Politics. Rivista di Studi Politici
1(1),2014, 47-68

ISSN 2279-7629

Alcune considerazioni su *hacking* ed innovazione politica

Vittorio Milone

Abstract

In this article I try to explore some political and social aspects of the so-called *hacker* ethics, such as the possibilities of "bottom-up empowerment": for instance, I identify some *hacking* practices that distribute and democratize (bio)political control and are thus able to produce potential political innovation. Therefore, in spite of a socio-political context dominated by "proprietary and obscure" corporate oligopolies, we are still able to observe politically innovative *hacking* practices such as independent online (plat)forms of hacktivism or open source projects for promoting citizen science, making and bio*hacking*, which can also contribute potential (DIY/bio) political tools of control. Departing from the stereotype of "criminals of the information age", *hacker*s bring thus an important contribution to emphasize contemporary key issues such as the right to access a free flow of information, the openness and transparency of institutional and technological systems, the creative passion for sharing innovation and knowledge through their practices.

Keywords

Hacking - Political innovation - Bottom-up empowerment - Bio-hacking - Makers

1. Premessa. Alcuni aspetti sociali e politici del mondo *hacker* possono presentare risvolti interessanti dal punto di vista delle pratiche di democratizzazione e del "controllo/distribuzione" del potere (bio)politico dal basso. Questo articolo si apre con una parte introduttiva sull'*hacking* ed una breve analisi della letteratura presa in considerazione sull'argomento, con particolare riferimento alle tematiche connesse all'innovazione sociopolitica. Successivamente, vi è una sezione nella quale cerco di esaminare lo sviluppo di (piatta)forme di *networking* telematico indipendenti dalle forme di controllo pervasivo di oligopoli corporativi "oscuri e proprietari". In una seconda sezione, provo ad analizzare alcune (piatta)forme creative/innovative di *citizen science,*

making e biohacking, che facilitano la progettazione e la diffusione di mezzi di produzione e strumenti di controllo open source a basso costo, e mi soffermo anche in questo caso su quelle iniziative che più direttamente sembrano poter avere un impatto visibile sull'innovazione sociopolitica. Nelle conclusioni cerco di "tirare le somme" sulle potenzialità di innovazione politica connesse al mondo *hacker* ed alle pratiche di *hacking* prese in esame.

Il termine "hacker" è qui adoperato in modo alquanto differente dalla sua "accezione primigenia" dalla maggior parte dei cosiddetti media *mainstream*/generalisti, dove la parola sembra per lo più designare dei "criminali" dell'era dell'informazione. Molto diversamente, quello degli *hacker* è un fenomeno complesso ed articolato, con alle spalle delle etiche, pratiche e culture con delle loro storie/memorie, delle tradizioni letterarie ed un loro peculiare gergo largamente condivisi[1]. Gli *hacker* sono in senso letterale coloro che "fanno a pezzi" le cose per capirne il funzionamento e poterle modificare liberamente, soprattutto in un senso diverso da quello per il quale sono state originariamente "progettate". In *Hackers: Heroes of the Computer Revolution*, forse storicamente il lavoro più noto ed apprezzato sugli *hacker* stessi dal mondo *hacker by and large,* Steven Levy esordisce proprio delineando i tratti distintivi dell'etica *hacker*, individuandone gli elementi distintivi nella filosofia di "condivisione, apertura, decentralizzazione e nel poter mettere le mani sopra le macchine per migliorarle e migliorare il mondo" (Levy 2010, ix). La disponibilità delle macchine e del codice ed il cosiddetto imperativo dello *hands-on* sono viste come condizioni essenziali per poter capire nei dettagli cosa si sta utilizzando ed eventualmente anche per modificarlo creativamente, rendendo possibili delle operazioni per le quali "l'oggetto di *hacking*" in questione non era stato progettato inizialmente (Himanen 2001, 107-16). Si tratta sovente di una dimensione potenzialmente anche ludica, ben interpretata ad esempio da Linus Torvalds, sviluppatore del *kernel*[2] Linux, proprio nella sua introduzione al lavoro

[1]Il linguaggio degli hackers è in buona approssimazione "codificato", soprattutto nel cosiddetto "The Jargon File". Dal 1983 è stato anche pubblicato a stampa ed è aggiornato in Rete: http://www.catb.org/jargon/. Ultima edizione cartacea: (Raymond, 1996). Uno dei testi più influenti sulla storia dell'*hacking* è sicuramente Levy (2010).

[2]Il *kernel* è il nucleo (*core)* di un sistema operativo che gestisce richieste di input od output dal software e le traduce in istruzioni per l'elaborazione dei dati per la CPU e altri componenti elettronici di un computer. Il kernel è una parte fondamentale del sistema operativo di un computer moderno. GNU/Linux è un sistema operativo open source, cioè nel quale, diversamente dai caso dei più diffusi sistemi operativi commerciali a codice sorgente chiuso -

di Himanen, mediante il suo motto *"just for fun"* (Torvalds 2001*,* 9-12*).* Tale atteggiamento di Torvalds si trova in realtà in una sorta di tensione con gli *hacker* più esplicitamente motivati politicamente, come ad esempio i gruppi hacktivisti e -generalmente- con il movimento del Free Software, per i quali ultimi l'*hacking* del software libero è più qualcosa di simile ad una missione/visione politica e sociale, come si vedrà meglio in seguito. Himanen stesso infine ricorda come alla prima conferenza *hacker* del 1984 a San Francisco uno dei primi sviluppatori del computer Macintosh per Apple, Burrel Smith, sostenesse come l'atteggiamento *hacker* non fosse esclusiva del software, ma che si dovesse ritenere invece correlato con l'abilità e la dedizione con cui si fa qualcosa (Himanen 2001, 17). Tale considerazione è condivisa del resto anche da Eric Raymond, secondo il quale infatti ci sono persone che applicano l'atteggiamento *hacker* ad attività e contesti diversi dal software, e che tale disposizione a si può talvolta ritrovare ai più alti livelli di qualsiasi scienza o arte (Raymond 2001)[3].

Nel contesto della cosiddetta società della Rete e del ruolo centrale del software in essa in quanto *metamedium* tra i media divenuti programmabili (Manovich 2013, 2), l'*hacking* è stato indagato in quanto punto privilegiato di osservazione, proprio in quanto consente di mettere in primo piano questioni ritenute fondamentali come l'apertura e la trasparenza dei sistemi tecnologici ed istituzionali, il diritto di accesso ad un libero flusso delle informazioni, l'autonomia e la passione creativa per l'innovazione e la libera condivisione dei saperi: come accennato in precedenza, l'*hacking* è in questa sede analizzato non solo come modalità di approccio alle tecnologie − ad esempio, "mettendovi direttamente sopra le proprie mani" − ma anche come potenziale fattore di rinnovamento politico (Delfanti 2013, 139; Galloway 2004, 168-9). Infatti, senza conoscenza approfondita del software, il rischio è quello di trattare gli effetti e non le cause di certi processi o avvenimenti sociali, politici e culturali nei quali il software stesso sembra giocare un ruolo sempre più rilevante: come si vedrà meglio in seguito, questo è il pericolo che individua ad esempio Cory Doctorow nelle cosiddette "scatole nere", ovvero i sistemi tecnologici non aperti che difficilmente permettono un'analisi accurata delle loro dinamiche di funzionamento (2012b). Manuel Castells, nel suo epilogo a *L'etica hacker e lo*

quali ad esempio Windows e Mac Os X - il codice scritto dai programmatori è pubblicamente disponibile per verifiche, modifiche o personalizzazioni.

[3] Ripreso anche dallo stesso Himanen (2001, 17).

spirito dell'età dell'informazione di Pekka Himanen, sostiene proprio l'importanza di conoscere la cultura *hacker* per comprendere la contemporanea "società del network" e scrive che "la comprensione di questa cultura [*hacker*] e del suo ruolo nell'informazionalismo, in quanto fonte di innovazione e creatività, è il punto essenziale per la nostra comprensione della genesi della network society" (Castells 2001, 132).

In *The Exploit: A Theory of Networks* di Alexander Galloway e Eugene Thacker, l'*hacking* è preso in considerazione proprio per le sue potenzialità di liberazione e di *empowerment* sociopolitico nel contesto della società della rete e del controllo, delineando la necessità di un "asimmetrico antiweb" per il superamento dell'attuale "assetto di potere", caratterizzato sempre più spesso da un conflitto tra network (Galloway e Thacker 2007, 149-57). Nel suo *A Hacker Manifesto*, McKenzie descrive gli hacker/artisti/ricercatori e la loro cultura della condivisione come unico "bastione" contro il dominio − nella società della rete- dei "vettorialisti", ovvero di imprenditori e *corporation* detentori di brevetti e copyright ed in controllo delle principali piattaforme tecnologiche (McKenzie 2004). Gabriella Coleman in *Coding Freedom: The Ethics and Aesthetics of Hacking* effettua un'inchiesta etnografica sul mondo degli *hacker*, in particolare sulla loro significativa presenza nel cosiddetto Free Software Movement. All'interno dello stesso movimento, pur non necessariamente con piena consapevolezza e nell'ambito di una pluralità di declinazioni di etiche e pratiche, gli *hacker* con le loro stessa attività assumono una rilevante dimensione politica: Coleman situa gli *hacker* in una "critica al liberalismo dal suo interno", poiché li considera allo stesso tempo forti sostenitori della libertà di espressione, che gli *hacker* però utilizzano in buona parte per mettere in discussione un altro pilastro del liberalismo come la proprietà intellettuale rivelando le "linee di frattura" tra i due (Coleman 2013, 9), e situandosi in questo modo allo stesso tempo al centro ed ai margini della "tradizione liberale"[4].

Coleman tratta il liberalismo nei suoi registri culturali, nelle sue differenti modulazioni culturali ed istituzionali nello spazio e nel tempo: gli *hacker* del free

[4]Per Coleman il liberalismo non è da intendersi in questo contesto né nell'accezione europea di privilegiare il libero mercato, né come "quasi sinonimo" del Partito Democratico statunitense: si tratta invece proprio di un impegno e di una sensibilità morale e politica a proteggere - tra l'altro - le libertà civili e l'autonomia individuale, in particolare la libertà di espressione, il diritto ad uguali opportunità e la "meritocrazia" (2013, 2).

software "riconfigurano" infatti nella loro pratica diversi tratti del liberalismo: ad esempio, nella "collaborazione competitiva" e nell'intenso impegno per la libertà di espressione e "coltivazione" (del sé), nell'importanza conferita alla conoscenza ed all'implementazione della meritocrazia, aspetti che si affiancano alla sfida alla legislazione della proprietà intellettuale: per molti *hacker* del Free Software le tutele della proprietà intellettuale non costituiscono infatti uno stimolo alle idee e alla conoscenza, ma una forma di restrizione che va contrastata con strumenti legali che trattino la conoscenza e gli altri prodotti della creatività non come proprietà di qualcuno ma come elementi che possano essere liberamente condivisi, distribuiti e modificati (Coleman 2013, 11)[5].

Coleman aggiunge, inoltre, che gli *hacker*, partendo da capisaldi del pensiero liberale come la libertà di espressione, hanno costruito intorno alla loro pratica tecnica un substrato teorico e delle nuove rivendicazioni politiche (come appunto, ad esempio, "Code is Speech")[6], ma che in questo percorso hanno mostrato anche un marcata predilezione per una concezione di lavoro "non

[5]Secondo Coleman, inoltre, l'*hacking* eccede anche in altri sensi il liberalismo: ad esempio, nella sua dimensione gioiosa ed estetica di tensione verso l'autorealizzazione, che sembra in certi casi avvicinare una sensibilità quasi romantica, una forma "elevata" di espressione individuale che pone in primo piano anche originalità, passione e creatività. Gli *hacker* configurerebbero inoltre una concezione piuttosto peculiare del "soggetto liberale", lontana dall'idea di "consumatore motivato dall'interesse personale" ed un "attore razionale" dal punto di vista economico (2013, 11). Si tratterebbe infatti piuttosto di una visione dell'individuo con al centro autonomia, spirito critico e libertà d'espressione, ma nel caso degli *hackers* questa teorizzazione si affianca a momenti di gioia estetica quasi trascendente che trascendono il concetto di "utilità", e nei quali gli hacker arrivano a sottoporsi anche a notevoli privazioni fisiche - come la mancanza di sonno - tendendo quasi ad identificarsi con l'oggetto e con lo scopo della propria attività. Si veda in proposito anche (14). Gli hacker sono inoltre in conflitto anche con una certa tendenza "neoliberale" a ricercare la possibilità di rendere un qualcosa potenziale "proprietà" (privata) dovunque possibile, incluso il software (4). Secondo Coleman, infatti, il conflitto tra libertà di espressione e proprietà intellettuale sarebbe potenzialmente in atto almeno dai tempi della Costituzione Americana, ma non sarebbe stato in precedenza così "visibile" perché sia il *free speech* sia la proprietà intellettuale "occupavano" in passato uno "spazio" molto minore rispetto ad oggi (9-10).

[6] Uno dei momenti "epifanici" di questa tensione tra *hacking* e liberalismo per Coleman è una manifestazione di strada di gruppi di hacker nel 2001 a San Francisco in favore di un programmatore imprigionato per avere scritto codice giudicato in violazione dell'allora appena approvata normativa statunitense sul copyright: durante il corteo viene scandito infatti proprio il motto "Code is Speech". In questo senso, la riformulazione/estensione del *free speech* come libertà di produrre codice e la produzione di Free Software stessa viene ad evidenziare le contraddizioni/linee di frattura con la legislazione della proprietà intellettuale che cercava di espandersi sempre più, anche nei "nuovi" contesti di produzione "immateriale", tanto da essere stata talvolta considerata come l'attuale "motore" per un secondo movimento delle "enclosures" (2013, 10).

alienato", che si avverte soprattutto nella passione creativa intorno all'*hacking* ed nel desiderio di accesso e condivisione dei risultati del lavoro stesso[7].

Utilizzando le categorie di *Protocol: How Control Existsafter Decentralization*di Galloway, si può affermare che la tendenza alla (ri)appropriazione degli spazi, delle potenzialità e dei desideri da parte degli *hacker* è continua (Galloway 2004, 168-9). Incessanti sono però anche i tentativi di mercificazione dei risultati dell'*hacking* da parte del mondo *corporate*, e di "integrare" alcuni aspetti dell'*hacking* nella pratica aziendale. Tali dinamiche possono essere viste a loro volta come un esempio di "appropriazione" dell'etica *hacker* da parte di grandi oligopoli corporativi. Tali soggetti però sembrano interessati ad una concezione di "etica hacker" assai parziale, prevalentemente in quanto immagine di *coolness* e capace di attrarre giovani talenti, o - ancora - come mera "metodologia tecnica": infatti nella sostanza queste entità *corporate* se ne mantengono sensibilmente "lontane", ad esempio non rendendo pubblico il codice delle loro piattaforme proprietarie[8], né le informazioni sugli utenti raccolte, elaborate e vendute (Stumpel 2013, 275-7)[9]. La questione del controllo proprietario delle piattaforme informatiche nella mani di grandi *corporation* sarà discussa più in dettaglio in seguito nella sezione dedicata all'*hacktivism*.

---

[7] Coleman cita anche altri autori, tra i quali i già menzionati Galloway e McKenzieWark, che hanno sottolineato il legame tra la concezione hacker del lavoro appassionato, creativo, accessibile e condiviso e la critica marxiana sul lavoro alienato (2013, 14-15). Sull'approccio hacker al lavoro si veda anche il già citato (Himanen 2001, 107-116).

[8]programmazione informatica ed elettronica il codice sorgente è composto da file di testo che contengono istruzioni che il computer deve eseguire per portare a termine un determinato compito. Il codice sorgente è scritto in un linguaggio di programmazione leggibile e modificabile anche da esseri umani, che in seguito –per semplificare– è spesso compilato, ovvero "tradotto" in un linguaggio comprensibile solo alla macchina, di esecuzione molto più veloce. Un programma può quindi essere a sorgente aperta, quando il codice è disponibile a chiunque sia interessato oppure a sorgente chiusa, ovvero accessibile tipicamente solo ai creatori e/o ai "committenti" del programma stesso.

[9] Un esempio pertinente di questa "appropriazione" *corporate* dell'etica hacker può essere costituito da Facebook, che insiste spesso sulla propria "Hacker Way", ma mantenendo per l'appunto uno strettissimo controllo sul codice sorgente e sugli algoritmi di funzionamento della sua piattaforma. Un altro esempio potrebbe essere costituito da Google, che ha utilizzato parte del codice sorgente liberamente disponibile GNU/Linux per "integrare" Android, un sistema operativo mobile da esso "derivato", nel proprio ecosistema sostanzialmente "proprietario e a sorgente chiusa" di applicativi, algoritmi di ricerca e di plurimiliardaria distribuzione di "marketing diretto". Nelle conclusioni all'edizione del venticinquesimo anniversario di *Hackers: Heroes of the Computer Revolution*, Steven Levy parla anche di questo movimento di continua appropriazione e mercificazione del lavoro hacker da parte del "mondo business", con gli hacker che si "spostano" continuamente verso "nuove frontiere" (2010, 476-477).

Su tali premesse, Geert Lovink conferisce una grande rilevanza alla necessità di (ri)appropriazione dell'intera Rete: nell'introduzione a *UnlikeUs Reader*, Lovink scrive che è necessario rifare di Internet un'infrastruttura veramente indipendente, al fine di difendersi contro il dominio delle *corporation* ed il controllo statale, sostenendo quindi la necessità di mantenere una struttura di rete aperta[10]. Diversamente, come accennato in precedenza, si corre il rischio di studiare ed utilizzare delle "scatole nere" le quali, oltre ad essere dominio di poche grandi *corporation* e delle autorità che possono averne pieno accesso, risultano sconosciute nell'interezza dei loro meccanismi di funzionamento. Anche degli *hacker* possono essere in queste condizioni impossibilitati a "riappropriarsi" o semplicemente a "decodificare" quello che tecnologie oscure e proprietarie effettivamente fanno, e gli *hacker* stessi vengono "esortati" da Lovink a costruire delle piattaforme telematiche alternative (Lovink 2013a, 9-15). L'esclusione dall'accesso al codice sorgente, oltre a depotenziare l'*hacking*, è visto come parte di una vera e propria guerra al *general purposecomputing*[11]: ancora Lovink riprende appunto le tesi in tal senso di Cory Doctorow, che vede questa conflittualità contro il *general purposecomputing* come la "forma generale" di tutte le lotte viste sinora contro il copyright e brevetti nel software, le quali costituirebbero dunque solo una parte di un conflitto più ampio, che dovrebbe divenire sempre più evidente con la crescente pervasività dei computer nella società umana e vista anche la crescente disponibilità di dispositivi utilizzabili anche in ambito domestico di *personal fabrication* e − forse/prossimamente − di personal bio(techno)logy. Mantenere il computer *general purpose* in questo scenario renderebbe infatti assai più arduo conservare il controllo delle tecnologie di produzione, distribuzione, comunicazione ed in pratica di qualsiasi altro ambito dove il *computing* è e/o sarà presente in maniera rilevante. Si tratterebbe di un cambiamento radicale per certi versi simile a quanto avvenuto

[10] *UnlikeUs Reader* si potrebbe definire come una sorta di "manifesto politico dei media tattici", riprendendo ancora le categorie di Alexander Galloway in *Protocol*.

[11] Il *general purpose computer* è in buona sostanza il personal computer a cui siamo (ancora) abituati oggigiorno, cioè un elaboratore in grado di eseguire pressoché qualsiasi sistema operativo o programma venga sviluppato per esso, in contrasto con un possibile concetto futuro di elaboratore "limitato" a poter eseguire invece unicamente il software deciso dal produttore o da autorità politiche: un esempio odierno di condizioni assimilabili può essere ritrovato nelle piattaforme/ecosistemi "ipercontrollati" di tablet e smartphone Apple. Un computer *general purpose* può essere quindi programmato in ogni momento per eseguire una grande varietà di compiti, mentre un computer "specializzato" è di solito predisposto ad eseguire solo una serie predeterminata di compiti che in genere non è modificabile facilmente.

negli anni Settanta con l'avvento del personal *computing*: si vedano ad esempio le possibilità già utilizzabili fornite dalla stampa e dalla scansione 3D di autoprodurre agevolmente vari tipi di oggetti semplicemente creando e/o condividendo dei file di modellazione tridimensionale, inclusi "articoli" la cui detenzione possa essere considerata illecita (Doctorow 2012a)[12]. Queste dinamiche saranno esaminate più in dettaglio successivamente nella sezione dedicata ai makers e al bio*hacking*.

Steven Levy identifica infatti le nuove frontiere dell'*hacking* proprio nel bio*hacking*/DIY biology e nel cosiddetto movimento dei *makers*/Open Hardware, che estendono all'hardware e alla dimensione della produzione materiale il discorso del Free/Open Source Software. Levy si aspetta che gli *hacker* siano protagonisti anche di questa nuova fase di "profonda trasformazione", soprattutto riguardo il bio*hacking*, che si troverebbe ancora in quello che Tim O' Reilly definisce *"fun stage",* diversamente da quanto avviene nel mondo dei *makers*, dove la tendenza verso una prevalenza dello sfruttamento commerciale sembrerebbe invece già avviata[13]. "Grazie" (anche) al bio*hacking*, alle possibilità di "manipolazione liberamente accessibile" del codice informatico e di vari materiali produttivi "inorganici" si aggiungerebbero quindi anche quelle del cosiddetto *wetware* (2010, 477)[14].

2. Hacktivism e free software per l'innovazione politica. In questa sezione si cerca di esaminare il rapporto tra alcune forme di *hacking* e l'innovazione politica: in particolare, sono presi in considerazione il cosiddetto *hacktivism*, considerato come *hacking* politicamente motivato in maniera esplicita, e l'impatto politico del Free Software Movement. Come accennato nella premessa,

[12] Si veda ad esempio http://www.thingiverse.com, sito dedicato principalmente alla condivisione dei file di progettazione/stampa 3D, anche ad esempio per pezzi di ricambio non resi disponibili singolarmente o non più disponibili presso il produttore.

[13] Assai visibili sono le tensioni nelle comunità maker per imprese che decidono di "chiudere" i propri prodotti dopo aver fatto a lungo parte della comunità di condivisione open source in ambito hardware e software: ad esempio il caso MakerBot, probabilmente il più noto produttore di stampanti 3D *consumer,* che ha recentemente deciso di "chiudere il codice sorgente" di alcuni suoi prodotti per cercare di venderli in versione *plug and play* su scala più ampia, ovvero immediatamente pronti all'uso anche per un utente non particolarmente "tecnico/smanettone". Sulla vicenda si veda ad es.: http://makezine.com/2012/09/22/makerbots-mixed-messages-about-open-source-their-future.

[14] *Wetware* in questa accezione è un termine utilizzato per tentare di applicare i concetti di hardware e software agli "organismi viventi", nei quali ultimi si cerca di identificare i corrispondenti componenti/processi.

si possono citare una serie di pratiche di *hacktivism* che pongono in primo piano soprattutto le "potenzialità liberatorie" dell'*hacking*: ad esempio, esperienze di collettivi *hacker* che si sono schierati esplicitamente in conflitti e questioni politiche in varie parti del mondo: ad esempio, il cosiddetto gruppo di Anonymous, oppure the Cult of the Dead Cow e/o svariati altri, tipicamente allo scopo di sostenere "tecnologicamente" gruppi dissidenti in regimi autoritari od anche – ad esempio nei casi RtMark o Etoy – per "sfidare" il mondo *corporate* (Jordan 2002, 127-31; Galloway 2004, 227-32). Nella prospettiva dei cosiddetti *tactical media* – configurazioni di uso delle tecnologie a fini di lotta politica – sono infatti state teorizzate le potenzialità dell'*hacking* come possibilità di intervenire nei conflitti della *network society,* caratterizzati in maniera crescente da forme di lotta di network contro network e da scenari di conflitto (anche) immateriali dei quali "protocolli" gli *hacker* sono visti come i più "autorevoli interpreti" (Galloway 2004, 175; McKenzieWark 2004). Galloway sostiene ad esempio una visione della Rete come sito (della società) del controllo in essa inscritto proprio tramite il cosiddetto "protocollo", inteso come l'insieme di norme e convenzioni che rendono possibile l'esistenza della Rete e delle comunicazioni telematiche. Contro questi "dispositivi" non è possibile una "resistenza" nel senso che al termine viene conferito nella "interpretazione" delle dinamiche di potere delle cosiddette "società della disciplina", termine foucaultiano ripreso da Deleuze, ad esempio nel "Postscript on Control Societies" (Deleuze 1990). Galloway ribadisce che anche le strutture tradizionalmente centralizzate, le *corporation*, il marketing, la distribuzione e molto altro stanno tendendo ad assumere la forma network, tra l'altro per meglio poter contrastare i network che a loro si oppongono: basti pensare alle reti di "sorveglianza pervasiva", all'informatizzazione dei (bio) dati etc.

In questo quadro teorico gli *hacker* sono considerati "attori protocologici" in grado di mettere in discussione il "protocollo" portandolo ad uno stato ipertrofico: una strategia di resistenza tipica proprio della lotta di network contro altri network, diversa da quella tradizionale che si riferiva a conflitti contro entità centralizzate: Galloway cita ad esempio i cosiddetti *Tiger Teams* come forma di organizzazione iperspecializzata, temporanea e flessibile (Galloway 2004, 158-64). La capacità degli *hacker* di individuare la "possibilità" attraverso la conoscenza del protocollo è considerata da Galloway essenziale, anche

politicamente, per la nascita di un desiderio orientato verso qualcosa che è "possibile" volere. A questo proposito Galloway fa riferimento anche ad *A Hacker Manifesto* di McKenzieWark, quando parla dell'*hacking* come il "rendere possibile l'ingresso di nuove cose nel mondo": l'*hacker* è visto qui come in possesso di un istinto utopico, tendente verso l'innovazione ed il cambiamento (McKenzieWark 2004). Galloway riflette sugli effetti tattici di vari conflitti sulla Rete, e su "entità" che adoperano il network come diagramma organizzativo: Internet stessa ed il Free Software Movement, o i virus informatici, visti come indice delle "falle" nel controllo protocologico e proprietario, che possono mandare in ipertrofia il protocollo, portarlo più in là di dove dovrebbe spingersi, una condizione poco sorvegliata in cui esso può essere "scolpito" secondo i propri bisogni. Come accennato già nell'introduzione, Galloway e Thacker ipotizzeranno successivamente in *The Exploit* che in un contesto di conflitto di "network contro altri network" una contrapposizione di tipo asimmetrico sarebbe invece necessaria per superare lo status quo. Tale asimmetria dovrebbe essere resa possibile dall'emergere di qualcosa come un "antiweb" (2007, 149-57).

Come menzionato nella premessa, la teorizzazione delle possibilità di contributo all'innovazione delle forme di lotta e di organizzazione sociopolitica da parte degli *hacker* può essere ritrovata anche in alcuni recenti lavori teorici di GeertLovink, ad esempio nell'introduzione all' *UnlikeUs Reader:* qui Lovink pone in rilievo la privatizzazione e la mancanza di trasparenza della *governance*, dei dati e dei processi nei prevalenti social network telematici corporativi e fa appello alla costruzione ed all'utilizzo di reti sociali alternative veramente indipendenti e trasparenti (Lovink 2013a, 11). In "From Social Media Critique to Organized Networks", ancora Lovink sottolinea ad esempio come tali reti sociali corporative tendano a far emergere non tanto i "legami forti" e le possibilità di cooperazione, ma i cosiddetti "legami deboli", in un quadro di impoverimento delle possibilità di interazione "incorniciate" fortemente e riduzionisticamente – nella dinamica binaria mi piace/non mi piace, piuttosto che caratterizzate dalla effettiva possibilità di collaborazione ai fini di un'innovazione politica o sociale (Lovink 2013b).

Una serie di progetti di costruzione di reti sociali telematiche alternative "indipendenti" è stata in effetti intrapresa, sviluppando network caratterizzati

generalmente da maggiore apertura dal punto di vista della *governance*, della trasparenza e delle libertà degli utenti: dall'esperienza di Diaspora, l'esempio forse più noto, a quello del network utilizzato soprattutto dagli *indignados* spagnoli (Lorea), o ancora all'infrastruttura costruita dal movimento Occupy negli Stati Uniti per la comunicazione interna (InterOccupy.net), la quale ultima viene combinata ad un uso "complementare" e ridondante delle reti sociali corporative quali ad esempio Facebook e Twitter anche al fine di acquisire visibilità e "comunicare" in maniera più efficace a persone esterne al movimento (Terranova e Donovan 2013, 296-311).

Molto si è detto inoltre a proposito di meriti e limiti delle modalità di configurazione di rete maggiormente diffuse (centralizzata, distribuita e decentrata), proponendo ad esempio un controverso modello di "reti federate" e sperimentando modelli di social network in cui gli utenti possano autodeterminare in misura maggiore la trasparenza dei processi, la gestione dei loro dati personali ed il *framing* tecnico e sociopolitico del progetto stesso, determinato da una comunità di utenti e sviluppatori e non da un soggetto privato il cui fine principale sia il profitto[15]. Pur registrando un certo interesse per le reti sociali alternative, i progetti sinora realizzati non sembrano essere riusciti a superare gli ostacoli posti ad esempio dal cosiddetto *network effect* di cui al momento beneficiano alcune piattaforme corporative oligopoliste, realizzando però alcune esperienze di sicuro interesse e dimostrando se non altro che sono possibili dei "modelli alternativi", che per ora non sono riusciti a diffondersi su vasta scala (Sevignani 2013, 323-37; Cabello, Franco e Haché 2013, 338-46).

Un altro potenziale non trascurabile di innovazione politica intorno all'*hacking* può essere ritrovato nell'esperienza del Free Software Movement, che è invece riuscito a raggiungere dimensioni di scala assai più ampie, anche considerando la cosiddetta biforcazione tra il Free Software e l'Open Source Software, avvenuta a partire dal 1998: ovvero, tra un approccio – quello dell'Open Source Software – maggiormente pragmatico ed attento alle esigenze del mercato e della possibilità di profitto e la "visione" del Free Software Movement, incentrata sulle motivazioni etico-politiche dell'*hacking* e del software libero, come si possono ritrovare in Richard Stallman e nella Free

[15] Per una descrizione non eccessivamente tecnica delle varie topologie di network si può far riferimento a http://networkcultures.org/wpmu/unlikeus/resources/articles/what-is-a-federated-network.

Software Foundation da lui fondata (Coleman 2013, 78-9)[16]. L'impatto politico delle pratiche degli *hacker* del Free Software Movement sull'attuale *network society* è infatti tra i temi maggiormente dibattuti, originariamente soprattutto nel campo dei brevetti e dei diritti di autore. Ormai però l'influenza del Free Software può essere considerata travalicare ampiamente l'ambito originario come paradigma organizzativo, di fruizione e di distribuzione, anche grazie ad esperienze come quelle del Movimento della Free Culture ispirato da Lawrence Lessig (Coleman 2013, 196-200). Come si è visto anche in precedenza, la necessità di *open access*, di democratizzazione e partecipazione, di trasparenza e di libero flusso delle informazioni sono temi che sono storicamente presenti all'interno delle etiche e delle pratiche *hacker*. D'altro canto, secondo Coleman, anche quando i movimenti del Free Software sono sembrati non prendere posizioni politiche esplicitamente, il solo impatto dato dalla loro esistenza come "alternativa funzionante" ai modelli di organizzazione e sviluppo "opachi e chiusi" è considerato aver avuto una ampia rilevanza, anche per il loro prevalente "agnosticismo politico": un coinvolgimento più diretto delle comunità di sviluppatori lo si è infatti potuto osservare soprattutto quando fossero in discussione argomenti direttamente collegati al loro *hacking*. Questo avrebbe comportato una facilità di "leggibilità sociale" e di adozione (dei paradigmi) del Free Software da parte di individui posizionati socialmente in maniera molto varia, proprio per la mancata "polarizzazione politica" (Coleman 2013, 187-90).

D'altra parte, come si ricordava in precedenza, il forte "appeal" sia economico sia simbolico dell'*hacking* e del modello dell'apertura e del libero accesso è stato non di rado utilizzato dal mondo *corporate* come strategia di cattura di consenso e/o degli *hacker* stessi incorporando e appropriandosi di alcuni elementi o pratiche *hacker* per la propria *mission* aziendale: questo per certi versi "risuona" con la tesi di Castells sull'*hacking* come una componente rilevante/necessaria dello spirito dell'età dell'informazione (Castells 2001, 132).

3. Makers, biohackers e prospettive di empowerment dal basso. In questa sezione, anche qui senza pretesa di completezza ed esaustività, cerco di delineare alcuni recenti "fenomeni sociopolitici" relazionabili al mondo *hacker*, i

[16] Vale la pena notare che una delle più diffuse licenze del Free Software, la GPL ideata dallo stesso Stallman, è stata vista anche come un *hack* della legislazione del copyright. Si veda in proposito anche (2013, 70).

quali sono stati considerati contenere un rilevante potenziale di innovazione politica, non sempre esplicitamente "evidenziata". Tra gli esempi maggiormente noti vi sono probabilmente la nascita del cosiddetto movimento dell'Open Hardware e dei *makers* e le pratiche del bio*hacking*.

Il Maker/Open Hardware Movement, come accennato nella parte introduttiva, è per certi versi una (ri)trasposizione di elementi di etiche e pratiche *hacker* "storici" nella realizzazione materiale e nella produzione di hardware[17], reso possibile anche grazie alla disponibilità negli ultimi anni di strumenti di prototipazione a basso costo utilizzabili dal cosiddetto "utente domestico", oltre che – ad esempio – dai comparti dell'istruzione e della piccola/media impresa: tra gli altri sono da menzionare la "piattaforma" Arduino, piattaforme di sviluppo Open Hardware Linux embedded[18], e la diffusione di tecnologie di scansione, stampa e lavorazione 3D (Anderson 2013, 64-127). La nascita di un Maker Movement è collocabile intorno al 2005: diversamente dalle pratiche *hacker* storiche, si osserva fin dagli inizi un più marcato coinvolgimento e spinta *corporate* da parte ad esempio di gruppi editoriali *geekfriendly* come O'Reilly con il Make Magazine i quali, muovendosi nel solco dell'eredità culturale del Whole Earth Catalog e della tradizione DIY, vi vedono sin dai primi sviluppi anche una possibilità di business fatta di vendita di prodotti editoriali, componentistica ed eventi. A tutt'oggi il Make Magazine è forse il più visibile ed influente *trendsetter* nel mondo maker: O'Reilly è infatti il principale organizzatore ed il titolare del marchio delle cosiddette Maker Faires. Tali eventi possono essere visti come l'equivalente delle "conferenze hacker" e contribuiscono in maniera non trascurabile ad "orientare" lo sviluppo, la percezione di sé e la visibilità dei vari prodotti ed esperienze delle numerose "comunità locali" di maker nel mondo, non trascurando l'interessante modello dei Fab Lab (Tocchetti 2012)[19].

Il bio*hacking* è invece una pratica che può forse considerarsi ancora più recente e, come si ricordava in precedenza, è spesso considerato come l'attuale

[17] Per una visione in prospettiva storica dell'*hacking* dell'hardware si può ricorrere ad esempio al già citato Levy (2010).
[18] Si tratta di schede elettroniche, generalmente open hardware e software, a basso costo e facilmente programmabili, che permettono tra l'altro di leggere sensori, pilotare parti meccaniche o anche macchinari più complessi.
[19] I Fab Lab sono luoghi accessibili al pubblico attrezzati per la produzione e la prototipazione rapida dal basso, a costo ridotto e su piccola scala, dove si possono scambiare idee, competenze ed utilizzare in maniera relativamente economica le strumentazioni necessarie: http://www.fabfoundation.org/fab-labs.

frontiera dell'*hacking*. DIYbio è il maggiore dei network "informali" di biohacker, nato a Boston nel 2008 da un'idea di Cowell MacKenzie e Jason Bobe, quest'ultimo un dirigente del Personal Genome Project alla Harvard Medical School. Il movimento cerca di dare una dimensione collettiva e strumenti open source alla ricerca indipendente in campo biotecnologico condotta in ambiente non *business* e non istituzionale, basandosi su Internet come strumento di condivisione ed organizzazione in diversi gruppi a livello planetario. Il punto di partenza è la necessità di apertura dei saperi scientifici iperspecializzati verso la società, per un dibattito politico maggiormente orizzontale e meno "asimmetrico" su temi di crescente rilevanza nella contemporaneità (Landrain et al. 2013; Delfanti 2013, 111-29). Si tratta di un fenomeno per certi versi ancora ad uno stadio sperimentale o di ricerca "pura" (non ha ancora ottenuto risultati scientifici di grande impatto), con un coinvolgimento *corporate* al momento apparentemente assai più marginale che nel Maker Movement[20]. Questo lo rende per certi versi di maggiore interesse, in quanto orientato in misura minore alla ricerca della commercializzazione delle idee, aspetto che non può dirsi però del tutto assente: il rapporto nei confronti delle istituzioni scientifiche e – soprattutto – verso il mondo *corporate* è dunque di solito piuttosto "ambivalente" (Delfanti 2013, 57-8). Particolarmente interessanti ai fini della disamina del possibile impatto di questi movimenti sull'innovazione politica possono essere ad esempio anche esperienze di autocostruzione di materiali e strumenti di laboratorio open source e basso costo che abbassano le soglie d'ingresso al sapere, all'istruzione e alla pratica scientifica; la produzione e distribuzione di kit open source di autocostruzione di sensori a basso costo di inquinamento ambientale, sofisticazioni alimentari, rilevamento di infezioni di vario genere o di bioelettronica a basso impatto ambientale, come anche la decostruzione e riconfigurazione open/con costi ridotti di oggetti esistenti.

Tali iniziative possono essere viste come altrettanti strumenti di *empowerment,* costruiti e diffusi anche da singoli o piccoli collettivi indipendenti che possono permettere di ricavare, in maniera semplice ed economica, informazioni di vitale importanza per le comunità di appartenenza, anche ai fini di portare avanti con la maggiore consapevolezza possibile rivendicazioni e

[20] Si veda però ad esempio la recente iniziativa editoriale nel bio*hacking* dello stesso O'Reilly, intesa probabilmente a replicare l'esperienza del Make Magazine. http://www.oreilly.com/biocoder.

battaglie sociopolitiche su questi ed altri temi, rendendo DIYbio anche un luogo per esplorare le biotecnologie e per incoraggiare appunto la partecipazione dal basso nel dibattito e nelle decisioni tecno-scientifiche. Ad esempio, il centro La Paillasse a Parigi si pone tra gli obiettivi principali della sua attività proprio l'*empowerment* dei cittadini per permettere loro di partecipare alle scelte che riguardano l'uso di queste tecnologie e preserva la maggiore continuità possibile – si potrebbe così riassumere – con le pratiche *hacker* intese nella loro accezione "storica", ovvero, come ormai "noto", con gli elementi di apertura, condivisione, partecipazione, libero flusso di informazioni, creatività, innovazione ed autonomia (Landrain et al 2012)[21]. All'interno del bio*hacking* sono presenti inoltre anche componenti di "reazione" contro l'ondata di privatizzazioni e brevetti nel settore biotecnologico negli ultimi venti anni: l'*hacker* e biologa DIY Meredith Patterson nel suo "A Biopunk Manifesto" sostiene un "diritto alla ricerca" sullo stesso piano della libertà di culto o di espressione, per fare del mondo "un posto che ognuno può essere in grado di comprendere", anche al di fuori di costosissimi laboratori (Patterson 2010).

Spinte innovative dal basso come quelle citate possono influire sul quadro politico in molti modi, contribuendo sia a "distribuire" delle forme di controllo autonomo dell'operato ad esempio di governi e *corporation,* sia – ancora – a coadiuvare il rilancio glocale della micro/piccola impresa, tema potenzialmente centrale, ad esempio, nell'agenda politica del lavoro italiana vista la rilevanza di taledimensione organizzativa nel comparto produttivo nazionale[22]. Delfanti insiste però sulle complesse dinamiche dell'appropriazione /riappropriazione tra (bio)*hacker* e (bio)capitalismo: secondo l'autore da un lato risulta infatti arduo separare bio*hacker* e capitalismo, in quanto egli ritiene che, più che essere un

[21] Altri progetti di particolare interesse in questo senso: ad esempio, riconducibili alla cosiddetta componentistica bioelettronica biodegradabile per far fronte alla pesante impronta ecologica generata dal ciclo dei materiali per produrre componenti, dalla crescente penuria di alcuni di essi alle tecniche sempre più invasive e costose di estrazione. Come altro esempio, un biosensore allo yogurt a basso costo, autocostruito ed open source, che segnala la contaminazione di melamina nel latte. Proprio presso il centro Lapalaisse si sta lavorando a un inchiostro biologico prodotto da batteri che costituisca una alternativa biodegradabile e non inquinante agli inchiostri industriali attualmente in uso. Un altro ulteriore esempio può essere infine costituito da Amplino, un progetto open source ed a basso costo per la rilevazione rapida della malaria che può contribuire ad aprire orizzonti di welfare ed *empowerment* sanitario in luoghi del pianeta dove questo poteva in precedenza sembrare irrealizzabile.

[22] Si veda in proposito, ad esempio, il modello di organizzazione di percorsi di (ri)appropriazione di competitività portato avanti da Roland, ad esempio attraverso l'iniziativa "Artigiano tecnologico": http://www.rolandforum.com .

oggetto di cooptazione del capitalismo informatico, gli *hacker* ne siano stati in buona parte un elemento costitutivo. D'altra parte però, come si è visto, con le loro pratiche i biohacker sembrano anche possedere una forte *agency* per creare innovazione politica (2013, 139).

4. Conclusioni. In questo testo si è cercato di illustrare l'importanza delle culture, delle etiche e delle pratiche *hacker* nell'odierna società del network, delimitando il campo ad alcuni aspetti di esse maggiormente rilevanti ai fini del rapporto con l'innovazione politica. La relativamente lunga e complessa storia degli *hacker* appare infatti sufficiente a differenziare questo mondo in modo piuttosto netto dallo stereotipo banalizzante di "criminali dell'era dell'informazione", che ancora oggi numerosi media *mainstream* associano al termine "hacker" ed ai vari gruppi e comunità che in esso si riconoscono.

Nel corso di questo lavoro è stato possibile vedere come il mondo *hacker* racchiuda invece una molteplicità di gruppi e di esperienze, che sono state esaminate nella loro varietà di etiche e posizioni politiche: dalle ultime "tendenze" insieme promettenti e controverse del *making* e del bio*hacking*, ad un *hacking* motivato politicamente in maniera esplicita nei gruppi hacktivisti, o ancora all'influenza non meno rilevante di gruppi *hacker* come quelli legati al cosiddetto movimento del Free/Open Source Software, i quali ultimi – diversamente – tendono a prendere posizione politicamente soprattutto per questioni strettamente legate alle pratiche dell'*hacking*. La relativamente ampia rilevanza degli *hacker* del Free Software è determinata in buona parte, come si è visto, dalla loro stessa esistenza come modelli "alternativi" concretamente funzionanti di pratiche organizzative democratizzate, autonome e trasparenti, caratterizzate dalla condivisione delle conoscenze prodotte dagli *hacker* in questione, le quali non sono divenute proprietà intellettuale ed industriale "esclusiva" di pochi, e sono riuscite a travalicare ampiamente come "impatto" gli ambiti originari di applicazione. Nonostante la varietà di modulazioni dell'*hacking*, si è potuto osservare un più ampio quadro di riferimento culturale comune: gli *hacker* contribuiscono, come si è visto più volte, a portare in primo piano questioni di rilievo come la libertà d'informazione ed espressione, il diritto di accesso al libero flusso delle informazioni stesse, l'apertura la trasparenza e la

partecipazione nei sistemi tecnologici ed istituzionali, la passione creativa per l'innovazione e la libera condivisione dei saperi.

All'interno di queste tematiche, il mondo *hacker* appare percorso da importanti tensioni: da un lato, infatti, abbiamo un potenziale dell'*hacking* come strumento di possibilità di resistenza e democratizzazione che può contribuire a generare e favorire pratiche di riappropriazione di spazi, saperi, prodotti tecnologici, di rapporto non alienato con il lavoro e con i tempi e le modalità di produzione. D'altro canto, la frequenza e la facilità con cui alcune pratiche e risultati dell'*hacking* sono incorporati dal capitalismo della società del network ai fini di un rinnovamento del capitalismo stesso e dello sviluppo di nuovi modelli di business e di profitto ha favorito talvolta una visione dell'*hacking* come inestricabilmente legato al mondo corporativo, fattore di rinnovamento "interno" all'ordine sociale tecnocratico dominante.

In un contesto di progressiva estensione del cosiddetto *computing* pervasivo a tutti gli aspetti della vita degli individui, compreso quello bio(tecno)logico, l'odierna società del network appare infatti "dominata" da oligopoli corporativi e governativi enormi, inquietanti ed "oscuri" nelle loro modalità di funzionamento, soprattutto in forma di piattaforme (bio)tecnologiche ed informatiche onnipresenti e "distribuite". Tali piattaforme appaiono, infatti, favorire in apparenza il libero flusso delle informazioni, ma le loro modalità operative sono note nella loro interezza unicamente a chi le determina e ne detiene il controllo esclusivo, in particolare quello sulla proprietà intellettuale ed industriale ad esse associata.

In misura assai maggiore all'essere considerati come meri "interpreti privilegiati" (degli) strumenti di innovazione tecnopolitica, l'importanza degli *hacker* risulta piuttosto "segno" di notevoli mutamenti nei soggetti e nella pratica politica osservati anche nella crescente rilevanza di forme organizzative peculiari dell'odierna società del network e dell'informazione: come si è appena visto, le modulazioni dell'*hacking* presenti e future appaiono cruciali ai fini della continua riconfigurazione del "controllo" della società del network, sia in quanto potenziali elementi di rinnovamento, non di rado cooptati/incorporati o addirittura inestricabili dal (bio)capitalismo del network, sia come strumenti di decodifica, resistenza, e democratizzazione della "oscurità" di tali diagrammi organizzativi tecno-scientifici "dominanti". L'*hacking* risulta infatti "sito" di

possibilità di realizzazione trasparente, creativa, innovativa ed altrettanto "distribuita" di spazi e di pratiche di "smascheramento", liberazione e di (ri)appropriazione rispetto a tali diagrammi organizzativi, anche, ad esempio, attraverso l'abilità di sviluppare piattaforme (bio)tecnologiche realmente indipendenti e condivise.

Bibliografia

Anderson, Chris. 2012. *Makers: The New Industrial Revolution*. New York: Crown Business.

Cabello, Florencio; Marta G. Franco; Alexandra Haché. 2013. "Towards a Free Federated Social Web: Lorea Takes the Networks!". In *Unlike Us Reader: Social Media Monopolies and Their Alternatives*, edited by G. Lovink e M. Rasch. Amsterdam: Institute of Network Cultures.

Castells, Manuel. 2001. "L'informazionalismo e la network society". In *L'etica hacker e lo spirito dell'età dell'informazione*, traduzione di Fabio Zucchella, a cura di P. Himanen, 117-132. Milano: Feltrinelli.

Coleman, E. Gabriella. 2013. *Coding Freedom: the Ethics and Aesthetics of Hacking*. Princeton: Princeton University Press.

Deleuze, Gilles. 1990. "Postscript on Control Societies". In *Negotiations*, traduzione di Martin Joughin (traduzione alternativa come "Postscript on the Societies of Control". 1997. In *October: The Second Decade, 1986-1996*, ed. Rosalind Krauss et al. Cambridge: MIT Press.) New York: Columbia University Press.

Delfanti, Alessandro. 2013. *Biohackers: The Politics of Open Science*. London: Pluto Press.

Doctorow, Cory. 2012a. "Lockdown: The Coming War on General-Purpose Computing". http://boingboing.net/2012/01/10/lockdown.html.

Doctorow, Cory. 2012b. "The Coming Civil War over General Purpose Computing". http://boingboing.net/2012/08/23/civilwar.html.

Galloway, Alexander R. 2004. *Protocol: How Control Exists after Decentralization.* Cambridge, Mass: MIT Press.

Galloway, Alexander R., e Eugene Thacker. 2007. *The Exploit: A Theory of Networks.* Minneapolis: University of Minnesota Press.

Himanen, Pekka. 2001. *L'etica hacker e lo spirito dell'età dell'informazione*, traduzione di Fabio Zucchella. Milano: Feltrinelli.

Jordan, Tim. 2002. *Activism! Direct Action, Hacktivism and the Future of Society.* London: Reaktion Books.

Landrain, Thomas; Morgan Meyer; Ariel Martin Perez; Remi Sussan. 2013. "Do-it-yourself Biology: Challenges and Promises for an Open Science and Technology Movement" in *Syst Synth Biol*, vol. 7, n. 3, 115-126.

Levy, Steven. (1984) 2010. *Hackers: Heroes of the Computer Revolution.* 25th anniversary edition, con una nuova postfazione dell'autore. Sebastopol, CA: O'Reilly Media.

Lovink, Geert. 2013a. "A World Beyond Facebook: Introduction to the Unlike Us Reader". In *Unlike Us Reader: Social Media Monopolies and Their Alternatives*, edited by G. Lovink e M. Rasch, 9-15. Amsterdam: Institute of Network Cultures.

Lovink, Geert. 2013b. "From Social Media Critique to Organized Networks". Discorso all'Académie d'été de l'école de philosophie pharmakon.fr. http://www.youtube.com/watch?v=WX4qUrNVQb8.

Lovink, Geert e Miriam Rasch (a caura di). 2013. *Unlike Us Reader: Social Media Monopolies and Their Alternatives*. Amsterdam: Institute of Network Cultures.

Manovich, Lev. 2013. *Software Takes Command.* NewYork: Bloomsbury, 2013.

McKenzie Wark, Kenneth. 2004. *A Hacker Manifesto*. Cambridge, MA: Harvard University Press. Versione 4.0 (disponibile a http://subsol.c3.hu/subsol_2/contributors0/warktext.html).

Meyer, Morgan. 2012. "Build Your Own Lab: Do-it-yourself Biology and the Rise of Citizen Biotech-Economies". In *Journal of Peer Production*, 2: "Bio/hardware*hacking*". http://peerproduction.net/issues/issue-2/invited-comments/build-your-own-lab.

Patterson, Meredith. 2010. "A Biopunk Manifesto", intervento al simposio "Outlaw Biology? Public Participation in the Age of Big Bio" presso "UCLA Center for Society and Genetics" a Los Angeles. http://vimeo.com/18201825.

Raymond, Eric S. 2001. "How to Become a Hacker". Versione "aggiornata" in Rete disponibile a: http://www.catb.org/esr/faqs/hacker-howto.html.

Raymond, Eric S. 1996. *The New Hacker's Dictionary.* Cambridge, Mass: MIT Press.

Sevignani, Sebastian. 2013. “Facebook vs. Diaspora: A Critical Study”. In *Unlike Us Reader: Social Media Monopolies and Their Alternatives*, edited by G. Lovink e M. Rasch, 323-337. Amsterdam: Institute of Network Cultures.

Stumpel, Marc. 2013. “Facebook Resistance: Augmented Freedom”. In *Unlike Us Reader: Social Media Monopolies and Their Alternatives*, edited by G. Lovink e M. Rasch, 274-288. Amsterdam: Institute of Network Cultures.

Terranova, Tiziana. 2004. *Network Culture: Politics for the Information Age.* London: Pluto Press.

Terranova, Tiziana e Joan Donovan. 2013. “Occupy Social Networks: The Paradoxes of Using Corporate Social Media in Networked Movements.” In *Unlike Us Reader: Social Media Monopolies and Their Alternatives*, edited by G. Lovink e M. Rasch, 296-311. Amsterdam: Institute of Network Cultures.

Tocchetti, Sara. 2012. “DIY Biologists as ‘Makers’ of Personal Biologies: How MAKE Magazine and Maker Faires Contribute in Constituting Biology as a Personal Technology”. In *Journal of Peer Production*, 2: “Bio/hardware *hacking*”. http://peerproduction.net/issues/issue-2/peer-reviewed-papers/diybiologists-as-makers//?format=pdf.

Torvalds, Linus. 2001. “Come agiscono gli hacker? Ovvero, la Legge di Linus”. In *L'etica hacker e lo spirito dell'età dell'informazione*, traduzione di Fabio Zucchella, a cura di P. Himanen, 9-12. Milano: Feltrinelli.