Cryptogenealogia

Primo frammento per una genealogia della crittografia (dai Cypherpunks a Wikileaks)

Vivien García, Carlo Milani

Sommario

La crittologia è ormai argomento di interesse generale. L'uso di massa di tecnologie digitali per comunicare, combinato agli scandali sulla sorveglianza diffusa hanno acuito la preoccupazioni per la salvaguardia della privacy. Proponiamo una metodologia genealogica, basata sugli archivi, attenta alle influenze incrociate fra tecnologie, discipline, ideologie e contesto storico. La applichiamo alla storia recente, tracciando una genealogia dal movimento Cypherpunk a Wikileaks. Per quanto controintuitivo possa sembrare, trasparenza radicale e desiderio di opacità hanno una radice comune.

Abstract

Cryptography has become a matter of general interest. The massive use of digital technologies for communication, combined with the surveillance scandals, have increased concerns about the protection of data and privacy. In this paper, we first present our genealogical methodology. Based on the study of archives, it pays special attention to the cross-influence between technology, discipline, ideology, and historical context. We then apply this methodology on recent history, tracing a lineage going from cypherpunks to Wikileaks. As strange as this may sound, radical transparency and wish for opacity share a common root.

Keywords: cryptography, genealogy, cypherpunks, wikileaks, history of ideas

1. Introduzione

Si è scritto e si continua a scrivere e parlare molto di crittologia, cioè degli strumenti per crittografare le comunicazioni, e di quelli di crittoanalisi, per svelarne il contenuto. La crittografia in particolare è ormai un argomento che ha travalicato ampiamente la cerchia ristretta degli esperti di sicurezza informatica. L'uso di massa di tecnologie digitali per comunicare su scala globale, combinato agli scandali riguardanti la sorveglianza di massa degli utenti (uno su tutti, l'*affaire* Snowden e il cosiddetto DataGate) hanno provocato una comprensibile preoccupazione per la salvaguardia della privacy.

Un indicatore chiaro dell'ampiezza di tali preoccupazioni è il fatto che parecchi fra i giganti dell'informatica ne abbiano preso atto e abbiano modificato i loro prodotti in tal senso. Solo nel 2016 citiamo la crittografia end-to-end introdotta da *WhatsApp* (società acquisita dalla Facebook, Inc. nel 2014) e l'implementazione dell'algoritmo AES-256 (Advanced Encryption Standard, con chiave a 256 bit, il massimo consentito dall'algoritmo) di default sui sistemi *iOS* di Apple. Queste novità sono state presentate pubblicamente con argomentazioni commerciali, come innovazioni che migliorano i prodotti nell'interesse dei consumatori. Parallelamente, la recente recrudescenza di attentati terroristici in diversi paesi occidentali e l'utilizzo (effettivo o supposto, non siamo in grado di saperlo con certezza) di strumenti crittografici da parte degli attentatori stessi, ha spinto alcuni politici e funzionari di alto livello a condannare senza appello la cifratura dei dati in generale.

Come prevedibile, la maniera con cui i media e il pubblico di massa ha affrontato tali questioni soffre di numerose semplificazioni e banalizzazioni. In informatica, come in moltissimi altri ambiti, è difficile formulare un discorso corretto se si parla di grandi categorie generali invece che di oggetti precisi. Impossibile e anzi non auspicabile, quindi, fare a meno della complessità teorica e tecnica, anche se è senz'altro fondamentale sforzarsi di renderla comprensibile per un pubblico quanto più possibile vasto.

Insistiamo in particolare sull'idea mai abbastanza ripetuta: la tecnica non è né buona né malvagia di per sé, non più di quanto sia neutra [1], e quindi "per questo motivo bisogna riscoprire l'arte del limite" [2]. È in questa prospettiva che vorremmo qui proporre un frammento di genealogia, riposizionare storicamente alcuni oggetti e fenomeni del mondo digitale e problematizzare in questo modo le loro condizioni le loro condizioni ideologiche e le loro appartenenze, spesso equivoche, a determinati regimi tecnici. L'idea non è di tentare di ritrovare un'origine in grado di rivelarci ogni sfaccettatura del presente, come se il passato contenesse *in nuce* il presente. Al contrario, vorremmo cercare di studiare filiazioni e provenienze allo scopo di, per riprendere Foucault, "inquietare ciò che veniva percepito come immobile, frammentare ciò che si pensava unito: mostrare l'eterogeneità di ciò che si riteneva conforme a sé stesso"[3].

Dopo una riflessione metodologica nella quale descriveremo il nostro modo di procedere, e ne daremo ragione, torneremo su eventi della storia recente che ci condurranno dal movimento Cypherpunks a Wikileaks. La posta in gioco di tale percorso consiste nel mostrare che, per quanto controintuitivo possa sembrare,

trasparenza radicale e desiderio di opacità e oscurità in questo caso hanno una radice comune.

2. Questioni di metodo

2.1 Un approccio genealogico

Il primo punto da chiarire riguarda l'approccio generale adottato. Lo qualifichiamo come genealogico, nel solco tracciato da Foucault. Risulta immediatamente evidente che si appoggia al passato, ma è necessario precisare il rapporto che instaura con esso. Non si tratta di proporre una storia lineare di oggetti tecnici e di discorsi che deriverebbe direttamente gli uni dagli altri, e che offrirebbero la chiave per comprendere il presente. Si tratta di tornare indietro nel tempo per rintracciare una *molteplicità di provenienze*.

In questo articolo abbiamo deciso di concentrarci su *una sola linea di discendenza*. Ma anche nel caso di questa semplice immagine dell'unica stirpe è cruciale focalizzare l'attenzione sulla molteplicità degli incontri e degli incroci invece che sul carattere apparentemente rettilineo della branca considerata. Ulteriore caratteristica peculiare del nostro metodo: convochiamo, mobilitiamo su uno stesso piano d'azione diverse dimensioni (filosofiche, scientifiche, politiche, tecniche…) nel tentativo di restituire le condizioni d'emergenza e le loro mutue rispondenze e corrispondenze.

In queste condizioni l'informatica si rivela attraversata in lungo e in largo dalle ideologie e dal politico, senza per questo ridursi a un semplice prodotto al servizio della politica o dell'ideologia. Questo percorso di ricerca implica il lavoro sugli archivi, ancora nel senso foucaultiano del termine, ovvero: "non la totalità dei testi che sono stati conservati da una civiltà, e nemmeno l'insieme delle tracce che è stato possibile salvare dal disastro di quella civiltà, ma il gioco delle regole che in una cultura determinano la comparsa e la scomparsa degli enunciati, il loro permanere e la loro cancellazione, la loro paradossale esistenza in quanto avvenimenti e cose" [4].

L'oggetto che prendiamo in considerazione qui esige tuttavia di ampliare un poco il quadro foucaultiano e di prendere in considerazione degli *oggetti tecnici*. Ma questi ultimi non vengono mai considerati a partire dalla loro mera tecnicità. Essa viene sempre messa in risonanza con testi teorici, ma anche manuali, licenze, insomma con una varietà di archivi. Colti nel contesto e posti su uno stesso piano, gli oggetti consentono di problematizzare il legame fra tecnologia, ideologia e potere. La sfida di un approccio del genere consiste nella maniera in cui mette in relazione il passato al presente. Mobilita elementi storici e li fa risorgere nella loro singolarità non per mero piacere e sfoggio di conoscenza, ma perché sono carichi di senso nel presente. L'ipotesi di fondo è che gli oggetti tecnici che mediano le comunicazioni siano uno dei luoghi d'elezione per il manifestarsi di conflitti sociali e psichici, appunto perché si pongono fra gli umani, a organizzarne le relazioni. Ecco perché questa genealogia è selettiva, prospettiva, consapevole; si costruisce nella situazione presente ed è parte in causa nei problemi che la contemporaneità le impone. Ma soprattutto, non deduce "la forma di ciò che siamo [...], ma sviluppa dalla

contingenza che ci ha fatto divenire ciò che siamo la possibilità di non essere, fare o pensare più ciò che siamo, facciamo o pensiamo"[5].

2.2. Politica e ideologie

L'ideologia ricorre più volte in questo discorso. Il termine è carico, appesantito da una polisemia spesso problematica. I suoi vari significati, soprattutto nel corso del XX secolo, lo hanno reso davvero ambivalente. Il nostro scopo qui, seguendo Michael Freeden, non è quello di prendere in considerazione le ideologie come statici "sistemi di credenze", come modelli arbitrari o convenzionali che i pensatori ci invitano ad adottare come fossero separati dagli attori. Al contrario, le ideologie sono intese come costrutti che riflettono gli usi sociali e storici, che possono cambiare ed evolvere nel corso del tempo. Inoltre in quanto modelli e sforzi di modellizzazione del reale, non solo discendono dal contesto, ma cercano anche di interpretarlo, di forzarlo e di dargli forma.

Con questo non vogliamo certo sostenere che la politica sia puro relativismo, tanto più che il relativismo puro e assoluto non è affatto relativo, ma è una forma mascherata di assolutismo [6]. Infatti è evidente che i contesti culturali, storici e sociali dati in cui una parola emerge "impongono alla maggior parte dei suoi utenti campi di significazione ordinari o sovrapposti, che i parlanti non possono facilmente scrollarsi di dosso". Ma le ideologie si distinguono l'una dall'altra perché "sono caratterizzate da una morfologia che presenta concetti nucleari di base, concetti adiacenti a questi e infine concetti periferici".

Freeden porta l'esempio dei liberalismi e sostiene che "la libertà si trova all'interno del loro nucleo 'concettuale', i diritti umani, la democrazia, l'uguaglianza sono adiacenti alla libertà, e il nazionalismo si situa alla periferia concettuale"[7]. Poiché le ideologie non sono fisse, i concetti che esse implicano possono spostarsi. Qualche cambiamento in un contesto può portare a nuove priorità che il vecchio significato di un concetto non è in grado di sostenere. Un caso assai frequente è un evento storico imprevedibile, che può coincidere in parte con l'invenzione di un nuovo oggetto tecnico. Il desiderio di appianare eventuali incertezze, inter o intra ideologiche, di una definizione concettuale, può comportare una ridefinizione parziale o condurre a focalizzarsi su un concetto adiacente all'interno della morfologia ideologica. Sul lungo periodo le mutazioni continue potrebbero metamorfosare/modificare addirittura il nucleo stesso, rendendo irriconoscibile l'ideologia originaria.

La morfologia esistente può, al contrario, trovarsi rinforzata. Freeden chiama questa operazione "decontestation", che traduciamo come *risoluzione di una controversia*. Ma come possiamo determinare quali ideologie appartengono a quale gruppo ideologico? La risposta di Freeden si avvale dello strumento della *Familienähnlichkeit*, l'*aria di famiglia*, individuato e analizzato da Ludwig Wittgenstein. Ciò significa che ognuna delle idee cardine non è necessariamente condivisa da ciascun membro della "famiglia". In quella mescolanza di appunti che sono le *Ricerche Filosofiche*, Wittgenstein portava l'esempio dei giochi. Le cose e le attività a cui ci riferiamo come giochi possono essere molto diversificate fra loro: giochi di carte, giochi da tavolo, giochi con la palla e così via. Non esiste un limite chiaro e netto, l'ambiguità regna sovrana e

l'indeterminatezza sembra non poter essere espunta in nessuna definizione. La denotazione di una parola non è quindi il suo significato. È l'uso del termine nel corpus del linguaggio che genera il significato, in maniera fluttuante.

La nozione di *aria di famiglia* precisa quella di gioco linguistico. Nel linguaggio si concretizzano forme diverse che non hanno in comune necessariamente un'essenza o una forma logica condivisa, ma soltanto somiglianze "qua e là" che "affiorano e scompaiono" [8].

L'approccio di Freeden si concentra solo su concetti politici e su come si costruiscono le ideologie. Il nostro oggetto di studio, però, non è costituito solo da discorsi. Dipende in primo luogo dalla disposizione e dalla concatenazione fra oggetti tecnici e utenti che utilizzano quegli oggetti in modi specifici. Se si ritiene che fra strumenti e idee, fra teoria e pratica sussista un abisso incolmabile, non c'è modo di superare la difficoltà. Ma non è il nostro caso.

Noi riteniamo che la scienza, la tecnologia e le società sono una co-costruzione, creazioni in un processo di messa a punto reciproca di macchine, relazioni sociali, individui, fatti e teorie. Su questo punto, siamo d'accordo con l'approccio elaborato da Latour e Callon nell'ambito della sociologia della scienza, la Actor-Network Theory (ANT), che si basa innanzitutto sull'analisi di controversie scientifiche. La ANT tende ad interpretare l'innovazione tecnologica come un costrutto, frutto di negoziati e, allo stesso tempo, correlata all'identità degli attori in gioco, ai loro bisogni, ai loro interessi e alle loro strategie. "Questo non vuol dire che ogni cosa viene negoziata in continuazione, ma significa riconoscere che nulla può essere regolamentato senza negoziazione e che non esiste un criterio di per sé evidente, che sia di verità o di efficacia. Le necessità sono costruite, rafforzate e garantite da rapporti di potere"[9]. Gli oggetti tecnici sono portatori di interessi nella formazione di reti eterogenee che combinano attanti di ogni tipo e dimensione, umani e non. Un approccio simile rigetta sia il banale determinismo tecnologico, che considera gli artefatti tecnologici come parti semplici di una struttura tecnologica complessa, sia il puro costruttivismo sociale, che nega agli oggetti la propria consistenza e coerenza e concede lo status di soggetto, nelle parole dei nostri definito "attante", solo all'essere umano.

3. Dal cypherpunk a Wikileaks e oltre

Sulla scorta di queste indicazioni, tracceremo ora una genealogia che ci condurrà dal movimento Cypherpunk a Wikileaks, aprendosi quindi su nuovi possibili affiliati alla famiglia crittografica. Si tratta della prima tessera di un ben più ampio e variegato mosaico, ancora tutto da comporre, relativo alla storia degli oggetti tecno-politici. In questo sforzo di cripto-genealogia utilizziamo solo gli archivi, per impiegare una terminologia foucaultiana, documenti ampiamente pubblicati sul Web. Abbiamo vagliato una grande quantità di dati e abbiamo agito su questo bacino come filtri umani per ricostruire un resoconto affidabile in un tempo ragionevole. Una selezione ragionata, cioè una critica nel senso più stretto del termine [10].

3.1 L'entusiasmo crittografico

La storia della scrittura di messaggi nascosti, la crittografia appunto, è molto antica, e intrecciata a doppio filo con la storia della guerra. Infatti l'arte di rendere segreti i messaggi è stata largamente praticata per scopi bellici da migliaia di anni. Ma solamente dalla metà del XX secolo la crittologia (crittografia + crittanalisi) si è costituito come un sapere scientifico rigoroso [11]. La nostra genealogia è ancor più limitata e inizia con il movimento di appassionati di crittografia chiamato cypherpunk. Julian Assange, co-fondatore di Wikileaks, è stato uno dei sottoscrittori e membri attivi di questo movimento. Una pagina web ospitata da un server della Berkeley University, sosteneva di essere l'originale homepage del gruppo cypherpunk, ma al momento di questa ricerca non risulta disponibile. WebArchive, una copia non completa del web, risale solo fino al 9 gennaio 1997: sono necessarie ulteriori indagini, ma niente di veramente rilevante sembra esista prima di 1988-1992. Per situare storicamente questi artefatti bisogna sottolineare che il web, nato ufficialmente nel 1991, ha iniziato a diffondersi solo nel 1993. L'attuale homepage Cypherpunk non è più ospitata da Berkley, ma a Tonga [12]. Cronologicamente, il primo testo importante per il movimento Cypherpunk è *The Crypto Anarchist Manifesto* (*Il Manifesto Criptoanarchico*, diverse redazioni e rimaneggiamenti, 1988-1992) di Timothy C. May, alias Tim May. Dal titolo si direbbe un testo politico: si riferisce esplicitamente all'anarchia, anche se non spiega di che tipo di anarchia si tratta. Si inizia con una strizzata d'occhio a Marx ed Engels, in particolare al *Manifesto del Partito Comunista*: "Uno spettro si aggira il mondo moderno, lo spettro della cryptoanarchia" [13], ma il testo contiene un riferimento alla nozione liberale di "mercato liquido" (*liquid market*). Nulla a che vedere con il comunismo né con l'anarchismo. Nonostante questi elementi politici, gran parte del testo ha uno scopo tecnico. Si ritiene che nella tecnologia informatica la privacy sia un bene di primaria importanza e si afferma che la crittografia sia il mezzo per raggiungere la privacy. Le parole chiave sono: anonimato, (poichè come dichiara l'autore, "la tecnologia informatica è sul punto di fornire la possibilità a individui e gruppi di comunicare e interagire con gli altri in maniera totalmente anonima" [14]), reputazione, segreto, fiducia, regolamentazione. Troviamo anche una forte tesi sull'impatto della tecnologia sulla società:

Così come la tecnologia della stampa modificò e ridusse il potere delle corporazioni medievali e la struttura di potere sociale, così anche i metodi crittologici modificheranno in maniera sostanziale la natura della corporazioni e l'interferenza del governo nelle transazioni economiche. [15]

I manufatti tecnici cambiano il mondo; sono attanti, diventano attori a parte intera del mondo. Ne deriva che l'atto di creare tali oggetti sta agendo attivamente sul mondo e lo sta trasformando. Dal punto di vista della storia della tecnologia, all'epoca della redazione del *Crypto Anarchy Manifesto* i principali strumenti di criptazione si basano su sistemi di crittografia convenzionali, come il Data Encryption Standard (DES) che utilizza una singola chiave per cifrare e decifrare, oppure l'asimmetrico RSA. Il DES è stato progettato nei primi anni 1970 sulla base della famiglia di algoritmi Lucifer, uno dei primi cifrari a blocchi, sviluppati in IBM. Ma si sospetta che il suo ulteriore sviluppo sia stato influenzato

dall'agenzia USA NSA (National Security Agency). L'algoritmo era stato probabilmente segretamente indebolito dall'agenzia in modo che potessero leggere facilmente i messaggi crittografati.

Invece il sistema RSA Hat è stato creato al MIT nel 1973. Quando il Manifesto è stato scritto, era ancora abbastanza sicuro (anche se nel 1985 è stato scoperto l'attacco Håstad), ma pesante da utilizzare per la potenza di calcolo allora disponibile. Un nuovo strumento chiamato PGP (Pretty Good Privacy) sarebbe apparso nel 1991, tre anni dopo la prima redazione del manifesto, in contemporanea con le sue successive modifiche. È interessante notare che il manuale di PGP sembra convergere pienamente con le preoccupazioni del *Crypto Anarchist Manifesto*. Combinando il sistema "Rivest-Shamir-Adleman (RSA) di crittografia a chiave pubblica con la rapidità di algoritmi di crittografia convenzionali veloci" viene presentato dal suo creatore, Philip Zimmerman, come un sistema di "crittografia a chiave pubblica RSA per le masse" [16]. Cosa inedita e sorprendente per un manuale tecnico, assume in vari passaggi un chiaro tono politico e critica in maniera esplicita l'istituzione allora vigente per la difesa della privacy:

Il lavoro principale della NSA [National Security Agency] consiste nella raccolta di informazioni […]. La NSA ha accumulato capacità e risorse per violare codici. Se le persone non possono accedere a sistemi crittografici di qualità per proteggere sé stesse, il lavoro della NSA è molto più facile. La NSA è anche responsabile per la raccomandazione e l'approvazione degli algoritmi di cifratura. Qualche critico sostiene che questo sia un conflitto di interessi, come mettere la volpe a guardia del pollaio. La NSA ha cercato di promuovere un algoritmo di crittografia convenzionale di suo sviluppo, senza dire a nessuno come funziona perché è riservato. Essi vogliono che altri si fidino di esso e lo usino. Qualunque crittografo però, potrà dirvi che un algoritmo valido non ha bisogno di essere riservato per rimanere sicuro. Solo la chiave necessita di protezione. Come si fa a sapere se l'algoritmo della NSA è veramente sicuro? Non è così difficile per la NSA progettare un algoritmo di cifratura violabile solo da loro se nessuno può vederlo. Che stiano deliberatamente vendendo una panacea avvelenata? [17]

Zimmermann era un attivista antinucleare di lunga data. Ha progettato PGP in modo che persone a lui affini potessero utilizzare in modo sicuro le BBS (Bulletin Board Systems) di allora, visto che ancora il Web non era di pubblico accesso su Internet, e archiviare messaggi e file con sicurezza. L'uso non commerciale del software è libero e il codice sorgente completo è incluso in tutte le copie.

3.2 Quale tipo di anarchia?

Due testi marcano il prosieguo dell'Odissea Cypherpunk e ci aiutano a comprendere la sua progressiva definizione. Il primo è *A Cypherpunk's Manifesto* (*Manifesto dei Cypherpunk*, 1993) di Eric Hugues. La sostanza è in pratica la stessa dei due documenti appena citati. Ma cambiano alcuni elementi. Paradossalmente, il titolo sembra essere più tecnico, ma il contenuto del testo è più politico. La prima frase mescola un chiaro orientamento liberale

con una visione del mondo basata su preoccupazioni tecniche: "La privacy è necessaria per una società aperta nell'era elettronica".

La privacy viene qui giustificata soprattutto a difesa della libera transazione economica, e si menziona l'idea di moneta elettronica. Il testo crea un'identità tecnico-politica, l'identità Cypherpunk, espressa con il pronome "noi". Definisce anche una metodologia attivista: "I Cypherpunks scrivono codice. Sappiamo che qualcuno deve scrivere software per difendere la privacy, e dal momento che non siamo in grado di ottenerla a meno che non lo scriviamo tutti, abbiamo intenzione di scriverlo. Pubblichiamo il nostro codice in modo che i nostri compagni Cypherpunks possano esercitarsi e giocarci. Il nostro codice è free da usare per tutti, in tutto il mondo [si noti che in inglese, *free* significa libero ma anche gratuito]. Non ci interessa affatto se non approvate il software che scriviamo. Sappiamo che il software non può essere distrutto e che un sistema ad alto grado di dispersione non può essere chiuso". [18]

Il secondo testo determinante è *The Cyphernomicon: Cypherpunks FAQ and More* [19]. Molto più esteso degli altri testi cypherpunk, nel complesso sviluppa le stesse idee. Da notare che un intero capitolo è dedicato a PGP. Diffondere il software e la crittografia in generale, con programmi educativi, dischetti contenenti saggi e programmi, siti FTP (File Transfert Protocol) e rave, convegni e raduni, è una parte importante del progetto Cypherpunk. Il suo interesse per la nostra ricerca è dovuto soprattutto al chiaro posizionamento politico esplicitato lungo tutto il testo: libertariano (libertario di destra) [20], o più precisamente anarco-capitalista. I liberali sono descritti come possibili alleati e l'autore si sforza di convincerli ad associarsi alla causa libertariana.

Ad esempio si chiede: Come si possono convincere i non libertariani (ad esempio i liberali) della necessità di una crittografia pesante, quando implica azioni ritenute illegali dallo Stato? May adduce come esempio il caso di un aborto, effettuato in un Paese che lo considera illegale, in seguito a stupro. Chi mai potrebbe essere contro la crittografia pesante, se questa consentisse di coordinare azioni simili per aggirare una legge ingiusta, e di organizzare la resistenza e il cambiamento? Quindi, in che senso la crypto-anarchia è anarchica? Analizzando i due manifesti e le dichiarazioni del Cyphernomicon, possiamo sostenere che i Cypherpunks sono nel complesso sostenitori destrorsi della libertà del mercato più che sostenitori della libertà delle persone.

Sia May che Hugues hanno ampiamente mostrato la loro fede cieca nella realizzazione per via tecnologica di ciò che oggi viene chiamato *frictionless market* (mercato senza attriti), che si ritrova in tanti discorsi sulle criptovalute basate sulla *blockchain* come tecnologia di liberazione. Nelle loro critiche le istituzioni politiche, e soprattutto quelle statali, vengono considerate limitanti e lesive delle libertà individuali. Sostengono l'eliminazione di questo tipo di strutture istituzionali in favore della sovranità individuale in un libero mercato. In questo contesto, l'accento sulla crittografia è ora facilmente comprensibile. La crittografia è l'oggetto tecnico che garantisce l'esistenza di sfere separate di libertà individuale e protegge le transazioni dirette (in particolare le transazioni economiche) al di fuori dal controllo dello Stato, stabilendo in tal modo, a

prescindere dalla legalità o meno dei procedimenti impiegati, un vero e proprio *laissez-faire* economico.

La politica, nel senso tradizionale del termine, scompare a favore delle relazioni volontarie e contrattuali tra gli individui sulla base di una libera economia di mercato. La politica intesa come *azione nello spazio pubblico condiviso* non ha semplicemente ragion d'essere perché gli spazi pubblici tendono a essere riassorbiti in spazi privati, assoggettati all'arbitrio individuale. La politica viene sostituita dalla tecnica, il governo non tende a socializzarsi in autogoverno, bensì a mutarsi in *governance*, in amministrazione. E attenzione! Siamo nel 1988-1992, cioè oltre vent'anni prima di Wikileaks e dell'era del DataGate.

3.3 Wikileaks e oltre

Ed ecco trascorsi vent'anni. Le tecnologie sono cambiate, il contesto è diverso. Anche gli attori si sono evoluti. Fra loro, Julian Assange compare qui per servirci come filo conduttore. Non abbiamo alcuna intenzione di formulare un giudizio sulla sua figura mediatica. Il suo percorso ci interessa perché mette in luce uno degli aspetti più misconosciuti di Wikileaks e per metterlo in risonanza con il recente passato.

Riepiloghiamo in estrema sintesi la vicenda di Wikileaks [21]. Wikileaks è nata nel 2006 come sito per pubblicare materiale riservato, segreto, confidenziale. Inizialmente ha utilizzato la stessa interfaccia di Wikipedia (fino al 2010), presentandosi come luogo in cui è possibile consegnare anonimamente documenti pericolosi; sarà il sito a rilasciare pubblicamente i materiali dopo averli vagliati. In un primo momento non è affatto sicuro e nemmeno anonimo spifferare qualcosa a Wikileaks; solo in un secondo momento l'organizzazione si doterà di sistemi relativamente sicuri. Assurge agli onori della cronaca internazionale a partire dall'arrivo, nel 2007, di Julian Assange, autoproclamatosi caporedattore (editor in chief). Assange è un hacker australiano nato nel 1971. Ha subito una condanna nel 1992 per reati federali in Australia (commutata nel 1996 in pena pecuniaria) [22].

La figura di Assange ha occupato le prime pagine dei giornali di tutto il mondo per mesi, prima e dopo il cablegate del Novembre 2010, quando Wikileaks ha diffuso i cablogrammi, documenti diplomatici segreti (ma non classificati come top secret) riguardanti soprattutto le malefatte del governo americano. Accusato di violenza sessuale nei confronti di due donne in Svezia, per evitare l'estradizione, Assange si è rifugiato presso l'Ambasciata dell'Ecuador a Londra, dove vive da metà giugno 2012 con lo status di rifugiato politico. L'*affaire* Wikileaks risponde pienamente ai canoni della Società dello Spettacolo di debordiana memoria. In quanto spettacolo esso stesso, i colpi di scena sono sempre possibili.

Certo, Assange non è Wikileaks. Anche se è molto difficile separare l'organizzazione dal suo leader carismatico, ci sono molte persone e gruppi di supporto coinvolti, che proseguono nel lodevole sforzo di rendere disponibili materiali altrimenti di difficile reperimento. Wikileaks ha portato alle luci della ribalta documenti necessari per comprendere il presente e ricostruire l'accaduto. La base dati pubblicata, in continua crescita, è una miniera di

informazioni a disposizione dei ricercatori e dei cittadini tutti, di chiunque non si accontenti di rimanere alla superficie e voglia mettere in discussione le proprie certezze. Queste informazioni entrate nella sfera pubblica riguardano tutti, devono essere valorizzate, discusse e raccontate in modo da diventare un patrimonio comune, cultura critica condivisa.

Al di là dei contenuti, però, riteniamo che la forma non sia indifferente. Ci viene spontaneo domandarci quale visione politica sia espressa da una testata giornalistica, da un media qualsiasi, da un intellettuale pubblico; eppure in questo caso sembra non pertinente, quasi che l'enormità scandalosa delle fughe di notizie renda irrilevanti le modalità, e nello specifico la struttura tecnica e organizzativa, i suoi presupposti. Ma i mezzi non sono semplici intermediari, la tecnologia non è mai neutra, ma è invece come abbiamo già detto un attante, un attore a parte intera sulla scena pubblica. È poter-fare, in questo caso poter raccogliere e disseminare informazioni. Il potere può essere gestito e diffuso per l'emancipazione di individui e comunità, oppure accumulato per opprimere e dominare, ma in nessun caso è un ingrediente anodino dell'articolazione sociale.

A differenza dei tanti attivisti, militanti e sostenitori dei più vari orientamenti politici che hanno contribuito alla costruzione di WikiLeaks, la posizione di Assange è però nota. Certo, diversi esponenti della più becera reazione a stelle e strisce lo considerano un nemico pubblico degli USA, tanto che l'allora commentatrice di Fox News, Sarah Palin (ex governatrice dell'Alaska, sostenitrice del Tea Party) esortava a cacciarlo e abbatterlo al pari dei terroristi di Al Quaeda. Eppure la biografia dell'hacker australiano e le sue dichiarazioni esplicite raccontano tutta un'altra storia. In una lunga intervista di quel fatidico Novembre 2010 rilasciata a Andy Greenberg e pubblicata su Forbes chiariva l'obiettivo delle rivelazioni di Wikileaks nel quadro del mercato capitalista, che sosteneva a spada tratta: "perché ci sia un mercato, ci vuole informazione. Un mercato perfetto necessita un'informazione perfetta". In questo modo le persone sono libere di giudicare su quale prodotto orientarsi. Si dichiarava "libertariano", perlomeno dal punto di vista della concezione economica, e concludeva "Wikileaks è concepito per rendere il capitalismo più libero ed etico". [23] In diverse occasioni Assange ha ampiamente sostenuto e affermato la sua appartenenza al movimento Cypherpunk, che abbiamo visto essere legato a doppio filo all'ideologia libertariana e anarco-capitalista nello specifico. È stato definito anche un utopista neoliberale [24].

Ma il progetto Wikileaks nell'interpretazione di Assange estremizza le prese di posizione dei cypherpunks. Questi ultimi promuovevano e promuovono tuttora un attivismo basato sulla diffusione della crittografia, con lo scopo dichiarato di realizzare le condizioni necessarie per l'instaurarsi di transazioni davvero libere. Wikileaks non si limita a sostenere lo scambio anonimo crittografato tra gli individui. Per raggiungere l'agognata privacy, presupposto della libertà di mercato, rivela paradossalmente (principalmente dando seguito a singole denunce anonime) segreti governativi e istituzionali, i segreti di coloro che sono considerati ostacoli per il libero scambio. La luce gettata sulle oscure trame governative è l'altra faccia della medaglia della privacy intesa come *diritto a*

essere lasciati in pace, “the right to be let alone” [25], così definito nel 1890 dai giuristi statunitensi Warren e Brandeis.

La politica libertariana promossa consapevolmente da Assange e in definitiva dall'attitudine Wikileaks, così come il progetto Cypherpunk, implicano un paradosso ancora più problematico. Da una parte, incoraggiano la proliferazione di interazioni sicure, anonime e dirette tra individui: è necessario scrollarsi di dosso con ogni mezzo, legale o meno, la mediazione delle istituzioni politiche. D'altra parte, considerano gli oggetti tecnologici come mezzi per trasformare il mondo, dunque sono consapevoli che chi controlla questi artefatti detiene un potere enorme. La mediazione delle vecchie istituzioni politiche è sostituita dalla mediazione della tecnologia. La tecnologia è nelle mani di chi la sa usare. La tecnocrazia viene presentata come garanzia di libertà.

3.4 La libertà, appannaggio dell'élite di "topi furbi"

Questo punto cruciale non viene ignorato nel saggio *Cypherpunks: Freedom and the Future of the Internet* (Cypherpunks: La libertà e il futuro di Internet, assurdamente tradotto in italiano come *Internet è il nemico*), di cui Julian Assange è co-autore insieme agli attivisti digitali Jacob Appelbaum, Andy Müller-Maguhn e Jérémie Zimmermann. La sua introduzione è sottotitolata *A Call to Cryptographic Arm*, Chiamata alle armi crittografiche. E chi sono i destinatari di questo invito? Chi sono i soggetti politici della politica Cypherpunk? Non certo le persone comuni, i cittadini di buona volontà, e nemmeno gli indignati o gli oppressi stanchi della politica istituzionale e desiderosi di libertà a cui affermano di rivolgersi i movimenti 2.0 che abbiamo rapidamente presentato in apertura. I destinatari sono una ristretta élite tecnica, una *truelite*. Sono i *clever rats*, cioè ratti intelligenti nelle parole di Assange:

Credo che sia il più probabile scenario per il futuro: una struttura totalitaria, estremamente chiusa, omogeneizzata, postmoderna, transnazionale con incredibili complessità, assurdità e schifezze, e dentro questa incredibile complessità uno spazio in cui possono intrufolarsi solo i topi furbi. [...] Come può essere libera una persona normale in questo sistema? Semplicemente non può, è impossibile. [...] Perciò credo che le uniche persone che riusciranno a conservare la libertà che avevamo, che so, vent'anni fa, perché lo stato della sorveglianza ne ha già eliminata un sacco, solo che ancora non l'abbiamo capito, siano quelle fortemente consapevoli degli ingranaggi del sistema. Perciò sarà libera soltanto un'élite di ribelli hi-tech, gli astuti topi che scorrazzeranno dentro il teatro dell'opera.[26]

In questo passaggio troviamo chiaramente manifesta una delle controversie più importanti delle attuali questioni politiche relative a internet. Di certo questi ratti intelligenti non hanno assolutamente nulla a che vedere, per esempio, con le masse oppresse alle quali si rivolge il messaggio politico nella tradizione socialista. Si tratta al contrario di un soggetto politico elitario, assimilabile a quello che l'hacker liberale Jaron Lanier ha definito *Nerd Supremacy*, suprematismo nerd [27].

4. Conclusione

Ci sembra abbastanza essenziale e urgente affrontare dettagliatamente le modalità con cui l'etica hacker è stata in parte perfusa dal suprematismo nerd. Questa influenza non lascia inalterate le manifestazioni politiche più tradizionali, ad esempio le rivelazioni di Wikileaks sulla candidata alla presidenza Clinton vanno a tutto vantaggio dello sfidante repubblicano. Al tempo stesso influenza anche i movimenti politici emergenti nati dalla partecipazione online, che condividono un approccio alla politica incentrato sulla componente digitale come elemento chiave dei cambiamenti. Sotto il velo della partecipazione in tempo reale, di opposizione ai “segreti” statali, aziendali e istituzionali, si nascondono forme di organizzazione gerarchiche, atteggiamenti tecnocratici?

In questo primo frammento abbiamo mostrato come nel breve periodo analizzato le tecnologie crittografiche non siano state un attore neutro dal punto di vista filosofico e politico. Al contrario, dai manifesti cypherpunk e dagli altri testi analizzati emerge una visione politica tutto sommato chiara. Gli oggetti tecnici non sono quindi neutri, ma incarnano convinzioni e ideologie dei tecnici creatori degli stessi. La pratica della crittografia, lungi dall’essere una mera opzione tecnica, appare fin dal principio parte di una più ampia strategia politica di segno libertariano e anarco-capitalista.

Per quanto controintuitivo possa sembrare, trasparenza radicale e desiderio di opacità hanno perciò una radice comune. La crittografia è l’elemento tecnico comune alle due opposte esigenze. È proprio questa tecnica di origine militare a consentire la strutturazione delle rivendicazioni tecno-politiche libertariane. È la percezione di uno stato di guerra permanente nel quale è necessario difendersi e attaccare e diffondere armi crittografiche a fungere da cornice per l'innovazione tecnica ovvero politica. Da una parte, la crittografia è inquadrata dai cypherpunks come scelta individuale capace di realizzare il desiderio di privacy, di opacità nei confronti del potere istituito. Una scelta da portare a tutti, da estendere alle masse. Dall’altra, in particolare con WikiLeaks, la crittografia diventa la maniera per consentire lo svelamento pubblico delle trame occulte della politica istituzionale, una riprova che il re è nudo. Trasparenza radicale del pubblico resa possibile dall’opacità personale del whistleblower. La crittografia viene posta come garanzia tecnica di entrambi i valori.

Per quanto riguarda future ricerche che volessero approfondire la metodologia genealogica qui proposta, anche l'archivio recente della mailing list cypherpunks è una miniera di informazioni [28]. Vi sono inoltre almeno due oggetti tecnici legati alla crittografia senz'altro degni della massima attenzione: le criptovalute e la blockchain su cui si basano. Come abbiamo visto già all'inizio degli anni Novanta i Cypherpunks si interessavano alla moneta elettronica e d'altra parte l'implementazione di smart contract garantiti dal registro crittografico mostra notevoli affinità con la loro visione del mondo.

Bibliografia

[1] Donald A. Norman (1993), *Things that make us smart*, Defending the Human Attributes in the Age of the Machine, Addison-Wesley, cap. 10, “Technology is not neutral”

[2] Luvison, A. "La crittografia, uno snodo cruciale per la cybersicurezza", *Mondo Digitale*, 16, http://mondodigitale.aicanet.net/2016-2/articoli/01_La_crittografia_uno_snodo_critico_per_la_cybersicurezza.pdf (settembre 2016)

[3] Foucault, M. (1971). "Nietzsche, la généalogie, l'histoire". In: *Œuvres II*. Paris: Gallimard, p. 1287.

[4] Foucault, M. "Sur l'archéologie des sciences : réponse au Cercle d'épistémologie", *Cahiers pour l'analyse*, no 9, été 1968, 9-40.

[5] Foucault, M. (1984). "Qu'est-ce que les lumières", In: *Œuvres II*. Paris: Gallimard, p. 1393

[6] Ibañez, T. (2013) Il libero pensiero. Elogio del relativismo, Elèuthera, Parte prima, passim.

[7] Freeden, M. (1996). Ideologies and Political Theory: A Conceptual Approach. 52; 78.

[8] Wittgenstein, L. (2009). Philosophical Investigations. Trans. by Gertrude Elizabeth Margaret Anscombe, Peter Michael Stephan Hacker, and Joachim Schulte. Oxford: Wiley & Blackwell. § 65-89.

[9] Callon, M. (2006). "Pour une sociologie des controverses technologiques". In: *Sociologie de la traduction.* Ed. by Madeleine Akrich, Michel Callon, and Bruno Latour. Paris: Presses des Mines, 135-157, http://books.openedition.org/pressesmines/1196 (sett. 2016).

[10] L'etimologia di critica rimanda al verbo greco krino = separare, cernere, scegliere e, in senso più lato, discernere, giudicare, valutare. Criticare significa quindi in primo luogo effettuare una scelta in base a una riflessione, utilizzando la facoltà del giudizio.

[11] Per una ricostruzione di questo passaggio epocale, si veda Angelo Luvison, "La crittologia da arte a scienza: l’eredità di Shannon e Turing", *Mondo Digitale*, http://mondodigitale.aicanet.net/2015-5/articoli/03_crittologia_da_arte_a_scienza.pdf (sett. 2016).

[12] https://www.cypherpunks.to/ le informazioni ottenibili tramite WHOIS sono estremamente scarse, il Tonga Network Information Center riporta: Tonic V1.1 whoisd - cypherpunk ns.cypherpunks.to - cypherpunk asteria.debian.or.at (sett. 2016)

[13] May, Timothy C. (1988). *The Crypto Anarchist Manifesto.* http://www.activism.net/cypherpunk/crypto-anarchy.html (sett. 2016).

[14] ibid

[15] ibid

[16] Zimmermann, Philip (1990). Pretty Good Privacy, RSA Public Key Cryptography for the Masses: PGP User's Guide.: http://openpgp.vie-privee.org/manupgp1.htm http://www.pgpi.org/docs/italian.html

[17] ibid. N.B.: la traduzione italiana disponibile risulta modificata rispetto all'originale inglese

[18] http://www.activism.net/cypherpunk/manifesto.html

[19] HTML https://www.cypherpunks.to/faq/cyphernomicron/cyphernomicon.html Versione originale https://www.cypherpunks.to/faq/cyphernomicron/cyphernomicon.txt (sett. 2016)

[20] Il libertarianesimo è un variegato complesso di correnti politiche che, a partire dagli anni Sessanta del Novecento, si pongono come realizzazione radicale delle libertà individuali, in un contesto esclusivamente di libero mercato e considerate in totale opposizione a qualsiasi tradizione e pratica socialista. Alcune varianti ritengono che sia possibile mantenere un minimo di società condivisa, confondendo volutamente le relazioni sociali con le istituzioni sociali, e si configurano perciò come minarchismo (fautori dello «Stato minimo»). Ma l'individualismo radicale apparentemente "anarchico", nelle opere dei pensatori libertariani più noti, come Murray N. Rothbard e Robert Nozick, si può realizzare solamente con l'abbattimento delle istituzioni sociali oppressive, tra le quali spicca lo Stato; da cui la definizione paradossale di anarco-liberali o anarco-capitalisti. Una fonte di ispirazione e idee libertariane è la fondatrice dell'Oggettivismo, Ayn Rand, anche se personalmente si opponeva alla loro visione. Per un inquadramento critico, si veda Ippolita (2016), *Nell'acquario di Facebook. La resistibile ascesa dell'anarco-capitalismo*. Per un approccio opposto, si veda il portale di orientamento anarco-capitalista http://www.ozarkia.net/bill/anarchism/faq.html

[21] Wikileaks è raggiungibile all'indirizzo https://wikileaks.org (sett. 2016). Per una disamina critica, si veda Lovink, G., Riemens, P. "Twelve Theses on WikiLeaks", in Brevini, B., Hintz, A., McCurdy, P., *Beyond WikiLeaks: Implications for the Future of Communications, Journalism and Society*, (2013), 245-253

[22] La storia di Assange è stata narrata da Suelette Dreyfus nel suo libro *Underground: Tales of Hacking, Madness and Obsession* sulla Electronic Frontier. L'hacker Mendax, un personaggio fondamentale della vicenda, è Assange. Un ragazzo con competenze di alto livello e attivo in vari progetti di codice; il più importante probabilmente è il sistema di deniable encryption Rubberhose, nome in codice Marutukku (1997-2000), pensato per proteggere i dati degli attivisti.

[23] Greenberg, A., "An Interview With WikiLeaks' Julian Assange", Forbes, http://www.forbes.com/sites/andygreenberg/2010/11/29/an-interview-with-wikileaks-julian-assange/print/ (nov. 2016)

[24] "Ramona, Julian Assange - Also neoliberal utopian", Libcom.org, 27 agosto 2012 https://libcom.org/library/julian-assange-also-neoliberal-utopian (nov. 2016)

[25] Warren and Brandeis, "The Right to Privacy", Harvard Law Review. Vol. IV December 15, 1890 No. 5 https://web.archive.org/web/20090301043642/http://lawrence.edu/fast/boardmaw/Privacy_brand_warr2.html (nov. 2016)

[26] Assange, J., Internet è il nemico: conversazione con Jacob Appelbaum, Andy Müller-Maguhn e Jérémie Zimmermann (2013), 148-149 (ed. or. Cypherpunks: Freedom and the Future of the Internet)

[27] Lanier, J., The Hazards of Nerd Supremacy: The Case of WikiLeaks, The Atlantic, 20 dec. 2010

[28] Gli archivi recenti della mailing list cypherpunks sono disponibili all'indirizzo https://lists.cpunks.org/pipermail/cypherpunks/

Biografia

Vivien García, dottore (PhD) in filosofia, premio tesi 2016 dell'Università di Grenoble, specializzato in filosofia politica, s'interessa alle implicazoni politiche, sociali ed etiche delle tecnologie digitali.

E-mail: vivien.garcia@alekos.net

Carlo Milani (PhD) è traduttore. Si è laureato in Lettere all'Università degli Studi di Milano. All'attività editoriale affianca l'informatica con alekos.net - tecnologie appropriate. Insegna archeologia, validazione delle fonti digitali, s-gamificazione. Tiene conferenze e formazioni in collaborazione con l'autore collettivo ippolita.net.

E-mail: carlo.milani@alekos.net