soluzione al problema della doppia-spesa introducendo un archivio distribuito peer-to-peer per generare una prova computazionale che metta le transazioni in ordine cronologico"

Il bitcoin non era la prima criptomoneta uscita sul mercato. Tentativi di creare qualcosa di simile c'erano già stati(*4) ma erano tutti falliti. Bitcoin invece, nella sua semplicità, aveva tutto quello che si chiedeva a una moneta digitale.

In una transazione tradizionale, quando un pagamento migra fisicamente fra un portafoglio e un altro, quest'ultima deve passare per un intermediario bancario il quale si occupa di verificare sia l'identità dei soggetti, sia la presenza o l'assenza di fondi. In una transazione fra portafogli bitcoin il sistema è invece completamente diverso(*5). La storia di tutti i pagamenti infatti risiede all'interno di una lunga catena

chiamata blockchain, dove ogni blocco risolto contiene una serie di dati che, in sostanza, rappresentano una sorta di fotografia temporale dell'intero stato del sistema. Si crea un blocco pressoché ogni 10 minuti, ed il suo limite, in termini di spazio virtuale, è esattamente di un megabyte, né più né meno. La risoluzione di un blocco di dati viene realizzata da un software apposito che altro non fa che verificare, controllare, calcolare e chiudere il blocco attraverso alcune operazioni computazionali. Questo lavoro viene fatto da alcune figure che nella comunità vengono chiamate i "miners"(*6) - letteralmente minatori - che attraverso dei computer potentissimi, o meglio schede grafiche pompate alla massima potenza, partecipano a questa sorta di gara matematica in cui il vincitore guadagna la sua quoticina di bitcoin.

Ma dove risiede la blockchain? Beh, è questo il bello: la blockchain è pubblica(*7) e decentralizzata. Non esiste, come si dice in gergo tecnico, un "single point of failure", ovvero un punto che, buttato giù, fa crollare tutta la catena. Questo rende la blockchain tecnicamente impossibile da bloccare. Inoltre nel suo codice sorgente, si introduce il concetto della scarsità: nell'intero sistema non si possono "minare" più di 21 milioni di bitcoin, e questo la rende simile all'oro, rara e con un alto valore intrinseco.

Dalla sua creazione, numerosi furono i tentativi di creare nuove monete digitali, ma il bitcoin, insieme a poche altre, conserva in sé i punti cardine più importanti: sicurezza e decentralizzazione(*8). Era l'uovo di Colombo. Internet aveva la sua moneta.

Un Ebay sulla Darknet

La valuta fu talmente popolare che appena tre anni dopo un ragazzo creò sulla darknet, sotto il sistema tor, un intero shop online dove si poteva acquistare utilizzando bitcoin. Per la natura della rete tor e la natura della moneta in questione, il sito divenne popolare come il luogo dove si potevano acquistare droghe leggere, meta-anfetamine e oppioidi. Il suo creatore Ross Ulbricht, un 23enne programmatore informatico, bandì dallo shop prodotti come carte di credito clonate, hacking, armi e pornografia infantile. Il sito divenne popolare col nome di "Silk Road"(*9), nome che richiamava quel lungo e bellissimo percorso intrapreso da Marco Polo alla scoperta della Cina. Nei suoi due anni di attività - dal 2011 al 2013 - totalizzò in transazioni qualcosa come 30 milioni di dollari, dimostrando così che il sistema era stabile, sicuro e poteva funzionare.

Come scrisse lo stesso Ulbricht sul suo profilo LinkedIn(*10):

"Vorrei poter usare la teoria economica per abolire l'uso della coercizione e dell'aggressione contro l'intera umanità. [...] Per questo motivo, sto creando una simulazione economica per dare al popolo una rappresentazione [...] di come si potrebbe essere vivi in assenza dell'uso sistematico della forza"

La vicenda è molto complessa(*11). Ross Ulbricht fu arrestato e poi condannato con l'accusa di aver effettuato riciclaggio di denaro sporco e distribuzione di droghe illegali sotto il nickname di DreadPirateRoberts. Silk Road - e questo può non sorprendere - fu fin da subito monitorata dalla DEA - Drug Enforcement Administration - che investigò per anni le sua attività e si infiltrò segretamente per analizzare le transazioni. Durante il processo intentato contro SilkRoad, fu dimostrato inoltre che l'agente segreto Carl Mark Force ebbe accesso al database per poi modificarne contenuti, chat interne e messaggi privati. In un messaggio - successivamente verificato come falso - inviato da DreadPirateRoberts all'utente RedAndWhite, si legge:

"Mi dispiace chiederti questo in un momento in cui ci siamo appena conosciuti, ma FriendlyChemist mi sta causando un sacco di rogne [..] Ho davvero bisogno di mettere un proiettile nella sua testa, se questo non ti causa troppi problemi"

Va detto e specificato che questa accusa di omicidio si rivelò falsa ben prima del dibattimento ma, nonostante questo, la sentenza finale la tenne in considerazione nel calcolo della pena(*12). Ross Ulbricht è attualmente in carcere con ben due ergastoli alle spalle, senza possibilità di condizionale. Si direbbe: colpirne uno molto bene, per educarne ancora meglio altri cento. Sul Global Politics and Strategy, giornale bimensile di geopolica, si trova un interessante articolo intitolato "Cryptopolik and Darkweb"(*13). In questo pezzo, gli autori analizzano nel dettaglio l'utilizzo della rete tor e il ruolo che ha bitcoin al suo interno. Si scrive fra le righe:

"[...] per tutelare la reputazione di Tor si consiglia di eliminare gli hidden-services, almeno per quanto riguarda la loro forma attuale"

Nell'oceano di critiche che si fanno alla darknet, si scopre che, in un totale di 5200 siti web analizzati, poco più del 15% sono quelli che utilizzano bitcoin per vendita e acquisto di droghe, e un altro 14% sono quelli quelli utilizzati per altre operazioni illegali. Questo potrebbe spaventare, ma visto nel complesso vuol dire che ben il 70% delle operazioni eseguite sul darkweb sono assolutamente

legittime, e chi usa tor lo fa essenzialmente per ragioni di sicurezza e privacy. Ergo: vietare il bitcoin o la darknet sarebbe come vietare il dollaro o bannare la Colombia. Giusto una piccola nota a margine: bitcoin non è strutturato per essere anonimo ma è fatto al contrario per tenere traccia di tutte le transazioni storiche attraverso la blockchain. Se così non fosse, come avrebbero potuto acquisire le prove per arrestare Ross Ulbricht?

We Are Legion - o quasi

Pochi anni prima, nei meandri di 4chan, un imageboard inizialmente nato per condividere discussioni su manga e anime, si cominciò a aggregare un gruppo di utenti che si coordinava per atti di hackeraggio informatico. Storicamente si fa risalire la nascita di questo gruppo sul /b/ board(*14) nel 2004 ma effettivamente la prima operazione eclatante con cui salirono alla ribalta dei media avvenne nel 2008. Si parla ovviamente di anonymous(*15), i cui membri si distinguono come quelli che in pubblico indossano le maschere di Guy Fawkes, il famoso terrorista che il 5 novembre 1605 attentò al Parlamento britannico(*16).

"We are anonymous. We are Legion. We do not forgive. We do not forget. Expect Us"

È, in sostanza, un movimento unico ma decentralizzato, composto da una massa enorme di persone identificabili soltanto dai loro scopi finali: dal trollare un radioamatore nazista che ritiene Obama "geneticamente inferiore" per governare gli Stati Uniti D'America, allo scagliarsi contro il circuito Visa alla base del funzionamento delle maggiori carte di credito. Una intera generazione ha forgiato le proprie idee inerenti alle libertà informatiche in questo ambiente. Non è un segreto che le idee del free software, dell'open access e del creative commons circolassero liberamente su questo board, ma a differenza di reddit(*17), il network fondato da Aaron Swartz, qui si parlava espressamente di attacchi informatici e di trolling, non di libertà informatiche nel senso politico del termine.

Gli anonymous, nel mondo dell'hacking, son sempre stati considerati - LulzSec(*18) e AntiSec sono rare eccezioni - come script-kiddies, ovvero come ragazzini poco esperti di sicurezza informatica, politicamente coinvolti, ma che in gruppo potevano organizzarsi per hackerare e floodare siti con un attacchi ddos et similia. Quando nel 2008 decisero, con l'operazione Chanology(*19), di sferrare l'attacco alla Chiesa di Scientology, per molti - come me - che osservavano dall'esterno, fu davvero uno spasso. Rilasciando online un video(*20) in cui Tom Cruise, famoso membro della Chiesa creata da Ron L.

Hubbard, elogiava le innumerevoli(?) potenzialità della dottrina, pianificarono una serie di attacchi informatici alla loro piattaforma e continuarono a disturbare le attività con telefonate, manifestazioni nelle maggiori città degli States e con costanti incursioni. Il danno ricevuto da Scientology fu enorme. La Chiesa fu costretta a cambiare tipo di comunicazione, a rivedere gli standard di sicurezza che il sito sembrava non avere affatto, e a cominciare una lunga china che poi l'avrebbe portata verso il declino. Fu, in altre parole, la rappresentazione chiara di quanto la rete, senza alcun leader, avrebbe potuto letteralmente imprimere un importante cambiamento nella società reale. Ma non era tutto rosa e fiori.

Pirati (tanto) politici

Nello stesso periodo, in Svezia, nel lontano nord dell'Europa, veniva spento PirateBay(*21). Appena due anni prima, due hacker informatici avevano dato vita ad una associazione no profit che aveva aperto il più ricco ed esteso repository di file torrent ci fosse sul web. Bittorrent, dopo la caduta di Napster e di Gnutella, era diventato il protocollo P2P più utilizzato per scambiarsi liberamente file coperti da diritto d'autore. Dopo il noto caso del DeCSS, un software sviluppato dal giovane programmatore Jon Johansen, era diventato infatti possibile decrittare anche dvd coperti da diritti d'autore su piattaforma Linux e successivamente ripparli in un file unico. E con l'arrivo delle alte velocità, PirateBay era diventato un serio pericolo, poiché risultava la fonte da cui molti utenti traevano i link da cui scaricare non soltanto musica, ma anche film, software ed ebook senza il DRM. Quasi contemporaneamente, nel gennaio 2006, un programmatore svedese, Rick Falkvinge, postò su un forum la proposta di un manifesto politico per un possibile nuovo partito. Gli argomenti di cui si dibatteva erano - finalmente - la rimozione delle leggi di copyright, un cambio radicale delle leggi relative al file-sharing, l'adozione di software open source nell'amministrazione pubblica e così via. Era appena nato il Pirate Party(*22), movimento che, di lì a breve, divenne uno dei pochi partiti ad avere una estensione transnazionale.

"Il Partito Pirata, nelle sue dichiarazioni di intenti, non prende posizione riguardo ad idee di destra o di sinistra. Siamo pronti a supportare sia i social-democratici che un governo non-socialista. L'unico problema che attualmente ci interessa è che la società del controllo di massa sia cancellata, e che cultura e conoscenza siano rese libere"

Il partito si organizzava in forum, meeting, discussioni e portava per la prima volta la politica dal virtuale al reale. Nel fare questo aveva adottato software open source sia per la costruzione delle proprie piattaforme online, sia per i propri siti web, sia per le votazioni interne ed esterne. Per il voto

on-line in particolare - *anche se altamente sconsigliato* - avere un software open source e non closed-source crea standard trasparenti e fiducia fra base e rappresentanti. Se oggi la net neutrality e la riforma del copyright sono argomenti che i partiti politici cercano di accaparrarsi, lo dobbiamo proprio alla nascita del Pirate Party e al suo fondatore che, in tempi non sospetti, portò un argomento fino ad allora relegato soltanto alla rete nella vita reale. Non troppo dissimile da quello che avvenne con il Green Party per le tematiche relative all'ambientalismo.

Il ruolo del nuovo giornalismo

Nel famoso film "Matrix" scritto dai fratelli - ora sorelle - Wachowski, Morpheus incontra Neo per la prima volta e lo porta, dopo averlo disconnesso dalla rete, all'interno di un programma di simulazione chiamato "struttura"(*23):

"A lungo non ci ho voluto credere [...] Potendo constatare la loro limpida, raccapricciante precisione, mi è balzata agli occhi l'evidenza della verità. Che cos'è Matrix? È controllo. Matrix è un mondo virtuale elaborato al computer, creato per tenerci sotto controllo [...]"

Il giornalismo è uno di quei classici sistemi complessi che richiedono più passaggi e più interazioni per la risoluzione di un problema. Trattandolo come un algoritmo informatico, potremmo dire che ha una sua "complessità computazionale" intrinseca: si raccolgono dati, si selezionano, si interpretano e se ne fa un resoconto che sia più chiaro possibile. Nel farlo, il giornalismo si esercita in quel complicato *lavoro di divulgazione* che consiste nel cercare di trasformare qualcosa di scritto per addetti ai lavori in un testo leggibile da un pubblico più ampio possibile. È un lavoro nobile, che non pone - o non dovrebbe porre - l'attenzione sul soggetto che lo compie ma sul destinatario che ne riceve gli effetti. All'interno del processo che porta alla scrittura di una inchiesta, il giornalista si esercita nella ricerca delle fonti, ma ciò è spesso un problema di non facile soluzione. A volte si hanno indizi, intuizioni ma le fonti spesso restano nascoste, chiuse a chiave con doppia mandata, quasi impossibili da trovare. Pasolini nel 1974 scriveva(*24):

"Io so. Ma non ho le prove. Non ho nemmeno indizi. Io so perché sono un intellettuale, uno scrittore [...] che coordina fatti anche lontani, [...] che ristabilisce la logica là dove sembrano regnare l'arbitrarietà, la follia e il mistero."

Internet, da questo punto di vista, è stato un game changer. Fonti che fino a pochi anni fa erano difficili da scovare son diventate, con minor sforzo, accessibili e analizzabili più facilmente. Il giornalismo dunque si è trasformato all'interno della società moderna, portando alla nascita di realtà che hanno fatto emergere il grassroots journalism (giornalismo dal basso), il crowfunded journalism (giornalismo finanziato dai lettori) e il data journalism (giornalismo basato sui dati). ProPublica ne è un esempio virtuoso: nata nel 2007 e finanziata - ma non soltanto in realtà - dai lettori, è stata protagonista di alcune inchieste che le hanno fatto meritare ben quattro premi Pulitzer. In un tempo di crisi dell'editoria e di assenza di vero giornalismo di inchiesta, questo fenomeno emergente rappresenta un respiro vero per l'informazione libera poiché si focalizza non più, come si suol fare, sulle breaking news, ma solo e soltanto sulle inchieste che richiedono tempo, pazienza, attenzione, e raccolta certosina dei dati(*26).

Ma ci sono dati, informazioni importanti, che son davvero difficili da ottenere. Sono quelle informazioni top secret, interne ai dipartimenti di sicurezza, a cui soltanto alcune persone selezionate hanno accesso. A volte però accade che dall'interno del sistema qualcuno ne abbia abbastanza e decida di diffonderle. Ma come fare a proteggere il suo anonimato? Come fare a rendere anonima la fonte e pubblici i documenti? È a questo punto che si incontra Wikileaks.

Mendax è tornato

Il dominio wikileaks.org venne registrato nel lontano 2006 per essere semplicemente una "wiki" dove pubblicare alcuni documenti classificati relativi alla guerra in Afghanistan. Il fondatore non era di certo nuovo alle cronache. Julian Assange infatti era conosciuto nel mondo del cyber-attivismo col nickname di "Mendax"(*27). Si interessò sia di informatica che di fisica. Si iscrisse all'università di Melbourne per poi abbandonarla poco prima di conseguire il diploma di laurea. In giovane età fu condannato per essersi infiltrato illegalmente nei server del Pentagono e in quelli della NASA. Uno dei crimini informatici di cui è sempre stato sospettato è l'attacco col worm "Wank" durante il lancio della sonda Galileo(*28). Il giorno 18 ottobre 1989, sui monitor del Kennedy Space Center, apparve la scritta:

"You talk of times of peace for all, and then prepare for war"
[Parlate di un futuro di pace per tutti, e intanto vi preparate per la guerra]

Il sistema che proponeva Wikileaks era molto semplice, anche se strutturalmente complesso(*29): fornire una piattaforma dove tutelare l'anonimato e la sicurezza dei "whistleblower". La sottomissione delle

fonti avveniva grazie al sistema Tor, di cui abbiamo parlato in precedenza, il quale assicurava un certo grado di anonimato grazie agli strati intermedi in cui transita la sua connessione dati. Diventava quindi un database di documenti forniti da fonti pressoché anonime e in grado di destabilizzare la narrazione che i governi nazionali amavano fornire di loro. Uno dei primi leaks che balzarono alle cronache furono i documenti per il trattamento dei detenuti nel carcere di Guantanamo Bay(*30). Quelle foto e quei materiali riservati dimostravano la ripetuta violazione della convenzione dei diritti dell'uomo e del cittadino(*31), che vietava i metodi di tortura coercitiva per estorcere informazioni. A seguito di quell'operazione, il sito fu oscurato per la prima volta da parte dal governo degli Stati Uniti ma continuarono a sopravvivere alcuni suoi mirror come quelli in Belgio e in Irlanda. Si inaugurò da allora la battaglia del "impero statunitense" - ho scelto le parole con cognizione di causa - contro Wikileaks, in cui la Russia, seguendo il noto principio del "i nemici dei miei nemici sono miei amici", cominciò a fare la sua parte proteggendo Assange.

Appena un anno dopo, Wikileaks fece ancora parlare di sé. In aiuto degli anonymous, che su 4chan avevano deciso di ingaggiare la battaglia contro Scientology, rilasciando qualcosa come 110 documenti(*32) fra cui audio originali di Ron Hubbard in cui si descriveva l'assurda storia di Lord Xenu e dei Thetans intrappolati sulla Terra. Ma fu soltanto pochi mesi dopo che avvenne il caso più eclatante. Nel 2010 un semplice soldato, addetto alla sicurezza informatica durante la guerra in Iraq, rilasciò a Wikileaks ben 700 documenti classificati che segnarono la storia del giornalismo moderno. Nella notte fra il 21 e il 22 maggio del 2010, Adrian Lamo, grey-hacker famoso fra le altre cose per aver bucato il server del New York Times, fu contattato da un certo Bradley Manning che sosteneva di lavorare a Baghdad come intelligence analyst. Manning rivelava di essere stato confinato in isolamento per problemi comportamentali e che da otto mesi ormai aveva accesso ad informazioni classificate, sette giorni su sette, 24 ore su 24. Nei giorni in cui Lamo ricevette la chat, era spesso via dal computer poiché viveva ancora in attesa di un alloggio fisso. Non gli piaceva ciò che stava leggendo, ma lo lasciò parlare lo stesso. E Manning si sfogò completamente(*33). Fu una pessima decisione.

Manning: Non posso credere che mi stia confessando proprio a te
Manning: Sono stato isolato per così a lungo. Volevo soltanto essere gentile, e vivere una vita tranquilla, ma gli eventi mi forzano a cercare nuovi modi per sopravvivere. Son abbastanza intelligente per capire cose succede, ma senza speranza per decidere cosa fare. Nessuno sembra accorgersi di me. [...]

Lamo: Quindi hai deciso di inviare i documenti?
Manning: Si
Manning: 260.000 in tutto. Erano tutti conservati in un server centrale.
Lamo: Qual è il tuo piano finale?
Manning: Sono già stati inviati a Wikileaks
Manning: E Dio solo sa cosa accadrà ora
Manning: Voglio che la gente sappia la verità. Senza informazioni, non si possono prendere delle decisioni consapevoli.

Il 26 maggio 2010 Adrian Lamo, chiuso il laptop, si diresse immediatamente verso l'FBI(*34) per mostrare l'intero log della chat. Nessuno sa quale fu la vera motivazione - se personale o coercitiva - ma questa azione portò, in pochi giorni, all'incarcerazione di Bradley Manning e a un processo che rischiò di vederlo condannato alla pena capitale per "attentato alla sicurezza nazionale". Ma quelle informazioni erano importanti. Talmente importanti che Julian Assange, dopo averle ricevute, verificate e selezionate, le inviò ai giornali più importanti che cominciarono a pubblicarle una dopo l'altra. In quei documenti era anche incluso un video(*35) registrato da un elicottero Apache che, nella New-Baghdad, mostrava dei militari mitragliare dall'alto civili inermi. Venne diffuso col titolo di "collateral murder" e in esso si vedeva inequivocabilmente che l'attacco fu un errore: i militari scambiarono un lungo obbiettivo fotografico per un RPG. Fra i bersagli dell'attacco vi erano uomini anziani, bambini, e due giornalisti della Reuters, Saeed Chmagh e Namir Noor-Eldeen.

Ma di errori accidentali in quella guerra ne furono commessi tanti. Come l'attacco al fosforo bianco - scoperto dai giornalisti italiani Torrealta e Ranucci - che nel novembre 2004 illuminò la notte dell'intera città di Falluja. Chi è dunque il colpevole? Chi rilascia informazioni classificate o chi commette crimini di guerra?

Gli androidi forse non sognano più

Mentre internet entrava nelle case di ognuno di noi e i personal computer diventavano oggetti di uso comune, stava avvenendo un'altra rivoluzione: internet diventava lentamente "da taschino". Ben prima di Iphone e Android, c'era Apple Newton(*36). Era il 1993 e la Apple sviluppò questa piccola serie di device costosissimi che permettevano, per la prima volta, di avere una funzione che sarebbe diventata popolare quale anno dopo: la HTR - Handwritten Text Recognition - ovvero la possibilità di poter

scrivere sullo schermo come si fa su un foglio di carta. Il device più popolare fra quelli della serie fu probabilmente il Messagepad, che utilizzava un linguaggio di programmazione proprietario per poter costruire le sue applicazioni interne. Fu considerato innovativo per quei tempi ma fu presto superato dai palmari che supportavano PalmOs(*37), per la loro semplicità d'uso e il loro aspetto pionieristico. In particolare, la versione 2.0 introduceva il supporto al TCP/IP, che quindi permetteva al palmare di potersi connettere alla rete internet. PalmOs divenne particolarmente popolare nella comunità hacker per un tool chiamato HackMaster(*38) che permetteva di installare applicazioni di terze parti per far fare al PDA di turno praticamente qualsiasi cosa fosse tecnicamente possibile. Fu un successo strepitoso e la comunità open source contribuì immensamente producendo tool e hack di ogni genere. Anche Symbian fece la sua parte in quel periodo e Nokia lo adottò come sistema operativo principale per i suoi device. Venne implementato, inoltre, il protocollo WAP(*39) che permetteva di accedere ad applicazioni, sistemi e pagine web scritte appositamente per essere visitate da piattaforma mobile.

Per tanti anni la situazione si stabilizzò e l'internet da taschino rimase qualcosa per pochi adepti. Arrivò il 2007 e da Cupertino in California, Steve Jobs stupì tutti con la presentazione dell'Iphone, un nuovo device(*40) che includeva al suo interno un telefono, un sistema per la navigazione internet e un'applicazione per ascoltare musica. Fu un enorme successo di marketing: migliaia si accalcarono davanti agli Apple Store e all'uscita di ogni nuovo modello si ripetevano le stesse scene di isteria. Sembrava quasi non si potesse vivere senza un Iphone. Nonostante lo stupore però tutto ciò era in qualche modo giustificato. Sembrava che il futuro avesse varcato la soglia del presente e fosse arrivato nelle case di tutti. Internet nel palmo di una mano, semplice e con il multi-touch. Ma internet non fu inventato con l'Iphone, come l'ascolto della musica non fu inventato con l'Iphone, come il GPS in mobilità non fu inventato con l'Iphone, come la fotocamera non fu inventata con l'Iphone, come il telefono non fu inventato con l'Iphone. Ma era quel sistema unico, tutto in uno, che stupì tutti.

Iphone divenne così popolare che tutti i big dell'informatica furono costretti a inseguire. Anche Microsoft ci provò, per poi fallire miseramente. E Google, da Mountain View, fece la sua mossa. Con una presentazione molto più scarna e molto più tecnica di quella fatta da Steve Jobs, nel 2007, con un video in low-res sul canale di Android-Developers, Sergey Brin e Steve Horowitz presentarono un sistema operativo open source basato su un kernel Linux modificato per piattaforme mobili. Si chiamava Android(*41) e veniva rilasciata una SDK sulla quale costruire le prime applicazioni.

Le parole "Linux" e "open source" fecero da specchietto per le allodole. La comunità XDA-developers cominciò a lavorare a fondo sul sistema e nacquero le prime ROM alternative, i primi sistemi di root(*42) per Android, le prime modifiche e le prime personalizzazioni. E mentre si giocava a scovare le vulnerabilità del sistema e si gioiva per un Linux arrivato sul mobile, ben pochi si accorgevano che stavamo assistendo all'evoluzione di un gigante dell'informatica che avrebbe cambiato il suo motto da "don't be evil" (non essere malvagio) a "do the right thing" (fai la cosa giusta)(*43). Chi avrebbe deciso cosa sarebbe stata la cosa giusta da fare resta oggi ancora da stabilire.

Twitter non è Rousseau

Quando nel 1762 Jean Jacques Russeau, filosofo francese e innovatore del pensiero politico, pubblicò il suo "Contratto Sociale"(*44), offriva la prospettiva di un ideale Stato democratico e l'idea che l'uomo fosse, per diritto di nascita, libero e non destinato alla schiavitù. Nella Francia dell'Ancient Regime, dove gli Stati Generali avevano mostrato quanto fossero estese crisi e povertà all'interno del regno, quelle idee fecero rapidamente presa nei circoli letterari. Guidati dai giacobini, il 14 luglio 1789 un gruppo di rivoluzionari si diresse verso la fortezza della Bastiglia(*45). Era cominciata la Rivoluzione Francese che avrebbe portato in poco tempo all'istituzione di una prima Costituzione e alla caduta della monarchia.

Nel corso dei secoli molte rivoluzioni sociali hanno intersecato il corso della storia. Ma quella che, in assoluto, ha richiamato l'attenzione dei media come la rivoluzione dei social, o meglio come la "twitter revolution"(*46) fu quella che avvenne in Iran nel 2009. Mahmoud Ahmadinejad, l'allora presidente iraniano, politico conservatore e benedetto dall'ayatollah Khamenei, correva per il suo secondo mandato. I suoi oppositori, Mousavi e Karroubi, progressisti e rappresentanti del Green Party, si opponevano alla sua rielezione e presentavano un programma riformatore basato sull'idea di riorganizzare il Paese in un'ottica laica, con supporto alle organizzazioni non governative, attenzione ai diritti umani, al miglioramento della condizione femminile, riforma scolastica e così via. Un bel sogno per quella terra che aveva vissuto i fasti sotto il regno di Persia. Gli osservatori internazionali avevano già segnalato irregolarità ben prima della tornata elettorale, ma quando arrivò il giorno, i risultati vennero forniti appena due ore dalla chiusura dei seggi e ciò apparve obiettivamente molto sospetto. La vittoria di Ahmadinejad generò malcontento nella popolazione, la quale cominciò a riversarsi nelle strade protestando contro il governo neo-eletto. Ma ci fu qualcosa di nuovo rispetto alle proteste che avevamo vissuto fino ad allora: le persone si coordinarono attraverso i social-media, e in particolare

attraverso twitter che permetteva di comunicare la protesta anche attraverso piattaforme mobile. L'unione dell'internet da taschino e dei nuovi social media fu un menu esplosivo. E lo stesso fenomeno si verificò parimenti giusto un anno dopo quando, dalla Tunisia, partirono una serie di rivolte che segnarono un evento globale, ricordato dalla storia col nome di "primavere arabe"(*47).

Ci fu però qualcuno che fece le pulci a quella rivoluzione, e in particolar modo ai tweet apparentemente partiti dall'Iran. Analizzando i dati(*48), l'istituto Sysomos si accorse che poco meno dell'1% dei tweet erano partiti dall'Iran, mentre la parte più ingente veniva da Europa, UK e USA. Questo era dimostrato non solo dalla geolocalizzazione degli account, ma anche dalla lingua con cui si tweettava. Gli account iraniani infatti comunicavano in Farsi - lingua comunemente parlata in Iran - mentre gli altri comunicavano in Inglese, come se i cittadini iraniani residenti all'estero stessero supportando i loro amici e fratelli che in patria lottavano per avere una democrazia compiuta. O forse c'era dell'altro? Evgeny Morozov nel suo libro "The Net Delusion"(#21) scrisse:

Nell'euforia collettiva che conquistò i media occidentali durante gli eventi in Iran, le voci in dissenso ricevettero molta meno attenzione di quella che ricevette la narrativa della twitter revolution. [...] Hamid Tehrani, editor di Global Voices scrisse "l'Occidente non aveva posto l'attenzione alla condizione iraniana, ma soltanto al ruolo che stava svolgendo la tecnologia"

Va sempre tenuto a mente infatti che l'equazione "internet, più tecnologia, più connessione, uguale più democrazia" è ideologicamente sbagliata. Se fosse vero che a più internet corrisponde più democrazia, con tutti gli strumenti in nostro possesso, con le interazioni, con le decine di social network che abbiamo a disposizione, avremmo già cambiato il mondo da un pezzo. Ma c'è sempre il fattore umano che ci si mette in mezzo. Ed è su quello che bisogna lavorare.

Riferimenti

(*1) https://www.thebalance.com/subprime-mortgage-crisis-effect-and-timeline-3305745
(*2) https://www.thebalance.com/lehman-brothers-collapse-causes-impact-4842338
(*3) https://bitcoin.org/bitcoin.pdf
(*4) https://www.investopedia.com/tech/were-there-cryptocurrencies-bitcoin/
(*5) https://www.coindesk.com/learn/bitcoin-101/how-to-store-your-bitcoins
(*6) https://tokeneo.com/5-largest-bitcoin-farms/

(*7) https://blockstream.info/

(*8) https://cointelegraph.com/tags/decentralization

(*9) https://www.newscientist.com/article/mg24933260-400-silk-road-review-the-true-story-of-the-dark-webs-illegal-drug-market/

(*10) https://www.linkedin.com/in/rossulbricht

(*11) https://arstechnica.com/tech-policy/2015/02/the-hitman-scam-dread-pirate-roberts-bizarre-murder-for-hire-attempts/

(*12) https://freeross.org/real-untold-story/

(*13) https://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085

(*14) https://smartech.gatech.edu/handle/1853/53595?show=full

(*15) https://www.theatlantic.com/technology/archive/2020/08/hacker-group-anonymous-returns/615058/

(*16) https://www.historyextra.com/period/stuart/guy-fawkes-gunpowder-plot-facts-bonfire-night/

(*17) https://mashable.com/2014/12/03/history-of-reddit/?europe=true

(*18) https://www.theguardian.com/technology/2013/may/16/lulzsec-hacking-fbi-jail

(*19) https://www.pcworld.com/article/141839/article.html

(*20) https://www.reddit.com/r/videos/comments/35nr6m/tom_cruise_scientology_video_original_uncut/

(*21) https://www.engadget.com/2014-12-16-pirate-bay-shutdown-explainer.html

(*22) https://en.wikisource.org/wiki/Pirate_Party_Declaration_of_Principles/2.0

(*23) https://piped.kavin.rocks/watch?v=EVM5-_fusjs

(*24) https://www.corriere.it/speciali/pasolini/ioso.html

(*25) https://www.propublica.org/nerds/happy-birthday-creative-commons

(*26) http://wi.mobilities.ca/crowdfunding-culture/

(*27) https://www.theguardian.com/media/2011/jan/30/julian-assange-Wikileaks-profile

(*28) https://cdn.muckrock.com/foia_files/2019/04/23/5._GSMR_Report_1989_RIF.pdf

(*29) https://watermark.silverchair.com/jjcmcom0420.pdf

(*30) https://wikileaks.org/gitmo/

(*31) https://www.standup4humanrights.org/en/declaration.html

(*32) https://wikileaks.org/wiki/Scientology_leaks_by_date

(*33) https://shadowproof.com/merged-manning-lamo-chat-logs/

(*34) https://www.theguardian.com/world/2013/jan/03/adrian-lamo-bradley-manning-q-and-a

(*35) https://piped.kavin.rocks/watch?v=5rXPrfnU3G0
(*36) https://www.wired.com/2013/08/remembering-the-apple-newtons-prophetic-failure-and-lasting-ideals/
(*37) https://www.theverge.com/2012/6/5/3062611/palm-webos-hp-inside-story-pre-postmortem
(*38) http://wiki.c2.com/?HackMaster
(*39) https://www.geeksforgeeks.org/wireless-application-protocol/
(*40) https://piped.kavin.rocks/watch?v=Lyx_va6f10s
(*41) https://piped.kavin.rocks/watch?v=1FJHYqE0RDg
(*42) https://source.android.com/
(*43) https://gizmodo.com/google-removes-nearly-all-mentions-of-dont-be-evil-from-1826153393
(*44) https://www.earlymoderntexts.com/assets/pdfs/rousseau1762.pdf
(*45) https://www.history.com/this-day-in-history/french-revolutionaries-storm-bastille
(*46) https://www.theatlantic.com/technology/archive/2010/06/evaluating-irans-twitter-revolution/58337/
(*47) https://www.history.com/topics/middle-east/arab-spring
(*48) https://web.archive.org/web/20100304085941/https://blog.sysomos.com/2009/06/21/a-look-at-twitter-in-iran/

Capitolo 5 - E le genti che passeranno

Dipendenti o Cittadini?

Nel novembre 2004 Beppe Grillo, noto comico italiano, nella postfazione al libro "Regime" scritto dal giornalista Marco Travaglio, annunciava:

"Nel prossimo spettacolo, ho deciso di fare politica anch'io. [...] Ora voglio abbinare i teatri e la rete, cioè Internet. Per fare politica senza intermediari, senza politici [...] Lancio un movimento politico che, tanto per cominciare, punta a smuovere un milione di persone. Lo chiameremo 'A furor di popolo' "

Un po' di storia. All'inizio del 2004 la Casaleggio Associati, azienda di web marketing, aveva contattato Beppe Grillo proponendogli l'apertura di un blog. Cavalcando l'indignazione sulla politica italiana tipica di quel periodo, avrebbero centrato la loro attenzione nel rappresentare quella parte del paese che vedeva la cosiddetta "casta(*2) dei politici" con il fumo negli occhi. La Casaleggio fu lungimirante: per farlo passare come movimento nato "dal basso", stimolò la creazione di gruppi chiamati "amici di Beppe Grillo" sulla piattaforma Meetup, che poi furono la base di partenza per quel partito che nel 2009 diventò "Movimento 5Stelle". La sua creazione da zero ricordava dunque molto la nascita di Forza Italia dai club Mediolanum, ma questa volta si agiva usando il web, piattaforma che aveva ancora la nomea di essere libera ed indipendente. Niente a che vedere con iniziative come il partito Pirata di cui abbiamo già parlato, nato davvero dal basso sulla base di un manifesto scritto a più mani.

Questa era una delle prime volte in cui si erano spostate le strategie di marketing dai vecchi media ai nuovi media. E ciò era di certo interessante ma allo stesso tempo molto pericoloso, perché vedeva lentamente la perdita di significato di quello che aveva voluto dire Internet fino ad allora, con il suo

background strutturatosi attorno al cyber-attivismo. Bisognava avere memoria lunga per ricordarselo, e in molti quella memoria, lentamente, era scomparsa. Fu in parole povere un esperimento ben riuscito, e quel laboratorio politico fu studiato e analizzato a fondo.

Oh My Barack

Uno dei primi politici che comprese come utilizzare internet e i social media per creare una estesa base elettorale, fu l'allora senatore dell'Illinois Barack Obama. Durante la prima candidatura alla presidenza degli Stati Uniti d'America, il suo team elettorale lanciò un tool chiamato MyBO - My BarackObama(*3) - che aiutò la creazione di gruppi di supporto ed eventi sul campo. La piattaforma ricevette una serie di critiche(*4) poiché dava accesso a informazioni piuttosto sensibili come indirizzi e dati anagrafici dei potenziali elettori. Come fosse *una sorta* di Facebook ma *all'esterno* di Facebook. Non è di certo un caso che uno degli strateghi delle presidenziali del 2008 fosse proprio Chris Huges, ex co-fondatore di Facebook, dalla cui esperienza probabilmente aveva importato tutte le dinamiche social. Sul suo blog(*5) infatti scrisse:

"La grandezza di questa comunità e il valore del suo lavoro è senza precedenti. Individui di oltre 50 stati hanno creato più di 35.000 gruppi e dato vita a più di 200.00 eventi in giro per il paese. [...] Non vi è dubbio quindi che questi eventi locali abbiano giocato un ruolo importante nella vittoria di martedì scorso [...]"

Simili dinamiche si ripresentarono nel 2012 quando Barack Obama corse per il suo secondo mandato. Questa volta la app aveva un altro nome: Obama For America(*6). Si registrarono circa un milione di persone e, per sincronizzare i profili degli utenti con i metadata presenti su Facebook, si era deciso di utilizzare la prima versione della "Facebook Graph-API"(*7) . Per chiarire meglio, una API è letteralmente un "pezzo di codice" appartenente ad una piattaforma che può essere richiamato da un altro sistema per invocarne alcune funzioni interne. Ma in questo caso c'era più di un problema.

Quel semplice pezzo di codice, in termini di privacy, era veramente un colabrodo. Sulla spinta delle critiche arrivate dai media, nell'aprile del 2015 Facebook fu costretta a fare una rapida correzione(*8) introducendo una prima modifica nella versione 2.0, e riducendo così di ben 50% i dati a cui la API poteva fornire accesso. Un miglioramento, certo, ma che mostrava in maniera palese ad un pubblico non tecnico che i metadati degli utenti erano la vera risorsa del social network blu.

Ma cosa aveva spinto Facebook a tornare indietro sui suoi passi e modificare la sua API?

Quel rimorso che cambia il mondo

Edward Joseph Snowden nacque nel luglio del 1983 negli Stati Uniti da una famiglia di umili origini. Seguendo le orme del nonno, ammiraglio presso la flotta navale e successivamente ufficiale del servizio segreto statunitense, lavorò prima presso la CIA e nel 2013 fu assunto come collaboratore esterno presso una struttura della NSA con sede alle Hawaii. Nel suo libro autobiografico "Permanent Record"(#22) Edward Snowden scrive:

"Quando l'ho conosciuto io, Internet era qualcosa di diverso. Era un amico, un genitore, era una comunità senza frontiere, una voce e milioni di voci. [...] Ma internet come lo conosciamo oggi è irriconoscibile, ed è diventato il risultato di un sistematico controllo dei pochi verso i molti"

Nel corso della sua permanenza nei servizi segreti statunitensi, Snowden venne a contatto con diverse tecnologie e diversi programmi che lo fecero ricredere sulle vere intenzioni della sorveglianza antiterrorismo. Nel 2007, internamente alla NSA, sollevò i suoi dubbi venendo ripetutamente ignorato. A suo parere si stava arrivando a controllare tutta la popolazione mondiale. I sistemi coinvolti andavano da motori di ricerca interni strutturati per intercettare comunicazioni private di liberi cittadini, fino a interfacce che permettevano di accedere a chat private, email, trasferimento dati, video conversazioni, dati dei social network e via dicendo. Da un sistema di sorveglianza che era, in passato, effettuato con tutte le tecniche possibili ma in via del tutto eccezionale, si era passati a uno spionaggio globale a cui tutti i cittadini del mondo erano soggetti, volenti o nolenti. Molto peggio quindi del vecchio Echelon, molto peggio di qualsiasi altro sistema conosciuto fino ad allora.

Internet aveva dato un enorme vantaggio competitivo a NSA e CIA le quali non si erano fermate davanti alle restrizioni della FISA - Foreign Intelligence Surveillance Act - ma avevano esteso le loro ricerche a un range globale. L'antiterrorismo, dunque, era diventato banalmente la scusa non per isolare i membri dell'Isis o di Al Quaeda(*9), ma per creare un archivio personale di chiunque fosse attivo sulla rete. I metadati erano diventati armi non convenzionali e non più strumenti tecnologici. Fu così che nel 2013 - dopo aver tentato invano di ammonire i suoi colleghi e i suoi superiori riguardo i rischi che si stavano correndo, e sul fatto che si stava contravvenendo ai princìpi stessi che stavano alla base della

costituzione degli Stati Uniti - Snowden prese qualche giorno di malattia per riprendersi da un nuovo attacco di epilessia e volò a Hong Kong per incontrare il giornalista Glenn Grenwald e la videomaker Laura Poitras(*10). Qui, in una stanza di un albergo, Edward Snowden rivelò la sua verità. Consegnò un archivio di dati che conteneva al suo interno sia informazioni classificate, sia un indice ben modulato e un glossario per permettere di ricercare quei documenti in maniera coerente. Scrive Greenwald nel libro "No place to hide"(#23):

"L'archivio fornito da Snowden era letteralmente immenso. [...] I programmi di sorveglianza erano strutturati per agire principalmente sul popolo americano, ma decine di Paesi nel mondo ne erano coinvolti. Paesi tipicamente alleati come Francia, Brasile, India e Germania erano affetti da questa indiscriminata sorveglianza di massa"

Quelle rivelazioni furono esplosive. Il Guardian e il New York Times uscirono in prima pagina con i primi documenti(*11), e nei giorni seguenti la notizia fece il giro del mondo. Questo mise in imbarazzo il governo degli Stati Uniti che, senza aspettare neanche un giorno, accusò Snowden di aver complottato contro la sicurezza nazionale, cosa che lo costrinse successivamente a fuggire in Russia dove chiese asilo politico.

Un anello per domarli tutti

Gli stati Uniti facevano parte di un consorzio internazionale chiamato "Five Eyes Alliance"(*12) di cui erano membri anche Regno Unito, Canada, Nuova Zelanda e Australia. Questo voleva dire che ogni partner del network poteva condividere con gli altri tutti i dati raccolti senza doverlo domandare per vie ufficiali. L'ammontare delle rivelazioni risultò enorme. Una analisi approssimativa, realizzata dall'allora direttore dell'NSA Keith Alexander, stimò una quantità di documenti trapelati che andava da 50.000 fino a circa 200.000.

I programmi di sorveglianza descritti erano innumerevoli. PRISM(*13) per esempio, probabilmente il più esteso di tutti, era capace di intercettare email, chat private, chiamate in voip, login e dettagli appartenenti ai dati presenti sui social network. In una presentazione in pdf condivisa sul Guardian dal giornalista Glenn Greenwald, si legge come molti service provider e compagnie dell'information technology collaborassero attivamente al tracciamento. Si va da Google, Yahoo, Facebook, Microsoft fino ad arrivare ad Apple. Nel sistema STORMBREW invece la NSA aveva accesso ai dati

direttamente dai cavi di fibra ottica, senza passare dai service provider, che lavoravano come autostrade attraverso le quali passavano le informazioni. XKEYSTORE(*14) invece era decisamente il più spaventoso. Si parla infatti di un potente front-end che raccoglieva tutti i metadati in maniera passiva e, attraverso un motore di ricerca non troppo dissimile da Google, permetteva di avere accesso a tutto l'archivio disponibile.

Immaginate quindi di essere un ufficiale e di dover tracciare una persona sospettata di terrorismo: attraverso le vostre indagini, secondo le rivelazioni diffuse da Snowden, potevate avere la possibilità di controllare una quantità di persone che arrivava a coprire l'intera popolazione mondiale. Tutto questo senza che la cittadinanza lo sapesse, con l'avallo del governo degli Stati Uniti e con la collaborazione delle grandi aziende del mondo IT.

Si capiva pertanto il perché della estrema opposizione dei governi per i sistemi di crittografia nelle comunicazioni e a qualunque strumento che permettesse di avere un minimo di privacy. XKEYSTORE tecnicamente lavorava su piattaforma RedHat e database Mysql, ed era talmente esteso che ben 700 server in oltre 150 siti erano sparsi per tutto il mondo. Non si pensi però che soltanto gli Stati Uniti avessero accesso a questo sistema. Dai dati condivisi da Snowden, ben quattro nazioni avevano avuto già avuto accesso a quella piattaforma: erano Germania, Svezia, Danimarca e Giappone.

Bisogna sottolineare inoltre che un programma non escludeva l'altro. Per raccogliere informazioni più dettagliate possibili, PRISM, XKEYSTORE, STORMBREW e altri erano usati contemporaneamente, e quando un addetto alla sicurezza dell'NSA aveva il permesso di fare una ricerca, questi risultavano strumenti importantissimi per intrecciare i metadati dei destinatari.

Mettiamo dunque il caso che il fine ultimo sia solo ed esclusivamente il terrorismo, e mettiamo il caso che sia del tutto legale, per scopi più o meno leciti, tracciare tutti cittadini alla ricerca di prove di reati che, forse, ha compiuto uno dei loro contatti. La domanda è: cosa succede se un sistema simile cade nelle mani di qualcuno che decide di utilizzarlo per altri scopi? Dicendolo con le parole di Snowden(*16):

"Dire che non mi interessa la privacy poiché non ho nulla da nascondere, è come dire che non mi interessa la libertà di espressione poiché non ho nulla da dire"

Chi di Brexit colpisce

Mentre nel mondo si discuteva di democrazia violata, in Scozia si svolgeva il referendum per l'indipendenza(*17) e negli Stati Uniti il presidente Obama correva per il suo secondo mandato(*18), sui forum 4chan cresceva quella che i media definirono successivamente l'alt-right(*19). Nata dai postumi della crisi economica del 2008, lentamente, prima sul web e poi nella vita reale, si era diffuso un sentimento di rivalsa nei confronti di quelli che venivano definiti i "poteri forti" e una volontà di tornare, culturalmente parlando, al passato. L'hub che connetteva tutti questi mondi era un sito americano chiamato Breitbart News(*20).

Nato nel 2007 dall'idea del giornalista Andrew James Breitbart, co-fondatore dell'Huffington Post(*21), fu rilevato nel 2012 da Steve Bannon dopo la morte improvvisa del suo fondatore. Da qui, Bannon trasformò quello che era esclusivamente uno dei punti di riferimento per la destra statunitense in un più grosso ed esteso punto di riferimento per tutte le destre del mondo. Coccolando le idee più becere come il suprematismo bianco, l'antisemitismo, l'omofobia e le cospirazioni a tutto tondo, Bannon creò un impero a cui cominciarono ad ispirarsi tutti i movimenti populisti che in quegli anni stavano vivendo il loro momento di splendore.

In Europa in particolare, dove la crisi dei sub-prime aveva attraversato l'oceano, nasceva un forte sentimento di euroscetticismo(*22) che lentamente attraversava tutti i confini nazionali. Partiti come l'UKIP nel Regno Unito, Front National in Francia, Alternative für Deutschland in Germania e Fratelli d'Italia in Italia rappresentano alcuni esempi delle destre nazionali che sfruttavano il momento di crisi economica e sociale per avanzare nei sondaggi. Nel Regno Unito in particolare, i Tory, tradizionale partito di destra liberale, vedevano calare la loro attrattiva nei confronti del partito fondato da Nigel Farage che proponeva l'uscita della Gran Bretagna dall'Unione Europea. Fu così che alla vigilia delle elezioni del 2015, David Cameron, allora primo ministro e leader del partito conservatore, promise agli inglesi un referendum sulla Brexit pur di raccattare qualche indeciso che, altrimenti, avrebbe votato per l'UKIP.

Il 23 giugno 2016 i cittadini britannici furono così chiamati alle urne: ben il 52% delle preferenze andò a favore dell'uscita(*23), interrompendo così, di fatto, il legame che il Regno Unito aveva stabilito fin dal 1973 con l'Unione. Fa di certo riflettere che il giorno dopo il voto, analizzando i dati forniti da Google Trends, la ricerca più popolare nel Regno Unito sia stata "cosa è l'Unione Europea?"(*24).

Facebook non ama Cambridge

Durante un'inchiesta avviata da Channel4, un importante canale televisivo inglese, Mark Turnbull, managing director di Cambridge Analytica dichiarava(*24):

"Non c'è nessun vantaggio nel puntare una intera campagna elettorale sui fatti. In sostanza è tutto basato sulle emozioni [...] Il grande errore che fanno i partiti politici è cercare di avere la meglio sugli argomenti invece di identificare il centro emozionale del problema"

Andiamo per gradi. Nel 2015 un data-scientist assunto dall'università di Cambridge venne ingaggiato da una azienda britannica denominata Cambridge Analytica. Il suo compito era semplice: produrre una app che riuscisse ad estrarre preferenze, likes e ogni informazione possibile dai profili presenti su Facebook. Lo scopo, da quello che gli era stato comunicato, era puramente accademico. Profilazione standard gli fu detto. E così Alexander Kogan lavorò al codice intitolandolo "This is your digital life"(*25). Se ben ricordate quello che ci siamo detti in precedenza, questa non era la prima volta che una API di Facebook veniva utilizzata per scopi elettorali, ma c'era un piccolo e non insignificante tassello da aggiungere. Dalle policy di Facebook, appena l'utente avesse ricevuto a schermo il risultato del suo test, se non espressamente specificato, i dati stessi avrebbero dovuto essere cancellati. Quando però Christopher Wylie, un contractor esterno che lavorava per Cambridge Analytica, li ricevette non li cancellò affatto, li trattenne nel database e cominciò, come si dice in gergo, a micro-targettizzare i profili interessati. Nella profilazione psicologica di 87 milioni di account(*26) - sì, 87 milioni - si sarebbe cercato anche di dividere i soggetti in micro gruppi a seconda degli interessi, categorie di appartenenza, preferenze politiche e non solo. L'idea era poter avere una base da cui partire per inviare messaggi personalizzati, in modo da ottenere il massimo risultato col minimo sforzo. Mentre programmatori e analisti lavoravano su linee di codice, dati e algoritmi, Alexander Nix(*27), il CEO di Cambridge Analytica, comandava tutta l'orchestra.

In ambito politico accadeva qualcos'altro. Nel 2015 stava per partire la campagna elettorale per la Brexit e Nigel Farage(*28), leader dell'UKIP e del progetto Leave.eu(*29), contattò il suo caro amico Steve Bannon. Quest'ultimo aveva appena rilevato Breitbart News ed era, guarda caso, membro del board di Cambridge Analytica. Non serve uno scienziato per fare la connessione: su indicazione di Bannon la compagnia di Alexander Nix si attivò subito per aiutare la campagna per l'uscita del Regno Unito

dall'Unione Europea. I risultati positivi dimostrarono che le strategie, anche se piuttosto truffaldine, di Cambridge Analytica erano efficaci e potevano funzionare alla perfezione. I metadati degli utenti erano diventati dunque non più soltanto oro digitale per Facebook ma anche per aziende di terze parti che li usavano a loro piacimento per influenzare gli andamenti politici. In fondo avere un sistema centralizzato da cui estrarre i dati, non avvantaggia l'utente finale ma soltanto aziende e governi che possono pescare con poco sforzo in un mare pieno di pesci. Fu soltanto attraverso una stupenda inchiesta dell'Observer(*30) e di Channel4 che si scoprì l'inganno, ma non prima di assistere ad un altro capolavoro di Cambridge Analytica: l'elezione alla presidenza degli Stati Uniti dell'allora imprenditore Donald J. Trump.

Il caveau dei controllori

William Gibson è uno degli scrittori che, nella storia della fantascienza, ha contribuito a plasmare quel genere letterario che chiamiamo cyberpunk. Spesso mi piace ripensare ai suoi panorami, alle sue descrizioni, ai suoi universi distopici, proprio perché meglio di altri era capace di farti respirare l'atmosfera di cosa per lui sarebbe stato il futuro. A volte - ma solo a volte - mi piacerebbe che il presente attuale fosse simile all'universo descritto da Gibson. Perlomeno in Chiba City(*31) se il tuo cervello era stato danneggiato da una micotossina, in qualche modo rientrare nella matrice non era esattamente così facile. Nel secondo capitolo di Neuromante(#24), fortunato libro della celebre "trilogia dello Sprawl", si può leggere:

"Cyberspazio. Un'allucinazione consensuale vissuta quotidianamente da miliardi di operatori in ogni nazione. Una rappresentazione grafica di dati estratti dagli archivi di ogni computer [...]"

Nel 2017 Julian Assange, il fondatore di Wikileaks, cominciò a far circolare una nuova serie di documenti. Una quantità immensa, sterminata, che costrinse Wikileaks a pubblicarli in più parti includendo una sorta di motore di ricerca interno per tracciare le parole chiave. Si trattava di documenti classificati che descrivevano, pagina per pagina, una serie di programmi che i servizi segreti statunitensi utilizzavano per introdursi nei devices dei cittadini inconsapevoli. Si andava dagli smartphone di Apple e Google, computer con Microsoft Windows a bordo, o addirittura SmartTv della Samsung. Erano inclusi anche tool per sistemi operativi come Linux o FreeBSD. L'archivio venne chiamato Vault7(*32) - vault come caveau - e il suo contenuto si rivelò letteralmente spaventoso. La pubblicazione avvenne in 24 parti, ognuna di esse con un nome in codice. Non è esattamente chiaro chi

abbia avuto accesso a quei documenti. Da indiscrezioni sappiamo che potrebbe essere stato un gruppo ben noto di hackers denominato "The Shadow Brokers"(*33) che, infiltrandosi nei computer degli "Equation Group"(*34) - un altro gruppo con non chiari collegamenti con CIA e NSA - avrebbe avuto l'accesso a quei dati.

Sappiamo anche che nel 2016, quando l'hack avvenne, vennero pubblicati una serie di samples sulla darknet che offrivano questi documenti sul mercato nero in cambio di bitcoin. Sappiamo anche che Edward Snoden dichiarò che l'hack poteva avere un link con i servizi segreti russi, mentre invece James Bamford, esperto in cyber-security, dichiarò alla Reuters che poteva essere stato addirittura un inside-job(*35) della NSA. Nessuno sa dunque cosa avvenne, tutto è davvero molto fumoso, ma di certo sappiamo due cose. La prima: i documenti rubati non erano recenti, ed erano datati a circa tre anni prima. La seconda: i documenti arrivarono certamente nelle mani di Wikileaks da fonti anonime. Era arrivato l'anno zero.

Year-Zero

Non era evidentemente la prima volta che Wikileaks era coinvolta in pubblicazioni di questo genere. Dal 2011, con l'inizio di SpyFiles(*36), Wikileaks aveva addirittura disvelato correlazioni fra aziende private e servizi segreti statunitensi. Nel 2015 per esempio, venivano diffuse informazioni riguardanti software creati dall'azienda tedesca Finfisher(*37) che agivano da backdoor per accedere da remoto ai sistemi. I tre tool agivano insieme per trasferire i dati dall'attaccato all'attaccante in forma criptata ed erano capaci inoltre di anonimizzare il traffico. La parte curiosa di tutta questa storia è che la cancelliera tedesca Merkel, una volta conosciuto l'interesse dell'intelligence USA a spiare le sue conversazioni, si mostrò indignata e cacciò dall'ambasciata americana in Germania un ufficiale della CIA(*38) coinvolto nella storia. Questo, letto con gli occhi di oggi, ha perlomeno il suono del ridicolo. Sappiamo infatti che proprio la Germania è stata una di quelle nazioni che hanno avuto accesso ed utilizzato quegli strumenti. Come dichiarò nel 2016 al senato americano James Clapper(*39), direttore della National Intelligence:

"In futuro i servizi di intelligence potrebbero usare l'internet delle cose per identificare, sorvegliare, monitorare e localizzare"

È una lunga lista quella diffusa da Wikileaks, ma proviamo a fare un po' di ordine.

***DerStarke**(*40)*: ideato per sistemi Mac, e capace di sopravvivere anche nel caso di formatti e si reinstalli il sistema. È strutturato per rimanere sul firmware ed è usato insieme ad altri due tool: NightSkyes, che agisce sullo spazio dell'utente, e SeaPea, che agisce direttamente sul Kernel. Viene utilizzato come strumento per interagire con la macchina remota ed eseguire codice.*

***Grashopper**(*41): piattaforma interna alla NSA, strutturata per creare malware per i sistemi Microsoft Windows. Ha la possibilità di rendere modificabili alcuni vecchi malware, editarli e aggiungere moduli predefiniti. La notizia dell'esistenza di questo tool era nota fin dai tempi della diffusione del leak contenente le mail del gruppo Hacking Team.*

***Hive**(*42): infrastruttura back-end in https usata per estrarre informazioni dal target per eseguire comandi da remoto. Da analisi tecniche effettuate pare non essere rilevabile in alcun modo.*

***Weeping Angel**(*43)*: ideato per essere installato sulle SmartTV della Samsung. Le caratteristiche principali son quelle di poter registrare audio e video da remoto all'insaputa dell'utente come una sorta di cimice spia. Originariamente pare essere stato prodotto dai servizi segreti inglesi, per poi essere modificato e migliorato da quelli statunitensi.*

***Scribbles**(*44)*: ideato per inserire dati, immagini, link invisibili e potenzialmente dannosi su documenti Microsoft Office. Se però lo stesso documento viene caricato con la suite LibreOffice oppure OpenOffice, il codice aggiunto risulta visibile in chiaro.*

***Archimedes**(*45)*: script capace di ridirezionare tutto il traffico interno della LAN verso un computer infetto e visualizzarlo su schermo da remoto.*

***Pandemic**(*46)*: script capace di modificare il codice di alcuni programmi pre-esistenti in modo da trasformarli in malware e diffonderli sull'intera LAN. Funziona su sistemi Microsoft Windows.*

***CherryBlossom**(*47)*: creato per prendere il controllo, modificare il firmware dei router, e ridirezionare l'intero traffico della LAN. Fra i modelli infettabili spiccano quelli della Motorola, Linksys, D-link e Belkin. Insieme ad altri due tool, il BrutalKangaroo che permette di creare una sotto-rete interna, ed*

Elsa che permette di estrarre il MAC address da ogni macchina connessa, è capace di selezionare il traffico in maniera intelligente.

***OutlawCountry**(*48)*: *script creato per essere installato su macchine Linux e capace di lavorare come modulo del Kernel. Modifica in backgroud il framework netfilter ed è capace di riscrivere on-the-fly the regole del firewall iptables.*

***BothanSpy**(*49)*: *script creato per estrarre informazioni, accessi, credenziali, addirittura chiavi GPG ed SSH da macchine Windows e inviarle direttamente a un server centrale controllato dall'NSA senza lasciare traccia sull'hard disk. GryFalcon ha le stesse identiche funzioni ma è invece strutturato per lavorare su macchine Linux.*

***Highrise**(*50)*: *tool installabile su piattaforme Android, capace di agire da proxy-sms, creando canali di comunicazione nascosti. Redireziona, in pratica, messaggi sms da un determinato target verso un altro predefinito dall'attaccante.*

***Aeris**(*51)*: *serie di script in python capaci di lavorare su sistemi posix - in altre parole Linux, FreeBSD e Solaris - modificando il codice sorgente di programmi installati sulla macchina. È capace di inviare l'output a una piattaforma remota e di modificare il tempo di trasmissione fra i pacchetti stessi.*

***CouchPotato**(*52)*: *tool capace di registrare immagini jpg e video avi da un device infetto - sessioni, utilizzo del browser, webcam e altro - da poi successivamente essere recuperati dall'attaccante.*

Se da un lato non c'era nulla di nuovo - i servizi segreti son noti per agire in tutti i modi possibili pur di arrivare ai loro scopi - dall’altro questo sollevava più di un problema. Qui non stiamo parlando più di sicurezza nazionale: qui parliamo di controllo globale. Il terrorismo era diventato un pretesto attraverso il quale effettuare un monitoraggio di massa senza precedenti. Ed era un precedente pericoloso: gli strumenti informatici si erano repentinamente trasformati in espedienti tecnici per bypassare leggi approvate attraverso processi democratici. Nel libro "The Wikileaks Files"(#25) scritto da Julian Assange c'è una interessantissima lista di politici spiati da parte degli Stati Uniti poco prima di incontri multilaterali come il G8 o il G20. Domanda retorica: non è forse anche questa una *questione di democrazia*? Non richiederebbe forse una *reazione* immediata da parte di tutti?

A proposito di democrazia

Come ci siamo già detti, quando nel 2016 si svolse la campagna elettorale statunitense, Donald Trump la affidò nelle mani di Steve Bannon(*53). Anche questa volta le tecniche di Cambridge Analytica la fecero ancora da padrone e la sfidante di Trump, Hillary Rodham Clinton(*54), fu attaccata pesantemente e senza sconti. Ma, ad un certo punto, avvenne qualcosa di nuovo che cambiò letteralmente l'andamento delle elezioni. Poco prima del voto infatti, Wikileaks pubblicò ben 30mila mail(*55) private provenienti dall'account personale della candidata democratica. Contenevano informazioni personali, dettagli su operazioni di copertura effettuate in Siria, pareri inopportuni sul secondo candidato democratico Bernie Sanders. Quando si avviò l'inchiesta inoltre, si scoprì che molte email - per errore? - erano state cancellate dal server primario. Questo, in periodo di elezioni, ebbe il suo effetto deflagrante sull'elettorato.

Nell'analisi realizzata da Secureworks, una azienda di sicurezza informatica, c'è il forte sospetto che, alla base del leak, ci fossero due gruppi di cyber-spionaggio russo: i CozyBear e i FancyBear. Partendo da questi presupposti, postulare che la Russia stesse cercando di sabotare le elezioni e che Assange stesse agendo su ordine di Putin, per i media fu davvero immediato. La verità è che ci son soltanto sospetti ma non certezze. Di certo però questo cambiò radicalmente il corso delle elezioni statunitensi, mettendo così in cattiva luce lo stesso fondatore di Wikileaks che, fino ad allora, era considerato come un eroe da buona parte dell'opinione pubblica. Ma Assange aveva fatto esattamente quello che avrebbe dovuto fare un comune giornalista: pubblicare e proteggere le fonti. Eppure, dallo stesso mondo della libera informazione, gli fu imputato l’errore imperdonabile di aver permesso ad una scheggia impazzita come Trump di andare al potere.

Vedo distopie di un mondo distopico: qui si cammina su un terreno scivoloso dove si richiede che libera stampa e libera espressione siano non più *diritti* fondamentali ma *poteri* che devono essere gestiti dall'alto.

Anche le API nel loro piccolo

Quando alla fine del 2019, nella provincia di Whuan, cominciò a diffondersi la ben nota pandemia dovuta al Sars-Cov-2(*56), si faticò a riconoscerla. La Cina ritardò la comunicazione delle informazioni, i governi presero provvedimenti senza troppa convinzione, e così il Covid-19 ebbe tutto il tempo per

diffondersi e mutare. L'11 marzo, quando fu chiaro a tutti che il problema era dannatamente reale e stava contagiando tutto il mondo, il WHO dichiarò finalmente la pandemia(*57). Fu soltanto allora che la politica cominciò - in attesa del vaccino - a mettere in atto provvedimenti come mascherine, lockdown e distanziamento sociale.

A pandemia annunciata accadde qualcosa di sorprendente: la maggior parte dei lavori inerenti al Covid-19 e l'isolamento delle varianti vennero pubblicati in modalità open access(*58) così da accelerare i tempi e diffondere rapidamente le informazioni. Questa fu una decisione straordinariamente razionale: dopo tanti errori, avevamo finalmente imparato dal passato. Poco meno di un anno dopo, i primi vaccini entrarono in fase di sperimentazione e si cominciò ad uscire - lentamente - da quella fase drammatica che sembrava non avere fine. Ma ci fu anche qualcos'altro e qui entra in campo, di nuovo, l'informatica.

Una delle richieste da parte della comunità scientifica fu come poter identificare rapidamente i contagiati(*59) in modo di impedire - o perlomeno rallentare - la diffusione del virus. La ragione era semplice: nonostante la mortalità fosse fortunatamente bassa, la curva del contagio continuava ad essere molto alta. Per questo e per molti altri motivi, il Covid-19 avrebbe potuto - se non identificato rapidamente - diffondersi a sette miliardi e mezzo di esseri umani. Una delle tante soluzioni proposte - si navigava ancora a vista - fu quindi una app per smartphone(*60) che permettesse di registrare e segnalare le persone infette con cui si veniva a contatto. Da parte del WHO vi erano vari modi per realizzarla: utilizzando protocolli aperti e decentralizzati come il DP3T(*61) , sviluppando magari una app in open source, rilasciando il codice sorgente su piattaforme come Github. Ma questo non avvenne affatto: ogni governo venne lasciato libero di scegliere se e come realizzarla privatamente.

C'era però ancora un piccolo problema da risolvere: come far parlare piattaforme diverse? Il nodo principale che gli sviluppatori si erano posti era che il sistema bluetooth fra Android e IOS - i sistemi operativi mobile più diffusi al mondo - aveva difficoltà nel trasferire informazioni in maniera coerente. Da qui la necessità di creare rapidamente un nuovo framework comune su cui lavorare. Google e Apple si attivarono subito e, a meno di un mese dalla dichiarazione della pandemia, rilasciarono la “Exposure Notification”(*62). Tramite questo documento di lavoro - veramente ben scritto devo dire - venivano fornite due API: una interna per l’utilizzo del protocollo bluetooth ed una per la conservazione e lo scambio dei dati covid fra differenti device. Era sicuramente un buon punto di partenza.

Ma la gente non la prese benissimo. I download di app realizzate per questo scopo oscillarono fra il venti e il 30% in molte nazioni ed inoltre, da analisi indipendenti, risultò che non tutti fra coloro che l'avevano scaricata avevano poi deciso di attivarla per il tracciamento. Questo non stupisce affatto: la democrazia è anche un *sistema di fiducia fra individui e istituzioni*, e quella fiducia, per averla in cambio, bisogna averla precedentemente guadagnata.

La risposta non è la censura

Durante il quadriennio di Trump, per un alieno in visita sulla Terra, non sarebbe stato facile comprendere cosa stesse davvero accadendo. Nei meandri di Reddit, un gruppo - i Qanon(*63) - cominciava a propagandare l'idea che il mondo fosse *dominato* da alcuni personaggi coinvolti in oscuri rituali satanici, legati fra loro nei cosiddetti "circoli della pedofilia", nottetempo bevitori di adrenocromo e dediti al rito della cabala. Lo scopo finale? Controllare il mondo per attuare il "nuovo ordine mondiale". Fa ridere già così senza aggiungere altro, ma in realtà c'è molto di più. Chi mise in giro queste deliranti bufale, si era quasi sicuramente ispirato ad un libro del 1999 scritto dal collettivo italiano Luther Blisset(*64) chiamato "Q" e al loro famoso libro/inchiesta del 2001 "Lasciate che i bimbi". Evidentemente però non c'è da stupirsi: esiste sempre una risposta semplice ad una domanda complessa - ma quasi sempre, purtroppo, è sbagliata(*65) -.

L'arrivo della pandemia, l'aggravarsi della situazione economica e l'ipotesi - mai dimostrata - che il Sars-Cov2 fosse stato diffuso *di proposito* dall'istituto virologico di Wuhan, aggregò rapidamente i sostenitori di idee *borderline* i quali identificarono in Trump una sorta di *soldato/eroe* in lotta contro il deep-state(*66). Il punto più alto di questo processo si ebbe proprio nel 2020 quando "The Donald" corse per il suo secondo mandato. La sua sconfitta - come prevedibile - fu di misura, sia nelle preferenze che fra i grandi elettori, ed allora, fra i sostenitori di Trump, cominciò a balenare l'idea del complotto: le elezioni erano state truccate e i voti postali manipolati(*67). Se ciò fosse rimasto sul web poco male. Invece, come avvenne nel caso pizza-gate(*68) - dove una fake-news si era trasformata in un evento reale - questo generò, durante il giorno dell'insediamento, il famoso attacco a Capitol-Hill(*69). Centinaia di supporter si recarono a Washington per ascoltare Trump che da un palco *sobriamente* dichiarò:

"Non vi riprenderete mai il nostro Paese con la debolezza. Dovete esibire forza e dovete essere forti [...] Se non combatterete come dannati, per voi non vi sarà più un Paese."

Ci furono 4 morti, 13 feriti, 52 arresti e una sensazione di spaesamento generale in tutta l'opinione pubblica. All'unisono Facebook, Twitter e Youtube censurarono Trump chiudendo il suo account(*70) e generando così una situazione senza precedenti. *Erano compagnie private, social network, o erano diventati repentinamente editori?* Questo creava un problema che aveva a che fare con l'ormai avvenuta centralizzazione di internet in mano a pochi monopòli: la democrazia degli stati cominciava a delegare parte della sua efficacia a *decisioni private* di *organismi privati*. Il web era cambiato fin troppo e noi, dall'esterno, avevamo partecipato alla sua evoluzione più come *spettatori* che come *attori principali*.

Riferimenti

(*1) https://www.disinformazione.it/regime.htm
(*2) https://www.ilfoglio.it/gli-speciali-del-foglio/2017/04/03/news/casta-stella-rizzo-lessico-antipolitica-m5s-grillini-128341/
(*3) https://www.nytimes.com/2008/11/09/technology/09iht-carr.1.17652000.html
(*4) https://blog.p2pfoundation.net/mybo-details-about-obama-campaigns-network-strategy/2008/11/19
(*5) https://web.archive.org/web/20081116004140/http://my.barackobama.com/page/community/post/chrishughesatthecampaign/gGxZvh/commentary
(*6) http://www.p2012.org/candidates/obamaorg.html
(*7) https://www.theguardian.com/world/2012/feb/17/obama-digital-data-machine-facebook-election
(*8) https://techcrunch.com/2015/04/28/facebook-api-shut-down/
(*9) https://since911.com/explore/history-isis
(*10) https://piped.kavin.rocks/watch?v=0hLjuVyIIrs
(*11) https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order
(*12) https://privacyinternational.org/learn/five-eyes
(*13) https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
(*14) https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data
(*15) https://twitter.com/snowden/status/947907576666185730?lang=en
(*16) https://news.arizona.edu/story/edward-snowden-compares-privacy-freedom-speech
(*17) https://www.bbc.co.uk/news/events/scotland-decides/results
(*18) https://www.bbc.co.uk/news/world-us-canada-20233064
(*19) https://arxiv.org/pdf/1905.02712.pdf
(*20) https://www.breitbart.com/

(*21) https://www.huffpost.com/

(*22) http://www.institutdelors.eu/wp-content/uploads/2018/01/euroscepticismoreurophobia-bertoncini-koenig-ne-jdi-nov14.pdf

(*23) https://www.jrf.org.uk/report/brexit-vote-explained-poverty-low-skills-and-lack-opportunities

(*24) https://piped.kavin.rocks/watch?v=cy-9iciNF1A

(*25) https://www.theguardian.com/uk-news/2018/apr/13/revealed-aleksandr-kogan-collected-facebook-users-direct-messages

(*26) https://www.spectator.co.uk/article/were-there-any-links-between-cambridge-analytica-russia-and-brexit-

(*27) https://www.forbes.com/sites/parmyolson/2018/03/20/face-to-face-with-cambridge-analytica-alexander-nix-facebook-trump/

(*28) https://invidious.tube/watch?v=cA3XTYfzd1I

(*29) https://web.archive.org/web/20160717183155/http://leave.eu/en/news/2016-06-26/a-new-epoch-begins

(*30) https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy

(*31) https://invidious.tube/watch?v=S89BHnaxULo

(*32) https://wikileaks.org/vault7/

(*33) https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/

(*34) https://www.csoonline.com/article/3178645/leaked-docs-suggest-nsa-and-cia-behind-equation-cyberespionage-group.html

(*35) https://www.reuters.com/article/us-intelligence-nsa-commentary-idUSKCN10X01P

(*36) https://wikileaks.org/the-spyfiles

(*37) https://www.dw.com/en/finfisher-spyware-preliminary-investigation-started-in-germany/a-18270876

(*38) https://www.reuters.com/article/us-eu-summit-idUSBRE99N0BJ20131024

(*39) https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper

(*40) https://wikileaks.org/vault7/document/DerStarke_v1_4_DOC/

(*41) https://wikileaks.org/vault7/document/Grasshopper-v2_0_2-UserGuide/

(*42) https://wikileaks.org/vault7/document/hive-UsersGuide/

(*43) https://wikileaks.org/vault7/document/EXTENDING_User_Guide/

(*44) https://wikileaks.org/vault7/document/Scribbles_v1_0_RC1-User_Guide/

(*45) https://wikileaks.org/vault7/document/Archimedes-1_0-User_Guide/

(*46) https://wikileaks.org/vault7/document/Pandemic-1_1-S-NF/

(*47) https://wikileaks.org/vault7/document/SRI-SLO-FF-2012-177-CherryBlossom_QuickStartGuide_SLO-FF-2012-170/

(*48) https://wikileaks.org/vault7/document/OutlawCountry_v1_0_User_Manual/

(*49) https://wikileaks.org/vault7/document/BothanSpy_1_0-S-NF/

(*50) https://wikileaks.org/vault7/document/HighRise-2_0-Users_Guide/

(*51) https://wikileaks.org/vault7/document/Aeris-UsersGuide/

(*52) https://wikileaks.org/vault7/document/Couch_Potato-1_0-User_Guide/

(*53) https://www.reuters.com/article/us-usa-trump-russia-cambridge-analytica-idUSKCN1IH36S

(*54) https://www.nationalreview.com/2016/10/hillary-clinton-nasty-corrupt-evil-crooked-ruthless/

(*55) https://www.theguardian.com/us-news/2016/nov/06/Wikileaks-emails-hillary-clinton-campaign-john-podesta

(*56) https://www.thelancet.com/journals/laninf/article/PIIS1473-3099(20)30641-1/fulltext

(*57) https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020

(*58) https://about.jstor.org/covid19/#:~:text=Expanded%20free%20access%20for%20participating,Archive%20and%20Primary%20Source%20collections.

(*59) https://www.aljazeera.com/economy/2020/6/30/indias-first-covid-19-vaccine-candidate-cleared-for-human-trials

(*60) https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7479586/

(*61) https://github.com/DP-3T/documents

(*62) https://www.google.com/covid19/exposurenotifications/

(*63) https://www.theatlantic.com/magazine/archive/2020/06/qanon-nothing-can-stop-what-is-coming/610567/

(*64) https://www.theartnewspaper.com/feature/was-qanon-america-s-most-dangerous-conspiracy-theory-inspired-by-italian-artists

(*65) https://www.newstatesman.com/society/2011/06/ask-simple-science-answer

(*66) https://journals.sagepub.com/doi/abs/10.1177/0032321720916604

(*67) https://abcnews.go.com/Politics/false-misleading-trump-team-claims-election-fraud/story?id=74179247

(*68) https://www.rollingstone.com/feature/anatomy-of-a-fake-news-scandal-125877/

(*69) https://www.washingtonpost.com/dc-md-va/2021/01/06/dc-protests-trump-rally-live-updates/

(*70) https://www.theguardian.com/us-news/2021/jan/11/opinion-divided-over-trump-being-banned-from-social-media

Capitolo 6 - Mi diranno che bel fior

Il concetto di responsabilità individuale

Piero Calamandrei fu una figura straordinaria per l'Italia. Giurista, professore universitario e antifascista, nel 1945 dopo la caduta del regime partecipò ai lavori della Costituente come rappresentante del Partito d'Azione. In un famoso discorso(*1) pronunciato nel salone degli Affreschi della Società Umanitaria a Milano disse:

"Però, vedete, la Costituzione non è una macchina che una volta messa in moto va avanti da sé. [...] perché si muova bisogna ogni giorno rimetterci dentro il combustibile; bisogna metterci dentro l'impegno, lo spirito, [...] la propria responsabilità."

Facciamo ora un esercizio di stile. Proviamo a sostituire la parola Costituzione con qualcos'altro e vediamo come suona:

"Però, vedete, la Democrazia Informatica non è una macchina che una volta messa in moto va avanti da sé. [...] perché si muova bisogna ogni giorno rimetterci dentro il combustibile; bisogna metterci dentro l'impegno, lo spirito, [...] la propria responsabilità."

Uno dei princìpi filosofici che nel corso del tempo mi ha permesso di vivere nella maniera più equilibrata possibile - con i miei tanti ma tanti limiti - è lo stoicismo(#26). Lo incontrai di straforo quando ero alle scuole, ma fu soltanto intervistando Massimo Pigliucci e seguendo il podcast di cui era conduttore - "Rationally Speaking" - che mi ci appassionai. Da quando Bertrand Russell, infatti, mi traviò sulla via dell'ateismo(*2) e Carl Sagan sulla via della scienza(#27) fu molto semplice per questa filosofia entrare a far parte della mia "famiglia di personalità multiple".

Lo stoicismo si fa risalire al 300 AC quando Zenone di Cizio, nella vecchia Atene, lo insegnava ai suoi discepoli nell'agorà. Immaginate di avere un bel giardino(*3) ricco di piante ed alberi. Per avere buoni frutti dovrete concimare il suolo e, contemporaneamente, recintare il giardino per metterlo al riparo da contaminazioni esterne. Nella metafora precedentemente descritta, fornita da Crisippo da Soli, i frutti rappresentano l'etica, il suolo la fisica e le recinzioni la logica. Ergo: le regole della natura forniscono il concime alle piante da cui nascono le regole etiche, ma per far sì che il nostro giardino cresca incontaminato e rigoglioso, dobbiamo proteggerlo con le regole della logica.

Restando centrati sul pragmatismo delle idee e sulla produttività delle nostre azioni, ne consegue che, nella nostra vita, risulti più utile concentrarci soltanto sugli aspetti che possiamo controllare direttamente. Credere, dunque, che il mondo sia una *cloaca maxima* - fatta di gente cattiva che trama alle nostre spalle - potrebbe essere anche vero, ma occupare la propria vita a parlarne senza far nulla di concreto per cambiare lo stato delle cose risulta tecnicamente una perdita di tempo. L'unico impatto che possiamo avere sul mondo che ci circonda è attraverso la nostra vita, il nostro esempio, le nostre azioni.

Ribaltiamo dunque il punto di vista: se i grandi big del mondo IT hanno preso il controllo, la responsabilità non è "loro" ma "nostra". Non è impossibile però operare un cambiamento: bisogna riprendere in mano i princìpi dei padri fondatori di internet e rimettere in moto un movimento dal basso.

Leggero come un Container

Avete in mente quelle immagini delle "server farm" con lunghi corridoi stipati da destra a sinistra, con tante lucine che si accendono e spengono come fossero alberi di natale? Bene, se pensate che a ogni "hard disk" corrisponda un solo server, beh vi sbagliate. L'informatica nel corso del tempo è diventata talmente leggera che a ogni pezzo di metallo attaccato a una scheda madre possono corrispondere decine o centinaia di sistemi che lavorano insieme. Si chiamano "macchine virtuali"(*4) e servono tecnicamente per ottimizzare le risorse. Tutto si basa sul principio dell'overbooking. Facciamo un esempio: per ogni volo, ogni compagnia aerea mette normalmente in vendita più biglietti di quanta sia la sua capienza totale. Questo si basa sull'assunto che, statisticamente, non tutti i passeggeri saliranno a bordo: alcuni cancelleranno il biglietto, altri arriveranno in ritardo e altri magari avranno contrattempi.

Se trasliamo lo stesso principio nel campo informatico, non sempre si utilizzeranno tutte macchine virtuali alla massima potenza. Conseguentemente, avremo un enorme risparmio di risorse e, cosa non di poco conto, un enorme risparmio economico.

Negli ultimi tempi inoltre, son nati sistemi trasportabili, diversi ma molto simili alle macchine virtuali, chiamati "container"(*5). Questi oggetti nascono per interagire col cuore del sistema operativo in maniera completamente diversa. Mentre la macchina virtuale utilizza un oggetto chiamato "hypervisor" per essere eseguita, il container ha un funzionamento innovativo. Viene eseguito infatti come una sorta di "applicazione" a sé stante che simula una macchina virtuale ma che è, nella sua essenza, molto ma molto più leggera. Per spiegarlo con un esempio forse più semplice, se io volessi eseguire l'applicazione "caffè", col modello macchina virtuale dovrei caricare dalle mura della casa ai fornelli della cucina, mentre col modello container basterebbe caricare la moka, l'acqua e il caffè in polvere.

Domanda: come mai un end-user dovrebbe interessarsi a tutto questo? Il concetto è semplice: se è vero che tutto è diventato leggero e parzialmente facile da realizzare, se un computer può far lavorare più sistemi operativi al suo interno, se si possono utilizzare le risorse in maniera intelligente, cosa mi vieta di costruirmi un sistema in casa(*6)? La pigrizia? Oppure il fatto che, secondo la vulgata popolare, il computer deve essere una sorta di giocattolino scintillante adatto ad eseguire operazioni? La risposta, come al solito, è nella conoscenza.

Un Pinguino per amico

In questo libro ho parlato molto, forse troppo, di Linux. Ma Linux non è "42"(*7), ovvero la risposta alla vita, l'universo e tutto quanto. Se escludiamo il fatto che, oggi come oggi, trovare un tutorial(*8) diventa semplice ed immediato attraverso una semplice ricerca sul web, il principio base che mi spinge a consigliarlo come sistema principale per le operazioni quotidiane è, diciamo così, la "condivisione delle idee". Tutto il movimento open source, val la pena reiterarlo, è prima di tutto una comunità di persone, e poi, successivamente, una modalità di pensiero dove le idee vengono scambiate, condivise, migliorate.

Per quanto riguarda le performance, la leadership di Linux è tutt'ora indiscussa. Più del 90% dei super-computer infatti gira su kernel Linux(*9), quasi la totalità dei servizi web e cloud girano su Linux. E allora come mai, nel campo dei personal computer non è così popolare? Le ragioni sono tante, ma due

sono quelle principali. La prima: i programmi più popolari sono spesso programmi proprietari e girano su piattaforma Mac e Windows. La seconda: quando un consumatore acquista un computer, di norma trova o Windows o Mac preinstallato, in barba ad ogni principio logico. L'essere umano è un "algoritmo biologico" e in quanto tale è restio ai cambiamenti. Una esperienza però che viene in aiuto a chi si avvicina a questo mondo sono i cosiddetti "Linux day", iniziative di dibattito pubblico organizzate ogni anno dai Lug(*10) - linux user group - in cui la comunità si attiva per fare condivisione e divulgazione informatica.

Spesso si sente dire che uno dei difetti di questo sistema operativo, in campo desktop, sia la cosiddetta "frammentazione". Troppe distribuzioni simili fra loro, troppi desktop environment(*11). Cioè tradotto: troppa possibilità di scelta. Ma questo è davvero un difetto o piuttosto un vantaggio? Poter scegliere, da quel che mi ricordo io, non è mai stato un simbolo di imperfezione. Anche se Ubuntu sembra essere su Distrowatch(*12) quasi sempre ai primi posti fra i download, non è di certo l'unico Linux disponibile. Ci sono distribuzioni dedicate al media editing, distribuzioni dedicate al gaming, distribuzioni dedicate ai dev-ops, distribuzioni come Arch basate sul principio del KISS - *keep it simple, stupid!* -, distribuzioni come Kali dedicate al penetration-testing(*13). In sostanza, ognuno può creare una sua distribuzione. Basta perderci un po' di tempo sopra, e provare. Tanto.

In un hackmeeting(*14) che si tenne a Bologna nel lontano 2002, in una delle tante conferenze, sentì menzionare, non ricordo più da chi, una cosa chiamata "democrazia del codice". Si diceva "se io ho una moneta, tu hai una moneta, e ce la scambiamo, entrambi avremo una moneta. Se tu hai una idea, io ho un'idea e ce le scambiamo, entrambi avremo due idee. Se tu hai una linea di codice, io ho una linea di codice, e le condividiamo, entrambi avremo due linee di codice". Condividere risorse e condividere conoscenze è esattamente quello che serve in una comunità dove gli "individui" - e non il "codice" - si fidano l'uno dell'altro.

Inoltre, se questo non bastasse, c'è da ricordare che distribuzioni come Tails(*15) o Qubes sono probabilmente la scelta "de facto" per tutti i "whistleblowers", cioè gli individui che, come Chelsea Manning o Edward Snowden, vogliono poter condividere informazioni riservate proteggendo certosinamente il loro anonimato. In campo proprietario non esiste nulla di simile. E forse non è esattamente un caso.

Raspberry oh my Raspberry

Da adolescente, una delle cose che mi divertiva fare di più era andare in discarica, recuperare pezzi di computer rotti, ripararli, ri-assemblarli e montarci su Linux. Vedere come era composto al suo interno un computer, lavorare sulle schede col saldatore mi ha insegnato molto, sopratutto sull'importanza di quello che stavo maneggiando. Ogni singolo pezzo aveva il suo ruolo come una sorta di orchestra, ed era bellissimo vedere qualcosa che prima non funzionava rimessa in sesto e pronta per tornare al lavoro. Quando arrivarono i portatili, ricordo la mia diffidenza. Mi dissi "i computer cominceranno a diventare come giocattoli, e più i device si rimpiccioliranno più sarà difficile ripararli". Avevo ragione.

La riduzione delle dimensioni, unita all'obsolescenza programmata, ha trasformato, nel corso del tempo, gli oggetti tecnologici in costosi strumenti di cui si comprende sempre meno il funzionamento e che bisogna inoltre cambiare spesso. Avendo fatto per anni didattica scientifica a bambini di elementari e medie, questo lo avevo identificato come un "problema di percezione". E quando qualche anno fa mi trovai davanti alla mia prima Raspberry-Pi(*16) ne fui talmente entusiasta che, da ambasciatore Stem quale ero, decisi di portarla nelle scuole associata al modulo "Astro-Pi".

La Raspberry-Pi altro non è che un computer a scheda singola, piccola come una tessera del bancomat, leggera ed espandibile a piacere con vari moduli. È una piattaforma straordinaria per giocare e sperimentare, da rendere, se fosse mai possibile, obbligatoria nelle scuole, troppo indirizzate al "fare" piuttosto che al "comprendere". Ho visto bracci robotici strutturati attorno ad una Raspberry-Pi, sistemi per il telecontrollo, emulatori di Spectrum e Commodore64(*17), sistemi per la domotica, progetti inviati sulla Stazione Spaziale Internazionale. Il momento storico pertanto è propizio: imparare non è mai stato così divertente e così alla portata di tutti.

Paranoid Android

Si, anche Android è open source, ma Google non è esattamente amante della privacy. Il progetto nacque, se ricordate, come qualcosa di sperimentale di cui fu fornita una SDK per cominciare a sviluppare applicazioni. Se comprare un telefono Android non vuol dire avere un sistema completamente open source, il progetto Android AOSP(*18) rimane ancora un progetto open source e questo va messo in conto. Su un telefono che monta Android troviamo anche qualcos'altro. Si chiamano Google Play Services(*19) e lavorano come librerie per le applicazioni che avete sul vostro telefono. Tutto è centralizzato da Google, e questo, nella vulgata popolare, sembrerebbe essere una certificazione

di sicurezza. Ma è davvero così? La quantità di applicazioni disponibili sullo store prodotta specificatamente per infettare gli smartphone è ancora incredibilmente alta e non sembra diminuire nel corso degli anni. C'è un metodo ben testato per verificare l'affidabilità di un programma: avere a disposizione il codice sorgente, poterlo leggere, poter analizzare esattamente cosa fa. E soltanto poche applicazioni sul Play Store sono open source(*20). Da Android "stock" sono derivate diverse versioni, un po' come è accaduto su Linux con Debian e RedHat. I differenti flavour si chiamano "custom ROM", sono open source, e si possono liberamente scaricare e installare sul vostro telefono. Il più popolare fra questi è certamente LineageOs(*21), secondo forse solo a Paranoid Android, ma evidentemente non sono gli unici: la maggior parte sono disponibili per quasi tutti i device in circolazione e sono, inoltre, estremamente stabili.

Una delle cose interessanti - forse la più interessante in assoluto - è che, flashando attraverso ADB(*22) il sistema operativo, potrete evitare di aggiungere i Play Services. Ciò vuol dire che, in pochi passaggi, con qualche trick, potrete essenzialmente "de-googlare" il vostro telefono. Una volta fatto questo, basterà scaricare F-droid(*23) , alternativa libera al più noto Play Store, e migrerete anche dal vostro smartphone ad una scelta libera, etica e completamente open source.

C'è un Mammut che gira nella stanza

Nel 2018, quando scoppiò lo scandalo Cambridge Analytica, ci fu una fuga generale da Facebook. L'azienda di Mark Zuckerberg fu accusata di non prestare attenzione alla privacy, di profilare gli utenti e di basare essenzialmente il suo business sui metadata. La vulgata popolare dice che essere online vuol dire essere necessariamente esposti al profiling. Ma questo non è vero: le alternative esistono. Nello stesso anno in cui ciò accadeva, nasceva un piccolo gioiello: si chiamava ActivityPub(*24) , era un protocollo aperto, decentralizzato e strutturato per connettere fra loro piattaforme sociali. L'idea fu talmente rivoluzionaria che il consorzio W3C lo inserì fra gli standard consigliati del web.

Due anni prima, Eugen Rochko, un programmatore tedesco di 26 anni, stufatosi della supremazia di Twitter e di Facebook, aveva deciso di lavorare sul codice sorgente di GNU-Social, il social network sviluppato dalla Free Software Foundation. Lo rese molto più user-friendly, ne pubblicò il codice su Github(*25), e diede vita ad un nuovo software chiamato "Mastodon". Questo fu, storicamente, il primo social network ad adottare il protocollo ActivityPub. Attorno a esso si sviluppò qualcosa chiamato il "fediverso"(*26), cioè una rete di social alternativa che permetteva, praticamente in maniera completa, di

rimpiazzare tutti i social network più popolari. Mastodon infatti si presentava come una alternativa a Twitter e Facebook, Peertube a Youtube, Funkwhale a Spotify, Pixelfed ad Instagram, Writefreely a Blogger, Lemmy a Reddit e così via. Tutti connessi fra loro, tutti interoperabili.

Per capire meglio di cosa si parla, c'è bisogno di spiegare qualcosa di importante: quelli elencati sono tutti software open source, e ogni "nodo" è una "istanza decentralizzata" che può comunicare con tutte le altre. Non esiste dunque un solo Mastodon, ma centinaia di istanze Mastodon che comunicano fra loro. Questo ha permesso, nel corso del tempo, la creazione di luoghi con un'attenzione ai diritti lgbt, altri all'open source, altri ai manga, all'attivismo politico, alla poesia e via discorrendo. In una rarissima intervista al podcast "Nothing but the Toot"(*27), Eugen Rochko dichiarò:

"Penso che il punto centrale di Mastodon sia quello di essere un attrezzo utile soltanto al vostro scopo. Non venite utilizzati da lui. [...] Non si viene interrotti dal miglior contenuto. Si vede soltanto ciò che si vuole vedere"

Ecco dunque come aveva risposto la comunità open source al capitalismo della sorveglianza: lavorando, giocando, divertendosi, e partecipando allo sviluppo di qualcosa di innovativo.

Gli Open Standard

In origine era Google Talk e si basava sul noto protocollo aperto XMPP. Poteva comunicare con le altre piattaforme, essere utilizzato da programmi esterni come Pidgin, utilizzare OTR per criptare le comunicazioni e via discorrendo. Un bel giorno però Google decise di migrare la piattaforma a Google Hangouts dove il sistema di comunicazione non era più basato su un open standard ma era diventato proprietario, codice chiuso, e chi s'è visto s'è visto. Vai a fidarti di Google(*28).

Gli open standard, cercando di essere più chiari possibile, sono "formati" liberamente utilizzabili da tutti senza alcuna licenza e sviluppati da gruppi di esperti riconosciuti dall'intera comunità attraverso un processo pubblico. Se leggiamo attentamente la definizione data dalla Free Software Foundation e dalla Open Source Initiative, potremo notare come siano, in alcuni dettagli, leggermente differenti, ma entrambe concordano sui due punti chiave: universalità e inter-operabilità. In un sistema globale come internet, utilizzare gli open standard dovrebbe essere sempre una scelta di default. Dovrebbe.

Andiamo però su un esempio concreto. Quando la Sun Mycrosystem acquistò la Star Division dal suo creatore, sviluppò un nuovo software il quale cercava di essere l'alternativa libera a Microsoft Office. Dopo qualche tempo, la Sun rilasciò parte di quel codice sorgente, rendendo così possibile la nascita di una comunità che sviluppò un fork chiamato LibreOffice(*29). Fu in quel periodo che gli sviluppatori si posero il problema di quali formati fossero conformi alla filosofia open source. Da quella riflessione pubblica nacque un formato, un "open standard" chiamato ODT, che oggi è l'unico universalmente accettato da tutti gli office editor.

Il mio discorso però - ormai ne avrete la nausea - non vuole porre l'attenzione soltanto sulle aziende high tech, che di certo hanno la loro grossa fetta di responsabilità. La scelta di scrivere un documento in un formato proprietario e non in un formato aperto, o di utilizzare un sistema chiuso in luogo di un sistema che rispetta gli open standard, è tutta nostra. Per uscire dall'empasse nella quale ci troviamo, bisogna insomma includere anche il parametro "responsabilità personale". È la comunità che accetta, non il sistema che impone.

Macchine che analizzano macchine

Nei moderni sistemi di automazione esiste un programma chiamato "agente" che agisce come un "demone" e che analizza, ad intervalli temporali molto brevi, le macchine per verificare se ci siano degli errori nel sistema. Da un banale errore di mancanza spazio su disco o di alta utilizzazione della cpu, ad errori magari più importanti come il malfunzionamento di un database, ogni errore viene registrato e inviato ai cosiddetti "monitoring tools", in modo tale che un amministratore di sistema possa fare una analisi accurata e se possibile trovare una soluzione. Il miglioramento di questi oggetti è stato così repentino che, nel corso del tempo, l'approccio degli amministratori di sistema è completamente cambiato. Mentre anni fa la reazione ad una allerta in severità primaria era generalmente:

"Tze. Che cosa ne vorrà mai sapere quel coso più di me che ho configurato il sistema?"

oggi invece la reazione è diventata più o meno così:

"Bisogna controllare! Chiamate i pompieri!"

Se è certamente vero che una macchina può realizzare operazioni in molto meno tempo che un essere umano, è anche vero però che questo crea un piccolo circolo vizioso. Umani che creano macchine per analizzare macchine, ed umani che si fidano di macchine che analizzano macchine. E se la perdita di empatia nella nostra società fosse proprio dovuta al fatto che tendiamo ad analizzare e valutare gli esseri umani sulla base delle performance invece che sulla base della loro umanità? Ho un vaghissimo sospetto: temo che la risposta sia affermativa.

Online oppure Onlife

Cosa significa essere vivi all'interno di un mondo dove la iper-connessione la fa da padrone? È questo che si è domandato il prof. Luciano Floridi e il suo team di ricerca presso l'Unione Europea con lo studio "The Onlife Manifesto"(*30). In un documento liberamente scaricabile in licenza creative commons(*31), i 13 membri del panel analizzano vari aspetti della società digitale, domandandosi se fosse possibile ripensare il concetto di umanità e democrazia, che significato abbia assunto il concetto di spazio pubblico, quali siano i cambiamenti necessari per affrontare il cambio dall'analogico al digitale, e sopratutto cosa significhi oggi la parola online quando, in realtà, siamo tutti connessi 24 ore su 24 senza disconnessione fra il reale e il virtuale.

Per chi come me ha più di 30 anni, si ricorderà di certo il suono inconfondibile che separava l'essere online dall'essere offline: era quello del modem(*32) che convertiva il segnale telefonico in un segnale digitale. Veniva chiamato il "suono della balena", ed era così significativo perché segnalava, metaforicamente, l'accesso ad un mondo dove tutto poteva accadere.

Floridi nella sua analisi, prova a dividere la storia in tre fasi. La prima: la "preistoria" dove non esisteva la tecnologia. La seconda: la "storia" dove cominciava ad esserci la tecnologia e la società dipendeva esclusivamente dall'approvvigionamento delle risorse primarie come cibo, acqua e fonti energetiche. Nella "iperstoria" invece - la terza fase - la tecnologia diventava la sorgente fondamentale a cui la società si approvvigionava per ottenere e processare dati ed informazioni, e da cui era diventata al tempo stesso dipendente. Questo è un passaggio fondamentale poiché vuol dire anche che, in altre parole, non si può fuggire da essa e bisogna cominciare a farci i conti non soltanto da un punto di vista umano, ma anche da un punto di vista politico e filosofico. Citando sempre Floridi:

"Fra 50 anni, i nostri profigli potrebbero guardare a noi come non tanto differentemente da come oggi noi guardiamo le tribù dell'Amazzonia. Ci vorrà ancora un po' per cominciare a capire le trasformazioni che stiamo attraversando, ma forse è arrivato il momento di cominciare a lavorarci sopra"

Le nostre società, le nostre democrazie, son diventate sempre più simili ad una griglia di computer interconnessi che ad una serie di linee tracciate sulla cartina geografica. Popoli e identità non sono più divisi come nel passato. Ecco perché oggi è importante più che mai stabilire nuove regole sociali. Attraverso le macchine e l'interconnessione, siamo diventati non più esseri umani ma post-umani. E i nuovi algoritmi che verranno, dovranno riflettere la nostra vecchia e forse ancora analogica umanità.

Etica ed Open Source

Era ancora il 2018, e durante l'amministrazione Trump, presso il confine fra gli Stati Uniti e il Messico si era appena innescata una tragedia umanitaria. La ICE - Immigration and Customs Enforcement - un reparto di polizia statunitense addetto al controllo del territorio, bloccava e separava dalle loro famiglie più di 3000 minorenni messicani(*33) che, illegalmente, avevano tentato di attraversare il confine fra il Messico e gli Stati Uniti. I soggetti fermati venivano posti in centri di detenzione dove, secondo i rapporti di Amnesty International, avvenivano maltrattamenti ed abusi di ogni tipo. Le proteste furono enormi e vennero anche, inaspettatamente, anche dalla comunità open source. Chef, una sorta di piattaforma creata per amministrare e gestire più macchine all'interno di uno stesso sistema, fece un accordo commerciale con la ICE.

Fra i vari tool più popolari che gli sviluppatori utilizzavano per aumentare le potenzialità di Chef, ce n'era uno chiamato Chef Sugar(*34) creato dall'ingegnere Seth Vargo, e disponibile in licenza Apache. Quando si seppe che la compagnia Chef aveva preso accordi direttamente con la ICE, Seth rimosse il suo codice sorgente da github, affermando di non voler prendere più parte ad una violazione dei diritti umani così evidente come stava trapelando dagli organi di stampa.

Si era appena aggiunto un tassello importante: la responsabilità e l'etica del software. Sull'onda di quella protesta nacque prima il movimento NoTechForICE(*35) e successivamente qualcosa di completamente nuovo: la "Hippocratic License"(*36). Basandosi sul ben noto principio di Ippocrate "primum non nocere", la licenza ippocratica altro non era che un tentativo, molto ma molto imperfetto,

di riscrivere le regole della licenza open source MIT includendo al suo interno il principio etico. Si legge infatti:

"Il software non può essere utilizzato da individui, corporazioni, governi che sono attivamente noti per mettere in pericolo, danneggiare individui o gruppi meno privilegiati mentalmente, socialmente o politicamente"

Questo però, invece che risolvere il problema, ne aggiungeva altri. Era la Hippocratic una licenza open source? Certamente no(*37) perché non rispettava gli standard della definizione di open source. Era una licenza equa? Certamente no perché poneva dei paletti di utilizzo soltanto se si mettevano in pericolo gruppi o individui non privilegiati. Cosa accadeva se invece si mettevano a repentaglio le vite degli individui privilegiati? I diritti e l'etica del software valevano solo per alcuni e non per altri? E sopratutto, come si potevano introdurre all'interno di una licenza d'uso concetti così volatili come il bene e il male? Insomma i dubbi e le incertezze erano tante, ma la discussione era finalmente aperta: open source, da solo, non bastava più.

Come è potuto accadere

È da tempo che mi pongo questa domanda. Ormai faccio parte di questa community da più di vent'anni e, guardando indietro, ricordo molto bene di esserci entrato non per la bellezza del codice sorgente ma per la bellezza delle idee proposte. Tutta la comunità che si sviluppò attorno a Linux, e il movimento open source da cui proveniva, davano un senso a quello si faceva. I "lug" erano un posti accoglienti dove incontrare persone, imparare, scambiarsi idee, sognare un futuro migliore. La mia anima è ancora a Genova in quel lontano 2001 e a quegli hackmeeting che riunivano i migliori disadattati - già, oggi si chiamano nerd - che ho conosciuto in vita mia. Quando Redhat diventò commerciale(*38), quando Microsoft comprò Github(*39), quando la Linux Foundation mostrò il suo annual report da un Mac(*40), mi domandai cosa fosse andato storto. Forse l'open source era stato abbracciato da tutti - corporation e non - semplicemente perché era un modello più efficiente per fare business? In fondo Google, Facebook e Amazon, tanto per fare tre nomi a caso, hanno abbracciato il modello open source fin dall'inizio e non se la passano poi tanto male. Ma cosa c'è di male nel far business? Nulla, se soltanto la ricchezza fosse redistribuita. Cosa c'è di male a incamerare metadati? Nulla, se soltanto fossero usati per uno scopo decente.

E a questo punto sento la voce dei miei amici coder e sysadmin dietro le mie spalle: "io sono soltanto un programmatore, faccio codice, mi occupo di algoritmi, aggiusto cose, a ognuno il suo". Ecco, forse oggi questo non basta più. Se il concetto di responsabilità personale ricade di certo sull'utente - che scegliendo o non scegliendo un prodotto può fare la sua fortuna - lo stesso concetto dovrebbe ricadere anche su chi produce codice. In una conferenza del settembre 2020, Tobie Langel, attualmente consulente per la OSI Foundation, dichiarò(*41):

"Nessuno si sente a suo agio in questo tipo di conversazioni. La maggior parte dei professionisti dell'open source arriva da un tipo di cultura in cui l'unica cosa che davvero conta è essere capaci di modificare brillantemente il codice che essi sviluppano"

In fondo sarebbe come chiedere a Enrico Fermi di non partecipare al progetto Manhattan perché quelle sue conoscenze sull'energia nucleare avrebbero potuto aiutare a distruggere migliaia di vite. Ma lui faceva fisica mica politica. O forse le due cose son meno scollegate di quel che si possa pensare?

E ora?

Ricordo tempo fa di aver letto alcune riflessioni che Aaron Swartz aveva pubblicato sul suo blog. Erano una serie di articoli che descrivevano la necessità di avere nel web più sistemi come Wikipedia(*42). Non una sola quindi ma tante che replicassero la sua esperienza online. Ai tempi non avevo capito esattamente cosa volesse dire. Pensavo: non ne basta una se funziona bene? Siccome son lento di comprendonio, ci sono arrivato soltanto 15 anni dopo. Swartz parlava di due cose fondamentali: di comunità e di sopravvivenza. Se Wikipedia era di certo un brillante esempio di come costruire una comunità attorno a un progetto, non lo era invece di come costruire un progetto partendo da una comunità. Stava, in altre parole, parlando di un sistema verticistico che, senza dubbio alcuno aveva sempre funzionato nella storia dell'umanità, ma che il web aveva anche - nel suo statuto non scritto - l'imperativo di superare. Wikipedia inoltre rappresentava un sistema unico nel suo genere: cosa fare se fosse crollata? Da dove ripartire? Da qui la necessità, diceva Swartz, di avere più comunità, più Wiki e più progetti.

Ed è esattamente sulla responsabilità che vorrei centrare questi ultimi stralci di scrittura. Nel corso degli ultimi anni, dopo gli scandali di Cambridge Analytica, le rivelazioni di Snowden, i dati rilasciati pubblicamente da Wikileaks, si è sviluppato un importante dibattito che ha portato gli argomenti della

privacy online finalmente alla ribalta. Il libro della Zuboff ha inoltre contribuito a delineare il quadro all'interno del quale si sono sviluppati questi cambiamenti. Anche l'Unione Europea ha dato un aiuto alla comprensione del fenomeno attraverso lo studio multidisciplinare di cui abbiamo parlato in precedenza. Poi l'etica è entrata a gambe tese all'interno dell'ambiente open source con una discussione che, prima di allora, era considerata un'eresia. Cosa sta succedendo? Sta davvero cambiando qualcosa?

Quando circa 3 anni fa aprii il mio account su Mastodon(*43), in fuga a gambe levate da Facebook, cominciai a incontrare tanta bella gente che avevo letto e da cui avevo tratto ispirazione nel passato.

Aaral Balkan(*44) per esempio, come lui stesso si definisce un “cyborg-activist”, sono anni che batte sullo stesso punto: bisogna che la comunità lavori e incentivi lo sviluppo dello "small web" in contrapposizione a quello realizzato dai giganti dell'informatica. Lo small web, in quanto piccolo e personale, può essere gestito da individui e non da aziende, e in quanto tale può permettersi il "lusso" di rispettare alti standard di privacy, sicurezza ed etica. Ma ricavarsi una nicchia serena dove tutto funziona è una alternativa già vista nel passato. Bisogna anche agire sulla politica, sui regolatori, altrimenti è solo un gioco sterile a costruirsi una nuova bolla graziosa e colorata di arcobaleno.

Cory Doctorow invece - scrittore di fantascienza, attivista, blogger e podcaster - spinge il cuore oltre l'ostacolo. Nel suo ultimo libro "How to Destroy Surveillance Capitalism(#28)" propone di rompere i monopoli delle bigtech per ristabilire un equilibrio fra coloro che creano la rete - programmatori, amministratori, sviluppatori e, in generale, aziende IT - e fra coloro che utilizzano la rete. In questo modo, dal suo punto di vista, si impedirebbe ai vari Google, Amazon, Facebook e via discorrendo, di avere un controllo monopolistico dei metadati, attualmente centralizzati e in mano a pochi hub. Ma per fare questo basterebbe un attivismo militante di utenti consapevoli, che "sanno scegliere" e che non "si fanno scegliere", che collaborano alla formazione di una internet nuova e libera, che non subiscono passivamente il fascino della nuova applicazione del momento. È qui che i sistemi decentralizzati vincono su quelli centralizzati: ogni singolo fa le sue scelte personali, le integra, collabora, migliora e arricchisce l'intero sistema.

Bisogna, insomma, percorrere una strada che ha però due biforcazioni. La *prima*: la comunità deve sviluppare e *proporre nuove alternative* basate sull'open source, la privacy, gli open standard, la decentralizzazione e il creative commons. La *seconda*: la politica deve recepire questa richiesta dalla

base militante e *attuare un cambio a livello legislativo*. Abbiamo oggi circa 50 milioni di oggetti connessi su internet che comunicano fra loro, 4 miliardi di utenti registrati(*45) e circa 42 terabyte di dati scambiati. *Questa nuova rivoluzione digitale oggi non è più rimandabile*.

Riferimenti

(*1) https://www.filodiritto.com/piero-calamandrei-discorso-sulla-costituzione

(*2) https://www.theatlantic.com/personal/archive/2009/01/the-teapot-analogy/55930/

(*3) https://medium.com/the-sophist/toward-stoicism-3-0-694f2fbf6e41#:~:text=Chrysippus%2C%20one%20of%20the%20f oundational,must%20be%20rich%20and%20fertile.

(*4) https://www.networkworld.com/article/3583508/what-is-a-virtual-machine-and-why-are-they-so-useful.html

(*5) https://www.docker.com/resources/what-container

(*6) https://docs.nextcloud.com/server/latest/admin_manual/installation/source_installation.html

(*7) https://invidious.tube/watch?v=5ZLtcTZP2js

(*8) https://ryanstutorials.net/linuxtutorial/

(*9) https://www.top500.org/statistics/sublist/

(*10) http://www.linfo.org/lug.html

(*11) https://www.xfce.org/about/tour416

(*12) https://distrowatch.com/index.php

(*13) https://www.kali.org/docs/introduction/what-is-kali-linux/

(*14) https://www.hackmeeting.org/hackit02/programme.html

(*15) https://www.techrepublic.com/article/getting-started-with-tails-the-encrypted-leave-no-trace-operating-system/

(*16) https://www.zdnet.com/article/what-is-the-raspberry-pi-4-everything-you-need-to-know-about-the-tiny-low-cost-computer/

(*17) https://www.thegeekpub.com/13651/raspberry-pi-commodore-64/

(*18) https://source.android.com/

(*19) https://support.google.com/googleplay/answer/9037938?hl=en

(*20) https://ethical.net/technology/what-is-open-source-software-a-definition-history-of-oss/

(*21) https://download.lineageos.org/

(*22) https://developer.android.com/studio/command-line/adb

(*23) https://f-droid.org/en/docs/

(*24) https://www.w3.org/wiki/ActivityPub

(*25) https://github.com/tootsuite/mastodon

(*26) https://fediverse.party/

(*27) https://soundcloud.com/jackdaw-ruiz/nothing-but-the-toot-eugen-interview

(*28) https://www.disruptivetelephony.com/2015/02/google-finally-kills-off-googletalk-and-XMPP-jabber-integration.html

(*29) https://www.libreoffice.org/about-us/libreoffice-timeline/

(*30) https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/Manifesto.pdf

(*31) https://library.oapen.org/handle/20.500.12657/28025

(*32) https://invidious.tube/watch?v=ckc6XSSh52w

(*33) https://www.bbc.co.uk/news/world-us-canada-44503514

(*34) https://web.archive.org/web/20180922082549/https://github.com/sethvargo/chef-sugar

(*35) https://scienceforthepeople.org/no-tech-for-ice/

(*36) https://firstdonoharm.dev/

(*37) https://opensource.org/docs/osd

(*38) https://www.redhat.com/en/blog/rhelvolution-brief-history-red-hat-enterprise-linux-releases-early-days-rhel-5

(*39) https://news.microsoft.com/announcement/microsoft-acquires-github/

(*40) https://www.fudzilla.com/news/44524-linux-foundation-president-uses-apple-os

(*41) https://www.mind.be/fosdem20/2020-02-02-ethics.html

(*42) https://web.archive.org/web/20130119170037/www.aaronsw.com/weblog/morewikipedias

(*43) https://fosstodon.org/@jolek78

(*44) https://small-tech.org/about/

(*45) https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

Manifesto

Internet è come la democrazia: perché rimanga libero bisogna lottare ogni giorno.

Serve promuovere protocolli di sicurezza che tutelino la privacy degli utenti finali.
Serve che la comunità open source si apra al mondo dei non addetti ai lavori.
Serve promuovere gli open standard e il creative commons.
Serve responsabilità personale e conoscenza.
Serve divulgazione informatica.
Serve coraggio.

Serve politica.

GLOSSARIO

algoritmo : sequenza di operazioni utilizzata per risolvere un problema
anarchia : ideologia basata sulla liberta individuale - contrapposta al potere precostituito
apache : server web in licenza open source
api : pezzo di codice che permette a due piattaforme di comunicare fra loro
arpanet : sistema di comunicazione globale - per uso militare - pre-internet
backup : sistema di salvataggio dati - di norma fatto su uno storage esterno
basic : uno dei primi linguaggi di programmazione
bbs : server centrali a cui connettersi per utilizzare servizi - internet prima del www
blog : weblog - diario online
browser web : programma informatico ideato per la navigazione su internet
c : linguaggio di programmazione
chat : sistema di comunicazione fra utenti realizzato attraverso diversi protocolli
citizen science : sistema partecipativo di raccolta dati scientifici attraverso la comunità di appassionati
net neutrality : indipendenza delle idee su internet
cms : strumento per la creazione di contenuti sul web
community : comunità - spesso utilizzato per descrivere un gruppo di persone su internet
computer : elaboratore elettronico
console : interfaccia comandi via terminale
cookies : sistema di tracciamento attraverso un sistema di comunicazione fra sito web e browser web
copyright : pratica creata per impedire di distribuire e modificare materiale proprietario
copyleft : pratica creata per distribuire e modificare materiale senza licenza proprietaria
crosslink : link reciproco fra siti web
cut & paste : copia ed incolla, spesso usato nell'accezione di assenza di verifica

cyberpunk : sottogenere della fantascienza - futuro tecnologico e distopico
cypherpunk : movimento proveniente dal cyberpunk focalizzato sul rispetto della privacy
dark web : parte di internet nascosta, accessibile attraverso un apposito software
dark web : parte profonda del deep web
database : sistema di archiviazione ed estrazione dati in strutture logiche
dataismo : società tecnologica basata sull'uso dei metadata
deep web : web non indicizzato dai motori di ricerca
distopia : contrario di utopia - altamente negativo
dotcom : gergo usato per descrivere le aziende che operavano su internet all'inizio degli anni 2000
e-mail : sistema di invio e ricezione di posta elettronica
exif : metadata contenuti all'interno di una immagine digitale
fft : trasformata veloce di furier - algoritmo matematico
file : contenitore di dati in formato digitale disponibile in diverse estensioni
filter bubble : accesso costante alle stesse fonti di informazione
forum : piattaforma online per discussioni - su web
free software : programma informatico rilasciato con licenza open source
freenet : rete nel dark net - vedere deep web e dark web
ftp : protocollo per lo scambio file
geek/nerd : utilizzato per identificare persone interessate ad argomenti tecnologici
gnu/linux : sistema operativo basato sul kernel linux
gopher : navigazione internet da terminale - internet prima del www
gui : graphical user interface - interfaccia grafica
hacker : persona appassionata che ama approfondire un argomento nel dettaglio
hard disk : disco fisso dove risiedono i dati macchina
hardware : elettronica con cui è composto un qualsiasi oggetto elettronico
high-tech : tecnologia avanzata, usato spesso in associazione con azienda
html : linguaggio di programmazione
i2p : rete nel dark net - vedere deep web e dark web
iaas : interface as a service
internet : sistema di comunicazione globale - per uso civile
interprete : esecutore di operazioni a partire da un determinato linguaggio di programmazione
irc : protocollo utilizzato per chat in stanze e canali

java : linguaggio di programmazione
javascript : linguaggio di programmazione
kernel : cuore del sistema operativo destinato a comandare tutti i processi macchina
laptop : computer portatile
leak : perdita - gergo tecnico per definire una fuga di notizie
linux : kernel derivato da unix - vedere le voci kernel e gnu/linux
linux live : particolare distribuzione linux che non salva i dati sul disco fisso
lisp : linguaggio di programmazione
mailing list : piattaforma online per discussioni - via email
metadata : insieme di dati provenienti da altri dati e strutturati in maniera gerarchica
motore di ricerca : sistema complesso di immagazzinamento ed estrazione dati provenienti dal surface web
mysql : database in licenza open source
news feed : usato per descrivere il sistema di aggiornamento proveniente da fonti rss
newsgroup : simile ad email ma con possibilità di inviare e ricevere ad un gruppo di indirizzi
newsletter : sistema elettronico di comunicazione attraverso e-mail
nickname : nome identificativo principalmente utilizzato online
offline : non in rete - fuori da internet
onlife : termine coniato per rappresentare la tendenza a vivere su internet
online : in rete - su internet
open access : sistema di fruizione e distribuzione gratuita di contenuti
open publishing : vedere open access
open source : sistema di condivisione aperta del codice sorgente
oracle-db : database prodotto dall'azienda oracle
p2p : peer to peer - infrastruttura con scambio dati fra pari
paas : platform as a service
paper : carta - termine spesso utilizzato nell'accezione di pubblicazione scientifica
perl : linguaggio di programmazione
personal computer : elaboratore elettronico da scrivania
php : linguaggio di programmazione su web in licenza open source
podcast : contenuto audio distribuito sul web
policy : regole presenti in una determinata community

porta : strumento attraverso il quale comunicano sistemi attraverso determinati protocolli

postgresql : database in licenza open source

privacy : riservatezza - termine indicato in analogia con la sicurezza online

profiling : profilazione degli utenti attraverso i metadata

prosumer : utente che fruisce e fornisce contenuti su internet

protocollo : tipo di comunicazione effettuato fra differenti sistemi

python : linguaggio di programmazione

rss : formato di distribuzione contenuti sul web

saas : software as a service

server farm : luoghi chiusi dove son contenuti computer server

sistema operativo : sistema di gestione hardware e software incaricato di far funzionare la macchina

sito web : struttura informatica contenente un server web navigabile attraverso un browser

BIBLIOGRAFIA

Libri presenti e citati

#1 WWW - Robert J. Sawjer

#2 Talking to my Daughter - Yanis Yarufakis

#3 The Age of Surveillance Capitalism - Shoshana Zuboff

#4 The Cathedral and the Bazar - Eric S. Raymond

#5 The Rise and Fall of Shawn Fanning's Napster - Joseph Menn

#6 Just For Fun: The Story of an Accidental Revolutionary - Linus Torvalds

#7 Free as in Freedom - Richard Stallman

#8 No logo - Naomi Klein

#9 The Medium is the Massage - Marshall McLuhan

#10 Wikinomics - Don Tapscott

#11 The Cult of the Amateur - Andrew Keen

#12 Who Controls the Internet - Jack Goldsmit & Tim Who

#13 The Art of Invisibility - Kevin Mitnik

#14 A Good Old Fashioned Future - Bruce Sterling

#15 Weaving the Web - Tim Berners Lee

#16 Being Digital - Nicholas Negroponte

#17 Homo Deus - Yuval Noah Harari

#18 Future Shock - Alvin Toffler

#19 Enlightenment Now - Steven Pinker

#20 Too Big to Fail - Aaron Sorkin

#21 The Net Delusion - how not to liberate the world - Evgeny Morozov

#22 Permanent Record - Edward Snowden

#23 No Place to Hide - Gleen Greenwald

#24 Neuromancer - William Gibson

#25 The Wikileaks Files - Julian Assange

#26 How To Be a Stoic - Massimo Pigliucci

#27 Cosmos - Carl Sagan

#28 How to Destroy Surveillance Capitalism - Cory Doctorow

Libri consigliati

Who controls the Internet - Jack Goldsmith & Jim Wu

The Hacker Crackdown - Bruce Sterling

Free as in Freedom - Richard Stallmann

A History of the Internet and the Digital Future - Johnny Ryan

The Shallows - Nicholas Carr

To be a Machine - Mark ò Connell

People vs Tech - Jamie Bartlett

Who rules the World - Noam Chomsky

Against Method - Paul Feyerabend

Data-ism - Steve Lohr

When Google met Wikileaks - Julian Assange

The future of Ideas - Lawrence Lessing

The Four Dimensional Human - Laurence Scott

Deep Fakes and the Infocalipse - Nina Schick

With a Little Help - Cory Doctorow

How Democracy Ends - David Runciman

Democracy Hacked - Martin Moore

The Forth Revolution - Luciano Floridi

CREDITS

CONTATTI

mail: jolek78@tutanota.com || xmpp: jolek78@conversejs.org

mastodon: https://fosstodon.org/@jolek78

STRUMENTI UTILIZZATI

libreoffice https://www.libreoffice.org/

calibre https://calibre-ebook.com/

gimp https://www.gimp.org/

MUSICA ASCOLTATA

https://cryochamber.bandcamp.com

COPERTINA

immagine: https://www.deviantart.com/mclelun

font: https://github.com/googlefonts/Inconsolata

LICENSE

DISCLAIMER

Ogni lavoro ha dei refusi e/o errori. E questo non è differente. Nessun imbarazzo quindi: se trovate anomalie, sentitevi liberi di segnalarle all'indirizzo jolek78@tutanota.com. Le correzioni verranno inserite nella prossima versione. Grazie!

-[jolek78]-