8º interprogramas de mestrado
FACULDADE CÁSPER LÍBERO

HACKING COMO EXPRESSÃO DO NOVO ATIVISMO

Murilo Bansi Machado[1]

Resumo

Este trabalho discute a prática do hacking de computador como expressão de um novo ativismo político, marcado pela incorporação dos hackers e das redes de comunicação. Para tanto, remete-se ao coletivo de hackers ativistas Anonymous, objeto de uma pesquisa em curso. A fim de lançar bases teóricas acerca do hacktivismo, recorre-se aos *software studies* e à chamada sociedade do controle. Conclui-se que o hacking pode ser considerado expressão de um novo ativismo político à medida que resiste ao controle protocológico, de forma que os hackers representam atores políticos de grande relevância.

Palavras-chave: Hacking; Hacktivismo; Anonymous; Estudos de software; Sociedade do controle.

Após um período de latência, que vigorou desde o início dos anos 2000 até quase o final da mesma década, o hacking de computador renasceu em sua forma mais politicamente transgressiva: o hacktivismo, ou ativismo hacker. Esse renascimento – que pode ser creditado, em grande medida, às ações empreendidas pela rede hacktivista Anonymous, um movimento distribuído em rede, sem lideranças e sem núcleo central de decisões – ocorre em um momento no qual um ecossistema comunicacional fundado em protocolos de controle e na supremacia do software tende à ubiquidade. E é precisamente nesse cenário, por sua natureza, que os hackers ativistas se tornam atores políticos de grande relevância.

É certo que nossas sociedades caminham, com velocidade cada vez mais incomum, para o protagonismo dessa forma de comunicação, que se consolida à medida que as tecnologias de informação e comunicação se tornam mais pervasivas. De acordo com o sociólogo Manuel Castells (2007), esse ecossistema comunicacional permite que diversos atores sociais interfiram no campo midiático e, portanto, nas relações de poder – de modo

[1] Mestrando vinculado ao Programa de Pós-Graduação em Ciências Humanas e Sociais da Universidade Federal do ABC (UFABC). E-mail: murilo.machado@ufabc.edu.br.

que este, segundo o autor, opera atualmente em uma nova estrutura tecnológica, sem a qual os movimentos sociais da "era da informação" e as novas formas de mobilização e resistência não poderiam ser concebidos. Com isso, Castells observa que as redes digitais de comunicação tornam-se a porta de entrada para o exercício do contrapoder, pois permitem que os mais diversos atores participem ativamente nos processos de comunicação global.

Neste trabalho, pretendemos mostrar que os hackers se tornam um desses atores cuja relevância política não deve ser relegada a segundo plano. E, para compreender de que forma este novo ativismo político é marcado pela incorporação dos hackers em seu processo, recorreremos a duas perspectivas que nos ajudam a pensar uma nova dimensão da sociedade contemporânea: a cultura do software e a sociedade de controle.

O RENASCIMENTO DO HACKING

Primeiramente, convém apontar que trataremos do hacking especificamente como uma atividade relacionada à programação, ou seja, à elaboração e modificação de programas de computador. Trata-se, conforme observaram Pekka Himanen (2001), Eric Raymond (on-line) e tantos outros pesquisadores e ativistas, de uma atividade lúdica, criativa, muitas vezes ativista, envolvendo um conjunto de hábitos e preceitos específicos que, em última instância, configuram-se em uma ética própria – a ética hacker. No entanto, não trabalharemos com uma noção muito cara a estes autores: a de que a ética hacker pode se estender aos vários níveis do campo social, de modo que é possível encontrar "hackers" entre os mais diversos profissionais, desde que estes sejam partidários da referida ética.

Em segundo lugar, faz-se necessário observar que nossa interpretação quanto aos hackers difere, e muito, daquela que os considera cibercriminosos ou mesmo ciberterroristas. Com base nela, hackers seriam os autores de ações como roubo de senhas, invasão de informações sigilosas, destruição de bancos de dados, e tantas outras. Essa interpretação, que também está presente, de certa maneira, na literatura acadêmica,[2] tem sido insistentemente propalada sobretudo pelos meios de comunicação. Todavia, já na década de 1980, hackers membros das comunidades de software livre combateram esse uso

[2] Cf. Dening (2001) e Arquilla e Ronfeldt (1997), por exemplo.

malogrado do termo, criando, para tanto, a alcunha "cracker" para designar pessoas que praticam esse tipo de vandalismo digital.

As origens do hacking de computador remontam à década de 1960, quando estudantes da área de computação passavam madrugadas inteiras em volta de máquinas que tinham a dimensão de salas gigantescas. E, com o surgimento da microinformática, em meados dos anos 1970, o hacking se firma em definitivo. Naqueles primórdios, os hackers eram positivamente vistos como pessoas que faziam da programação de computador um hobby, resolvendo problemas tecnológicos no espírito do faça você mesmo (Galloway, 2004).

Entretanto, observa Alexander Galloway (Idem:153), em meados dos anos 1980, "depois de uma combinação de tecnofobia pública e de uma agressiva legislação governamental, a identidade do hacker mudou […] para a de um fora-da-lei digital". O autor recorre a artigos e notícias veiculados à época pela imprensa norte-americana para ilustrar essa transição. Os hackers passaram a ser apontados como sabotadores e criminosos, frequentemente associados à invasão de sistemas e à produção e disseminação dos vírus de computador, que começavam a se espalhar com notável rapidez. Não raro eram noticiadas prisões exemplares desses "hackers criminosos". Esta imagem se manteve ao longo dos anos 1990.

A história do hacking teve um novo marco histórico no ano de 2001, por conta dos ataques terroristas às torres gêmeas do World Trade Center. A partir de então, passou-se a ter uma nova e incomum pressão pela política de vigilância sobre a população, sobretudo pela Internet, nos Estados Unidos e em boa parte do mundo. Vegh (2003) mostra que essa nova política reforçou a imagem dos hackers como potenciais ciberterroristas a serem combatidos sob os esforços da tão propalada guerra contra o terror. Com isso, "na virada do milênio, o termo hacker perdeu todo o seu significado original. Agora, quando as pessoas dizem hacker, elas querem dizer "terroristas" (Galloway, 2004:157).

Essa transformação se refletiu, evidentemente, na própria prática do hacking, que passou a ser profundamente desencorajada, quando não ameaçada. Embora essa prática não tenha deixado de existir – ao contrário, ganhou mais adeptos a cada dia em todo o mundo, principalmente nas comunidades de software livre –, pelo fato de seu significado original

ter sido completamente subvertido, o hacking inevitavelmente saiu dos holofotes, caindo em descrédito.

AS MÚLTIPLAS FACES DOS ANONYMOUS

Mas foi no final dos anos 2000 que se notou um verdadeiro renascimento do hacking, bem como do ativismo político associado a ele. Isso se deveu, notadamente, às ações do coletivo Anonymous, sobretudo a partir de 2008, quando o coletivo se voltou à ação política de massa.

De acordo com a antropóloga hacker Gabriella Coleman (2011), os Anonymous não são passíveis de uma classificação rígida. Isso porque a rede hacktivista contempla uma vasta gama de membros e seu nome é usado, em muitos casos, por quais pessoas que queiram realizar suas ações pela Internet ou mesmo em protestos de rua. Além disso, não tem uma liderança central, estrutura hierárquica ou mesmo um centro geográfico. Por isso, seria incorreto dizer que os Anonymous se configurem em um grupo. Trata-se, primeiramente, de uma vasta e heterogênea rede composta por grupos e indivíduos espalhados por todo o mundo, valendo-se da alcunha "Anonymous" e da máscara de Guy Fawkes,[3] vastamente popularizada pelo filme *V de Vingança*, para realizarem ações políticas diretas.

Originalmente, os primeiros registros da rede remontam ao 4Chan, um fórum de imagens muito popular nos Estados Unidos cuja característica principal (ou uma delas) é o anonimato. Àquele momento, os Anonymous se pautavam pelo princípio do *lulz*, uma corruptela de "LOL" (*laughing out loud*, ou rindo em voz alta, em tradução literal), e suas ações mais frequentes estavam associadas ao *trolling* – chacota, provocação, desestabilização da ordem, valendo-se de muito humor, sobre determinada pessoa ou organização. No 4Chan, essas ações eram coordenadas para que se aplicassem trotes telefônicos, muitos pedidos de pizzas para a casa de certo "alvo", revelação de informações

[3] Guy Fawkes foi um soldado inglês que tentou explodir o Parlamento britânico durante a Conspiração da Pólvora, em 1605. Responsável por guardar os barris de pólvora que seriam utilizados na explosão, ele acabou preso e condenado à morte.

pessoais destes alvos, ataques DDoS,[4] entre outros. Pelo menos até o ano de 2006, os Anonymous coordenaram várias dessas ações.

Em 2008, Coleman (2011) observa que os Anonymous passaram "do *lulz* à ação coletiva", transformando-se em um grupo de ativistas políticos, tendo como principal bandeira a liberdade de expressão, sobretudo na Internet. O episódio que marcou essa transição foi uma imensa onda de *trolling* contra a Igreja da Cientologia norte-americana. A Igreja produziu um vídeo, originalmente destinado apenas a seu público interno, em que o ator Tom Cruise louvava a doutrina praticada pela instituição. Ocorre que o vídeo vazou, tendo sido publicado por inúmeros sites e blogs. A Igreja, por sua vez, tentou barrar a circulação desse conteúdo ameaçando aqueles que o haviam publicado com ações na justiça por violações de direito autoral.

Diante disso, os Anonymous orquestraram uma imensa onda de *trolling* contra a Igreja da Cientologia em janeiro de 2008. Foram inúmeros posts em sites, blogs e redes sociais chamando a atenção para o fato de que a instituição estava adotando práticas que feriam a liberdade de expressão. Também se praticaram ataques DDoS contra sites da Igreja. Mas talvez o principal conteúdo produzido pelo grupo tenha sido um vídeo[5] (prática que se tornaria corriqueira nas próximas ações dos Anonymous) declarando guerra contra a instituição. Rapidamente, o vídeo ganhou circulação em escala global e, em 10 fevereiro daquele ano, os participantes decidiram ir às ruas: mais de sete mil pessoas saíram em protesto, sobretudo em frente às sedes da Igreja na América do Norte, Europa e Austrália. Os manifestantes, já naquele momento, passaram a usar a máscara que imita o rosto de Guy Fawkes. Desde então, a máscara se tornaria o símbolo da rede.

---

[4] DDoS, ou *Distributed Denial of Service* (ataque distribuído de negação de serviço, como é conhecido em português), é uma prática que consiste em acessar repetidas vezes determinado servidor de maneira tal, que este acaba por não suportar a sobrecarga. Com isso, ele para de oferecer seus serviços. Na prática, os sites que estão hospedados nos servidores que foram vítimas de um ataque DDoS bem-sucedido saem do ar. O fato de ser distribuído significa que (1) ou vários usuários ativistas passaram a acessar determinado site de maneira ininterrupta, geralmente por meio de um software específico que permite atualizar a página em velocidade tamanha, que um dedo humano não conseguiria acompanhar; (2) ou um computador principal (o mestre) obteve o comando de vários outros computadores (zumbis ou escravos), forçando-os a praticarem esta tarefa de ataque de negação de serviço. É preciso observar que, diferentemente de práticas criminosas, o DDoS não acarreta alteração de conteúdo das páginas, nem mesmo roubo ou danificação de suas informações. Ele simplesmente as desabilita. Por isso, alguns ativistas preferem chamá-lo de "protesto" em vez de "ataque" (Cf. STALLMAN, 2011).

[5] Disponível em: <www.youtube.com/watch?v=JCbKv9yiLiQ>. Acesso em 7 dez. 2011.

Dois anos mais tarde, em 2010, os Anonymous mais uma vez chamaram a atenção de todo o mundo com outra grande operação – desta vez, com o protagonismo mais explícito dos hackers. O caso diz respeito ao imbróglio envolvendo o Wikileaks e as empresas PayPal, Mastercard e Amazon, que atenderam aos pedidos do governo norte-americano de bloquear as doações monetárias destinadas ao site e de bloquear o acesso a seu servidor no qual o site hospedava seu conteúdo. Os Anonymous não apenas registraram seu apoio ao Wikileaks. Durante algumas horas e, em alguns casos, até mesmo alguns dias, seus hackers, nesta ocasião também organizados por meio do IRC,[6] foram responsáveis por desabilitar os sites dessas corporações, inviabilizando seus serviços – prática que se tornaria muito comum nos protestos protagonizados pelo grupo.

As ações dos Anonymous representam, após um período de latência, um renascimento do hacking e do hacktivismo em escala global e acabam por expor a figura do hacker como um ator político com o qual governos, corporações e agências de inteligência passaram a se preocupar constantemente. As duas perspectivas teóricas apresentadas nas seções seguintes ajudam a ilustrar a questão.

A SUPREMACIA DO SOFTWARE

A primeira delas provém dos chamados estudos de software, capitaneados, em grande medida, também pelo teórico de mídia russo radicado nos Estados Unidos Lev Manovich (2008).[7] Em seu livro *Software takes command*, ele argumenta que, da mesma maneira que a eletricidade e a máquina a vapor permitiram a existência da sociedade industrial, nos tempos atuais, o software é a ferramenta que torna possível uma "sociedade da informação global". Para o autor, o software opera como a força motriz das sociedades contemporâneas, organizando sua vida social, de maneira que todo seu sistema econômico e cultural opera tendo como base esses onipresentes programas de computador. Manovich observa ainda que a produção, distribuição e recepção da maior parte dos conteúdos

[6] IRC, ou Internet Relay Chat, é um protocolo simples de comunicação on-line. Ele pode ser usado para troca de mensagens pessoais ou de arquivos, de maneira privada ou coletiva. Os Anonymous optaram por usar tal ferramenta porque se tornou difícil coordenar grandes e complexas ações por meio de um fórum de imagens.

[7] Também em 2008 foi publicada outra obra seminal dos estudos de software pelo teórico de mídia Matthew Fuller (Cf. Fuller, 2008).

gerados pelos seres humanos são mediados por softwares – o que nos permitiria dizer que, mesmo já ao final do século XX, eles representaram uma nova dimensão que foi incorporada à nossa cultura.

O software, portanto, não deve ser visto como apenas mais um elemento que foi adicionado ao cotidiano, mas sim como uma camada que permeia todas as áreas das sociedades contemporâneas. Por conta disso, é preciso tentar compreender como os softwares estão modelando nossas culturas, e também como estas estão sendo moldadas por eles.[8]

Embora Manovich não leve em conta, em seu trabalho, uma definição conceitual básica entre softwares livres e proprietários, desconsiderando quão relevante é esta diferença para a produção, disseminação e uso dos softwares em si e suas demais aplicações, seu estudo nos traz contribuições deveras relevantes, sobretudo por chamar a atenção, sob diversos aspectos, o protagonismo dos programas de computador na sociedade contemporânea.

De fato, praticamente todos os tipos de comunicação que realizamos, excetuando-se as interações face a face, dependem de softwares – seja na produção, na transmissão ou na recepção de conteúdos. Trata-se, portanto, de uma ferramenta indispensável tanto para criar como para acessar informações, de modo que o exercício de pensar nosso mundo sem os programas de computador parece cada vez mais descabido.

Os softwares, por sua vez, são compostos por linhas de códigos (instruções) programadas para que, quando executadas, assumam determinadas funções e características. A depender da foma como sua arquitetura interna foi projetada, softwares podem tanto auxiliar como prejudicar, ou até mesmo limitar nossa comunicação. Esses emaranhados de códigos são precisamente o hábitat natural dos hackers.

Mais do que isso, os hackers dominam por completo a principal mídia com a qual temos contato na atualidade. Mas, de maneira mais ampla, pode-se afirmar que os hackers têm a grande capacidade de intervir de maneira penetrante, em razão de suas habilidades específicas, no campo comunicacional – o cenário onde o poder é decidido, se assumirmos a perspectiva proposta por Castells (2007).

[8] Manovich chega a propor o termo “software cultural”, no sentido de que ele é a principal ferramenta que nos permite criar e acessar bens culturais.

São passíveis de análise os inúmeros reflexos destas pressuposições no campo político, econômico e social, de modo que muitos deles já são patentes aos nossos olhos. Por exemplo, são dignos de nota os agrupamentos de hackers que, tal como as comunidades de software livre, produzem programas de computador com uma finalidade política e ativista bastante específica – o que a pesquisadora Alexandra Samuel (2004) classificou como *political coding*. É o caso de projetos como o *Hacktivismo*, que se dedica a programar softwares que driblam a censura na Internet imposta por alguns governos (como o "grande firewall" da China); do DeCSS, um software capaz de quebrar criptografias que protegem bens culturais de "violações de direitos de propriedade intelectual"; e também do Tor, programa que permite aos usuários navegarem anonimamente na Internet, não permitindo que seus rastros sejam seguidos.

Por essas e outras, uma sociedade altamente permeada pelos softwares em muitos de seus aspectos, o hacking ganha nova expressão política.

HACKING COMO RESISTÊNCIA AO CONTROLE PROTOCOLÓGICO

Outra interpretação deveras pertinente sobre o ativismo hacker vem do teórico americano Alexander Galloway (2004). Na esteira de Michel Foucault e, principalmente, de Deleuze, o autor argumenta que nossas sociedades estão imersas em um novo aparato de controle – ou melhor, em um novo diagrama de poder, para seguir Foucault. O diagrama em questão são as redes distribuídas e a tecnologia que o permeia é o computador. Além disso, o tipo de administração que rege esse cenário, controlando-o à exaustão, é o protocolo. Trata-se uma atualização da tão propalada "sociedade de controle" deleuziana.

E, se o sistema de administração de informações computadorizadas mais vasto que se tem notícia atualmente é a Internet, é justamente no cerne da computação em rede que está o conceito de "protocolo" – conjunto de recomendações e regras que determinam padrões técnicos e, com isso, governam o modo como "tecnologias específicas são acordadas, adotadas, implementadas e usadas pelas pessoas no mundo" (2004:7).

De maneira geral, o sistema de gestão dominado por protocolos permite que exista um alto grau de controle em um ambiente relativamente heterogêneo. Como Galloway adota a periodização da história feita por Deleuze (1992) com base na obra de Foucault, o

autor afirma que o diagrama do protocolo chega em uma fase da história seguinte à descentralização – ou seja, é posterior à passagem da administração social suprema do soberano (sociedades de soberania) às formas de controle mais burocráticas e distribuídas (sociedades disciplinares).

Galloway detalha a arquitetura de códigos sobre a qual a Internet opera para nos mostrar o modo como seus protocolos são hierarquizados e passíveis de serem controlados. E nos diz, novamente recorrendo a Deleuze, que, nesse novo diagrama, a resistência, necessariamente, passa pelo engajamento com formas distribuídas de administração protocológica. Afinal, o protocolo diz respeito a um tipo perverso de administração: está por toda parte, é universalizante. Renegá-lo é como ir contra a gravidade: os opositores terão pouco ou nenhum retorno. O exemplo mais comum desse controle está no conjunto básico de protocolos TCP/IP. Qualquer pessoa que queira se conectar à Internet precisa aceitá-lo, invariavelmente. E, justamente por isso, a resistência não deve ocorrer fora dele.

Galloway assume que, nesse cenário, os hackers passam a assumir um papel político fundamental. Primeiramente, porque os protocolos lhes são mais do que familiares, uma vez que eles programam códigos melhor do que ninguém. Mas, mais do que isso, os hackers não ignoram ou desejam a morte do protocolo, mas são os arautos das principais possibilidades dele. É por isso que as principais ações políticas diretas empreendidas por hacktivistas valem-se dos próprios protocolos para resistir a, ludibriar e hipertrofiar o controle.

Nesse sentido...

> … enquanto a resistência, durante a Idade Moderna, formou-se em torno de rígidas hierarquias e estruturas burocráticas de poder, a resistência durante a era pós-moderna forma-se em torno de forças de controle protocológico existente nas redes. O hacking significa que a resistência mudou […] Faz sentido que quaisquer forças que desejem resistir ao poder distribuído devam ser adeptas de estratégias distribuídas (Galloway, 2004:160).

Com isso, a resistência, em uma era permeada por redes distribuídas controladas por protocolos, tem os hacktivistas como atores políticos imprescindíveis. Para Galloway, os hackers mostram que, com o protocolo, vem à tona a excitante habilidade de alavancar as possibilidade de ação por meio dos códigos

CONSIDERAÇÕES FINAIS

O hacktivismo pode figurar atualmente como uma das possíveis expressões de um novo ativismo político, sobretudo após seu "renascimento", ao final dos anos 2000, capitaneado pelas ações da rede Anonymous. Essa premissa, no entanto, só podem ser considerada caso assimilemos a expansão de um ecossistema comunicacional horizontal, interativo, multidirecional e distribuído, pelo qual passa a maior parte de nossas informações sociais, culturais, econômicas, pessoais etc. É nesse ambiente que o hacktivismo ganha destaque e no qual merece ser pesquisado.

Neste trabalho, lançamos mão de duas perspectivas sobre as sociedades contemporâneas – revelando o protagonismo dos softwares na organização das relações sociais, econômicas e culturais dos seres humanos, e chamando a atenção para o protocolo de controle como um tipo de administração social.

Assumindo o campo comunicacional como o cenário no qual as lutas pelo poder são travadas (Castells, 2007), tanto os softwares como os protocolos de controle são intermediários imprescindíveis para adentrar esse campo. Dominar essas tecnologias, portanto, é algo estratégico. Mas, mais do que isso, como observou Galloway (2004), para fazer frente a um controle protocológico, distribuído e horizontal, é necessário agir *por meio* dos protocolos, de forma igualmente distribuída. Nesse sentido, os hackers chamam a atenção para seu potencial político ainda pouco explorado.

6. REFERÊNCIAS

ARQUILLA, John; RONFELDT, David. (Org.). **In Athena's camp**: preparing for conflict in the information age. Washington: RAND, 1997.

CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a Internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar, 2003.

_____. Communication, power and counter-power in the network society. **International Journal of Communication**, n.1, 2007. pp. 238-266.

COLEMAN, Gabriella. Anonymous: from the lulz to collective action. **The new everyday**: a media commons project. 2011. Disponível em:

<http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action>. Acesso em: 7 dez. 2011.

DELEUZE, Gilles. Post-scriptum sobre as sociedades de controle. In: _____. **Conversações**. São Paulo: Ed. 34, 1992. p. 223-230.

DENNING, Dorothy. Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing foreign policy. In: ARQUILLA, John; RONFELDT, David. **Networks and netwars**. Santa Monica, CA: Rand, 2001.

FULLER, Matthew. **Software Studies**: a lexicon. Cambridge: The MIT Press, 2008.

GALLOWAY, Alexander. **Protocol**: how control exists after decentralization. Cambridge, Massachusetts: MIT Press, 2004.

HIMANEN, Pekka. **A ética dos hackers e o espírito da era da informação**. Rio de Janeiro: Campus, 2001.

LEVY, Steven. **Hackers**: heroes of computer the revolution. Nova York: Dell Publishing, 1994.

MANOVICH, Lev. **Software takes command**. Nov. 2008. Disponível em: <http://lab.softwarestudies.com/2008/11/softbook.html>. Acesso em: 7 dez. 2011.

RAYMOND, Eric. Como se tornar um hacker. Disponível em: <http://www.linux.ime.usp.br/~rcaetano/docs/hacker-howto-pt.html>. Acesso em: 7 dez. 2011.

SAMUEL, Alexandra Whitney. **Hacktivism and the future of political participation**. Cambridge, Massachusetts: Harvard University, 2004. Disponível em: <http://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf>. Acesso em: 7 dez. 2011.

STALLMAN, Richard. Ataque, não: protesto! **O Estado de S.Paulo**, blog do caderno Link, 3 jul. 2011. Disponível em: <http://blogs.estadao.com.br/link/ataque-nao-protesto/>. Acesso em 7 dez. 2011.

VEGH, Sandor. **Hacking for democracy**: a study of the internet as a political force and its representation in the mainstream media. American Studies, University of Maryland, College Park, 2003.