A informação quer ser livre: uma análise sobre o ativismo dos artífices da rede e o controle na sociedade contemporânea

Bárbara Maria Farias Mota
Graduanda de Ciências Sociais da UFPE

Palavras-chave:
Ativismo hacker; Redes informacionais; Controle; Anonimato.

Keywords:
Hacktivism; Information networks; Control; Anonymity.

RESUMO: O objetivo deste artigo é analisar o ativismo político dos hackers e a relação entre esses indivíduos e o controle/vigilância presente nas redes digitais. Por meio de uma análise bibliográfica sobre a cultura hacker, o trabalho discorre sobre as atividades dos artesãos do código, tais como o desenvolvimento de softwares livres. Por fim, examina como os hackers ativistas, fazendo uso do anonimato, representam atores políticos estratégicos no contexto do capitalismo cognitivo, uma vez que os bens informacionais têm sido cada vez mais fundamentais para reprodução do capital.

ABSTRACT: This paper objective is to analyse the political activism of hackers as well as the relation of these individuals and the control/surveillance present in digital networks. By the means of a bibliographical analysis about the hacker culture, this paper dwells on the activities of these code's craftsmen, such as the development of free software. Finally, this paper examines how hacktivists, leveraging on anonymity, represent strategic political actors in the context of cognitive capitalism, given that informational goods are now even more fundamental to capital's reproduction.

> *A guerra é travada pelos grupos dominantes contra os seus próprios súditos, e o seu objetivo não é conquistar territórios, nem impedir que os outros o façam, mas manter intacta a estrutura da sociedade. [...] A guerra deixou de existir ao se tornar contínua.*
>
> *(George Orwell)*

> *É preciso lembrar que quando o produto é grátis, você é o produto.*
>
> *(Julian Assange)*

Introdução

As redes de comunicação fundamentadas na internet facilitam a articulação de novas formas de expressão que ultrapassam as fronteiras geopolíticas. Os espaços digitais fomentam a mobilização política, que muitas vezes pode ser empreendida sem a necessidade de identificação civil ou da intermediação de instituições formais. Por outro lado, a intensificação da digitalização das nossas informações (sociais, culturais, financeiras e pessoais) potencializa as possibilidades de interceptação destas por Estados e por empresas (MACHADO, 2013; SILVEIRA, 2012). Desse modo, ocorre não só a democratização das estratégias de ação política como também do controle/vigilância. Por isso, as redes informacionais são simultaneamente: redes de comunicação e de controle (SILVEIRA, 2012).

Qual a relação entre ativismo hacker e controle nas redes informacionais? Este artigo recorre a uma análise bibliográfica sobre a cultura hacker para analisar o ativismo político dos artífices da rede na sociedade contemporânea, onde aqueles que dominam a arte

da manipulação dos códigos informacionais detêm uma posição estratégica para influência política, já que essas instruções exercem a mesma função das leis determinando as ações em rede (LESSIG, 1999).

O artigo está divido do seguinte modo: a próxima seção apresenta as controvérsias presentes no termo hacker. A segunda seção concede especial atenção às atividades desses indivíduos no desenvolvimento de softwares aberto/livre, auxiliando na compreensão das motivações presentes no que pode ser compreendido por ofício hacker. A terceira parte discute a ampliação do controle/vigilância nas redes informacionais. A quarta seção contextualiza as atividades desses indivíduos frente ao controle presente nas redes digitais. Por fim, são trazidas as considerações finais do trabalho.

Hacker é diferente de cracker

De acordo com Silveira (2010) hacker em sua definição original era: "um programador de computador talentoso que poderia resolver qualquer problema, muito rapidamente, de modo inovador e utilizando meios não convencionais" (SILVEIRA, 2010). Essa visão também se encontra presente no glossário de expressões hackers, The Jargon File, que define estes indivíduos como pessoas que gostam de explorar os sistemas programáveis e de expandir as suas capacidades, indo além do instrumental necessário para utilização das ferramentas computacionais. O autor (idem, 2010) acrescenta que esse termo passa a ser fonte de disputas na medida em que as redes informacionais ganham importância econômica e social, disseminando uma visão negativa acerca desses indivíduos. Isso porque as práticas dos hackers pela defesa da liberdade de informações e o compartilhamento de códigos computacionais vão de encontro à lucratividade das corporações privadas, como as indústrias de copyright[1]. Uma ilustração do poder dessas indústrias foi o fechamento em 2012, do Megauploud, um dos maiores sites de compartilhamento de arquivos do mundo, sob a alegação da violação de direitos autorais. Outro exemplo ocorreu em 2014, quando a polícia Sueca confiscou servidores e demais equipamentos do The Pirate Bay, o maior site de compartilhamento de arquivos via torrent.

Para Raymond (1998), ícone do movimento Open Source, há práticas que claramente diferenciam os hackers dos crackers. Estes últimos destroem as coisas que os primeiros constroem. Ou seja, a atitude de um hacker, sobretudo no que se refere ao desenvolvimento de softwares de código aberto, consiste na resolução de problemas computacionais complexos e no compartilhamento da inteligência coletiva. Por sua economia ser baseada na reputação, o "título" de hacker não é autoconferido por esta pessoa. Nas palavras dele sobre hackers x crackers:

> *"Existe uma comunidade, uma cultura compartilhada, de programadores experts e gurus de rede cuja história remonta há décadas atrás, desde os primeiros minicomputadores de tempo compartilhado e os primeiros experimentos na ARPAnet. Os membros dessa cultura deram origem ao termo "hacker". Hackers construíram a Internet. Hackers fizeram do sistema operacional Unix o que ele é hoje. Hackers mantém a Usenet. Hackers fazem a World Wide Web funcionar. Se você é parte desta cultura, se você contribuiu a ela e outras pessoas o chamam de hacker, você é um hacker." (RAYMOND, 1998).*

Já para Castells (2007), os crackers vulnerabilizam os códigos computacionais, mas também são hackers, pois fazem parte de uma subcultura da cultura hacker. Além disso, ele critica a definição de Raymond (1998) sobre esses indivíduos por considerá-la generalista. De fato, os valores dessa cultura são devidamente compreendidos quando analisados sob a perspectiva dos desenvolvedores de software de código aberto (que reflete a característica da própria constituição da Internet). Mas segundo o autor (idem, 2007), há a necessidade de uma maior precisão conceitual que identifique: "os autores da transição entre um meio de inovação acadêmica e institucionalmente constituída e o surgimento de

1 Empresas detentoras do *copyright* de bens simbólicos, tais como filmes, músicas, programas etc.

redes auto-organizadas (ibidem, 2007, p.61)". Desse modo, ele recorre ao famoso estudo de Levy (2010) sobre o tema e compreende por cultura hacker o conjunto de valores e crenças que emergiram na interação online a partir da colaboração nos projetos autodefendidos de programação criativa. Nessa perspectiva, a Internet é originalmente resultante da cultura tecnomeritocrática (científica), mas o seu aperfeiçoamento vem dos inputs (contribuições) trazidos pela cultura hacker que interage na rede.

Desse modo, o hacker pode ser compreendido como o indivíduo que utiliza os seus conhecimentos técnicos para fins políticos ou motivações éticas. Já o cracker os utiliza para causar prejuízos (roubo de senhas de cartão de crédito, uso de botnets para lucro pecuniário, desenvolvimento de vírus computacional etc.) e é enquadrado como cibercriminoso. Essa distinção foi feita justamente por hackers, na década de 1980, em contraposição a representação popularizada pelos mass media, do hacker como sinônimo de criminoso.

Hackeando a jaula de ferro

No livro A ética dos hackers e o espírito da era da informação, uma alusão à obra do sociólogo Max Weber, Himanen (2001) evidencia que os hackers combinam o seu trabalho de modo menos rígido com as outras esferas da vida, já que este também é percebido como fonte de diversão para eles. Essa lógica de flexibilização do trabalho é cada vez mais presente na sociedade contemporânea e em diferentes tipos de atividades. Mas o principal fator motivacional, ou o "espírito" do trabalho hacker, não se trata apenas do dinheiro, mas sim, da criação de algo significativo para a comunidade com a qual ele compartilha suas ideias. Os hackers se guiam pela paixão gerada naquilo que fazem e têm uma ética ou "nética": o compartilhamento de informações é um imperativo moral. Por isso, eles distribuem os resultados de sua criatividade livremente, permitindo que outras pessoas possam – usá-los, testá-los e modificá-los – alimentando o ciclo da cultura livre (idem, 2001).

Similarmente, Torvalds[2] (2001) evidencia três fatores que impulsionam um hacker: sobrevivência, vida social e diversão. Para ele, o dinheiro compra a sobrevivência, mas dificilmente compra os laços sociais e a diversão. Por isso, o efeito social ocasionado por trabalhar coletivamente foi o que motivou os hackers do sistema operacional Linux a compartilharem suas ideias e a cooperarem voluntariamente. Contaria mais para o trabalho colaborativo o fato de a programação ser uma atividade interessante e desafiadora para os seus praticantes. Essa visão é corroborada por Sennett (2012) quando ele associa o próprio Linux a um tipo de artesanato público que é construído em oficinas online pelos artífices do código. Estes artífices, por sua vez, são definidos como pessoas dedicadas à arte pela arte, isto é, àquelas que se engajam na execução de um bom trabalho como fim em si mesmo; esses artesãos remodelam o código constantemente e este não é um objeto acabado e nem fixo:

> *"O kernel (núcleo de software) do código Linux está disponível a todos, pode ser utilizado e adaptado por qualquer um; as pessoas oferecem voluntariamente e doam seu tempo para aperfeiçoá-lo. O Linux contrasta com o código utilizado na Microsoft, cujos segredos até recentemente eram entesourados como propriedade intelectual de uma só empresa. Numa das aplicações mais utilizadas do Linux, a Wikipedia, o kernel permite o funcionamento de uma enciclopédia para a qual qualquer usuário pode construir."* (SENNETT, 2012, p. 34-35).

Essa perspectiva deságua naquilo que Raymond (1998), em referência ao desenvolvimento de softwares, define como modelo bazar em oposição ao modelo catedral. Neste último, um grupo fechado de programadores primeiramente elabora o código para depois liberá-lo aos interessados; no primeiro, por sua vez, os usuários são tratados como potenciais desenvolvedores e os códigos são construídos e compartilhados coletivamente, pois: "dados bastantes olhos, todos os erros

2 Linus Torvalds é um *hacker* e projetou o sistema de controle de versão, *Git*, para o desenvolvimento do *kernel* Linux.

são triviais'' (idem, 1998, online). Ou seja, a expressiva instantaneidade entre a detecção de bugs (defeitos) e as suas correções, por meio da cooperação direta em rede, fortalece a inovação e a criatividade no modelo aberto de desenvolvimento de softwares.

Mas para Stallman[3], fundador da Free Software Foundation[4], os benefícios técnicos preconizados no modelo Open Source são importantes, porém insuficientes para assegurar a liberdade no ciberespaço. Isso porque um programa pode até ter o seu código fonte aberto, mas isto por si só não o caracteriza como software livre, pois há quatro liberdades básicas que definem este: 0) rodar o programa como quiser para o propósito que desejar; 1) estudar o código fonte do programa e modificá-lo para os seus interesses; 2) fazer, redistribuir ou vender cópias exatas do programa para outras pessoas e 3) modificar o programa e distribuir essas modificações para o benefício da comunidade. Segundo ele, a liberdade plena em rede vem da utilização do código fonte para os propósitos individuais (as duas primeiras liberdades); e para os propósitos coletivos (as duas últimas liberdades). Além disso, ele enfatiza: "software livre é uma questão de liberdade, não de preço. Para entender o conceito, você deve pensar em liberdade de expressão e não em 'cerveja grátis' (STALLMAN[5], online)". Isso porque o software livre pode ser comercializado ao passo que o software proprietário pode ser distribuído gratuitamente. Consiste, essencialmente, na ideia de que o controle do programa deve ser exercido pelas pessoas (e não o contrário), permitindo a elas não ficarem reféns dos interesses de empresas de software proprietário, conferindo-lhes autonomia. Essas empresas, por razões comerciais ou interesses escusos, podem restringir as funcionalidades do programa, instalar aplicativos maliciosos e rastrear/espionar os usuários sem que estes tomem conhecimento disto.

Nesse sentido, Silveira (2010) percebe uma grande influência liberal no pensamento hacker, evidenciada na defesa de direitos humanos básicos como a liberdade de expressão, o que também justifica a forte oposição desses indivíduos ao bloqueio do compartilhamento de códigos. Isso condiz com o que o autor (idem, 2010) nomeia de individualismo colaborativo, ou seja, a busca pela autonomia individual por meio do acesso irrestrito às informações compartilhadas coletivamente. Ao se referir as comunidades de FLOSS[6] ele evidencia:

> *"Hackers do Floss têm um comportamento extremamente meritocrático. Ao mesmo tempo, seu hiperindividualismo é construído em processos colaborativos. Os desafios encontrados nos códigos e na aplicação dos protocolos devem ser enfrentados, e os resultados de sua superação devem ser informados a todos. O conhecimento deve ser livre para que outros possam contribuir enquanto ganham mais autonomia no processo de aquisição do conhecimento para si."* (SILVEIRA, 2010).

Esse processo resulta na projeção do que Sennett (2006) denomina por cidadão-como-artesão. Ao contrário do cidadão-como-consumidor, o cidadão-como-artesão necessita de esforço para descobrir o funcionamento do mundo ao seu redor. Isso porque os bens simbólicos - numa sociedade em que as tecnologias digitais exercem o protagonismo na intermediação da comunicação - são, metaforicamente, "barris de petróleo virtual". Como aponta Manovich (2008), assim como a eletricidade e o motor a combustão permitiram a existência da sociedade industrial, o software propiciou a existência da sociedade de informação global. E por isso exerce o comando das ações na medida em que nos comunicamos por dispositivos mediados por softwares. A comunicação na Internet é totalmente dependente de protocolos e de códigos computacionais. Por conseguinte, softwares com o código fechado não permitem a compreensão dos mecanismos de controle e de gerenciamento das ações em rede. Desse modo, um sistema operacional moldado para facilitar a vida dos usuários compromete até mesmo a democracia. Pois tal sistema, por agregar conveniência e praticidade, tem como custo a

3 "*Introduction to Free Software and the Liberation of Cyberspace*", TEDx, 2014. Disponível em: <www.fsf.org/blogs/rms/20140407-geneva-tedx-talk-free-software-free-society>. Acessado em 10/12/2014.

4 Para mais informações: http://www.fsf.org/.

5 "Richard Stallman: software proprietário é colonização digital", II Fórum Mundial de Educação Profissional e Tecnológica, 2012. Disponível em: <w3.ufsm.br/lince/index.php/noticias/184-richard-stallman-software-proprietario-e-colonizacao-digital>. Acessado em: 10/12/2014.

6 Abreviação de *Free/Libre/Open Source Software* (Software livre e de código aberto).

liberdade dos usuários sobre as suas próprias informações e ações.

Por acreditarem que nem tudo o que é mais prático é melhor, os hackers agem como artífices e buscam como evidencia Machado (2013) dominar a arte de manipulação dos códigos nas redes digitais de comunicação. Em decorrência disso, esses atores são privilegiados no contexto da sociedade informacional.

O controle na sociedade informacional

Lyotard (1986) evidencia os impactos das transformações tecnológicas no saber científico, discutindo como as máquinas informacionais afetaram a produção, o armazenamento

Maressa de Souza

e a transmissão do conhecimento, que passa a ser medido pela possibilidade da sua conversão em linguagem computacional e da sua tradutibilidade em quantidades (bits) de informações. Uma vez que na sociedade contemporânea a fonte da produtividade se encontra nas tecnologias de processamento das informações, as técnicas mais valiosas, portanto, são aquelas utilizadas para a manipulação de dados e voltadas à produção e ao gerenciamento dos conhecimentos (CASTELLS, 2001; SILVEIRA, 2012). Isso condiz com o que Cocco (2012) define por capitalismo cognitivo ou imaterial, no qual o conhecimento é utilizado para produção de outros conhecimentos e o suporte material, por vezes, é apenas a base para algo intangível. Exemplificando, ele cita a empresa norte-americana Nike: "o custo de produção de seus sapatos esportivos é estimado em não mais de 4% do preço de venda total; o resto é remuneração dos ativos imateriais (marca, pesquisa, patentes e o know how da empresa) (idem, 2012, p. 12)".

Em decorrência disso, no chamado capitalismo cognitivo, os bens intangíveis são fundamentais para reprodução do capital, pois seguem a lógica de inovação de que este necessita. Os bens materiais, por um lado, são escassos e destinados a se tornarem obsoletos, os bens imateriais, por outro lado, são abundantes e não se esgotam com seu uso, pois ao contrário, podem ser multiplicados e aprimorados quando da sua apropriação. Nas palavras de Flusser (1983): "é o aspecto mole, impalpável e simbólico o verdadeiro portador de valor no mundo pós-industrial dos aparelhos. Transvalorização de valores; não é o objeto, mas o símbolo que vale (FLUSSER, 1985, p. 17)".

Nessa perspectiva, as redes de comunicação fundamentadas na Internet se tornam um espaço privilegiado para intervenção de órgãos de governos e de corporações privadas que ampliam, com finalidades diversas, as possibilidades de captação da inteligência coletiva presente na rede.

Baseado nisso, Silveira (2012) compreende o controle como a capacidade que algo ou alguém possui de exercer fiscalização, monitoramento, regulação ou domínio da ação de objetos ou seres vivos. Ele caracteriza os quatro principais tipos de controle exercido na sociedade informacional, seguidos de suas finalidades, a saber: protocolos, que gerenciam a comunicação na rede; formatos, que respondem pela memória e pelo modo de armazenamento dos dados digitais; linguagens de programação, que definem as formas como vemos e organizamos os nossos desejos na rede; rastros de navegação, que são a base das atividades que fazemos no ciberespaço; e acesso, responsável pela permissão ou bloqueio das plataformas informacionais (idem, 2012).

Assim, o aumento da comunicação nas redes digitais vem acompanhado do maior potencial de controle eletrônico em massa. Por isso, independente dos propósitos, esse controle só pode ser exercido através da comunicação e de feedbacks que retroalimentem constantemente as informações do controlado para o controlador. Por esse controle ser distribuído assimetricamente, qualquer um que tenha habilidades, pode tentar observar, rastrear e influenciar o comportamento de outras pessoas no ciberespaço (ibidem, 2012). No entanto, um analista de dados do Google[7], por exemplo, tem maiores possibilidades de segmentação de anúncios online, quando comparado ao editor de um pequeno blog, que utiliza o Google Adwords para ampliação das receitas de seu site.

Portanto, os rastros deixados pelos usuários nas plataformas digitais são extremamente valiosos. Por meio desses vestígios, empresas criam perfis para análise preditiva e se voltam ao oferecimento de produtos e serviços antes mesmo dos potenciais consumidores saberem se irão querer ou precisar deles. Além disso, essas informações também influenciam no modo como a própria rede é experienciada. No Facebook temos um exemplo disso, o usuário dessa plataforma é justamente o produto que se automodela para publicização na sua vitrine virtual ao passo que fornece métricas das suas ações (curtidas, compartilhamentos, visualizações de páginas e cliques em propagandas) ou nas

7 "Site de maior audiência mundial de acordo com o Alexa Internet Inc., serviço que mede a quantidade de usuários que visitaram um site. Para mais informações: http://www.alexa.com/.

palavras de Silveira (2012):

> *"Inúmeras corporações capitalistas se especializaram em saber como nos comportamos, o que nos agrada ou repele, o que nos alegra e nos entristece. [...] A extração das oscilações de humor, e dos afetos, traz novas possibilidades de rendimentos e torna-se uma das principais atividades das novas formas de reprodução do capital. Se o Estado Chinês pode filtrar o tráfego de dados da Internet e identificar dissidentes de seu regime a partir do escaneamento de e-mails, as empresas de seguros podem utilizar os rastros digitais dos cidadãos para formar um banco de dados que informe as doenças preexistentes de seus clientes. Com tais informações, os convênios podem maximizar seus ganhos e reduzir possíveis perdas indesejadas com tratamentos dispendiosos."* (SILVEIRA, 2012, p.115).

Assange et al. (2012), um dos precursores do Movimento Cypherpunk[8], igualmente evidencia: desde a década de 1990 ocorre o aumento das possibilidades de comunicação em consonância com o aumento da vigilância global. Essa última era mais explícita na época, por ser realizada grosso modo, pelos Estados norte-americano, britânico e russo. No entanto, na medida em que se há uma maior pluralidade no controle das ideias - já que as redes de comunicação ampliaram para mais pessoas os espaços de produção dos conteúdos - há, por outro lado também, a pluralidade da vigilância, que se mostra mais difusa e não tão evidente quando comparada aquele período. Nas palavras do fundador do WikiLeaks:

> *"Quando nos comunicamos por internet ou telefonia celular, [...] nossas comunicações são interceptadas por organizações militares de inteligência. É como ter um tanque de guerra dentro do quarto. [...] Nesse sentido, a internet, que deveria ser um espaço civil, se transformou em um espaço militarizado. Mas ela é um espaço nosso, porque todos nós a utilizamos para nos comunicar uns com os outros, com nossa família, com o núcleo mais íntimo de nossa vida privada. Então, na prática, nossa vida privada entrou em uma zona militarizada. É como ter um soldado embaixo da cama."* (ASSANGE et al, 2012, p.53)

Esse alerta teve uma maior ressonância em 2013, quando Edward Snowden, ex-técnico da Agência de Segurança Nacional (NSA), revelou alguns dos programas de vigilância dos Estados Unidos, que se utilizavam de servidores de empresas como o Google e o Facebook. Os argumentos, em geral, para legitimar a violação da privacidade dos internautas se baseiam na evocação de expressões semânticas de autoridade, tais como a declaração do presidente Barack Obama nessa época: Você não pode ter 100% de segurança, e então 100% de privacidade e zero de inconveniência. Ou no combate, de acordo com Assange et al (2012), dos quatro cavaleiros do apocalipse da informação: pornografia infantil, terrorismo, lavagem de dinheiro e guerra contra as drogas. Desse modo, com a finalidade de garantir a segurança tenta-se legitimar a ampliação dos mecanismos de vigilância, transformando todos os indivíduos em criminosos potenciais.

Como os hackers agem diante do controle?

Frente ao controle distribuído assimetricamente, as estratégias de ação política na Internet também se dispersam, de modo que quanto mais se tente combatê-las mais possam se dissipar no espaço digital.

Nessa perspectiva, o ativismo hacker também denominado hacktivismo desponta como modo de resistência política, pois hackers conseguem embaralhar dados e apagar os seus rastros, gerando prejuízos ao exercício do controle nas redes informacionais (SILVEIRA, 2009). Baseado nisso, Machado (2013) afirma que não se trata de desenvolver táticas por fora da esfera dos protocolos (que determinam padrões técnicos necessários para comunicação em rede), mas de uma forma de engajamento projetada no interior dessa própria esfera, permitindo aos hacktivistas resis-

8 Movimento que preconiza pelo uso da criptografia (originária do grego "escrita secreta") como forma de ativismo político. Um dos lemas dos *Cypherpunks* é a máxima: transparência para os poderosos e privacidade para os fracos (ASSANGE et al, 2012).

tirem, ludibriarem e hipertrofiarem o controle.

Para Samuel (2004) o hacktivismo é a junção entre o ativismo político e o hacking de computador, através do uso não violento e legalmente ambíguo de ferramentas digitais com finalidades políticas. Esse tipo de ativismo se constitui, portanto, em ações de desobediência civil por meio do uso transgressivo de ferramentas digitais, a exemplo de: desfiguração de sites; redirecionamento de páginas; negação de serviço; roubo de informações sigilosas; paródia de sites; manifestações virtuais; sabotagens virtuais e desenvolvimento de softwares. Desse modo, esse tipo de prática se diferencia das ações ciberativistas comuns (petições online; votações online etc), que se encontram nos limites convencionalmente aceitos da atuação política, e das atividades ciberterroristas, que fazem o uso da violência para atingir seus objetivos (idem, 2004).

O hacktivismo tem relação com o controle exercido na sociedade informacional, pois vai de encontro à apropriação da inteligência coletiva na rede já que os hackers se utilizam do anonimato para preservação das suas identidades civis. Por anonimato, Silveira (2009) compreende a condição da comunicação não-identificada sendo exercida por interagentes que não possuem uma identidade explícita ou que a ocultam no espaço virtual (através do uso de ferramentas digitais, por exemplo). Por isso, a capacidade de defesa do não-rastreamento nas redes informacionais, está cada vez mais associada ao próprio controle dos dados pessoais. Isso, por conseguinte, se relaciona a anonimização na rede, já que o controle é avesso ao anônimo, incerto ou nômade (idem, 2009). Desse modo, a Internet, simultaneamente, é a expressão do controle informacional e a portadora das tecnologias do anonimato (SILVEIRA, 2012).

Para Wong e Brown (2013) atores políticos não estatais, como os Anonymous e o Wikileaks, por exemplo, são ativados pela lógica do anonimato na Internet e afetam as formas contemporâneas de se pensar o ativismo transnacional ao se engajarem no que os autores nomeiam de "a política de ninguém". Isto é, as tecnologias informacionais não são apenas um meio para tomada de decisões políticas, pois reconfiguram o próprio modo como a política se expressa:

> *"[...] O potencial de anonimato da Internet permite a emergência de diferentes tipos de protestos sociais. Ao contrário dos protestos físicos como uma demonstração de força, ativistas podem se reunir online, às vezes deliberadamente, às vezes acidentalmente, e expressar suas preferências políticas através do vazamento de informações ou atacando servidores." (WONG e BROWN, 2013, p.1024).*[9]

Assim, através de protestos virtuais, esses atores fazem exigências sem revelar quem são (o quem importa menos que o como). E impõem custos físicos (sem deixar vestígios no espaço físico) quando, por exemplo, documentos sigilosos de autoridades públicas são vazados. Ainda de acordo com os autores, a classificação dos Anonymous e do Wikileaks como grupos terroristas mostra-se inadequada, pois o terrorismo é definido na literatura por ações de violência (física e/ou psicológica) contra civis, implicando em potenciais danos físicos ou na morte destes.

Desse modo, esses atores, em geral, se envolvem em atividades descoordenadas e questionáveis legalmente, mas agem com fins ideológicos e políticos de mudança. Portanto, eles se distinguem de redes criminosas e/ou terroristas, já que a violência física não faz parte das suas táticas de ação e as suas motivações não operam para o lucro pecuniário (WONG e BROWN, 2013).

Considerações finais

Qual a relação entre ativismo hacker e controle nas redes informacionais? Esse trabalho buscou evidenciar como os dispositivos tecnológicos são onipresentes no nosso cotidiano, afetando a comunicação e consequentemente, permitindo a emergência de novos repertórios de ação política na dimensão virtual, que também é impactada pelo espaço

9 Livre tradução de: "[...] The anonymizing potential of the Internet enables different kinds of social protest to emerge. Instead of physical protest as a show of strength, activists can gather online, sometimes advertently, sometimes inadvertently, and express their political preferences through leaking information and attacking servers."

offline (físico). É justamente pela capacidade de anonimização na rede e pela sua natureza descentralizada – com baixa hierarquia para a organização de protestos - que existe "a política de ninguém" cunhada por Wong e Brown (2013).

A análise evidencia que as formas de engajamento estratégicas são aquelas que se utilizam do próprio controle existente nas redes informacionais para reconfigurá-lo, isto é, para extrapolar as regras estabelecidas nos protocolos que governam as nossas ações em rede. Com a ampliação das potencialidades de captação da inteligência coletiva, torna-se cada vez mais difícil (para não dizer improvável) não ser rastreado e ter o nosso tráfego de navegação analisado. Assim, o tipo de ativismo impulsionado pelos hackers se mostra como uma estratégia de contraposição ao controle presente na sociedade informacional, condizendo com os pilares da ética hacker: não importa quem você é, mas o que você faz. Ou de empréstimo da máxima Cypherpunk: privacidade para os fracos, transparência para os poderosos.

Isso porque atacar alvos poderosos transnacionalmente (através da derrubada de sites ou do vazamento de informações sigilosas), só é possível enquanto as identidades reais dos atores engajados nessas ações (legalmente ambíguas) permanecem desconhecidas. Ou seja, a invisibilidade individual fortalece a visibilidade coletiva quando esta é feita sob o manto do anonimato.

Referências Bibliográficas

ASSANGE, Julian et al. (2012), *Cypherpunks: a liberdade e o futuro da internet*. São Paulo: Boitempo.

CASTELLS, Manuel. (2007), *A Galáxia Internet: Reflexões sobre Internet, Negócios e Sociedade*. Lisboa: Fundação Calouste Gulbenkian.

_____. (2001), "O informacionalismo e a sociedade em rede". In: HIMANEM, Pekka. (Org.). *A Ética dos Hackers e o Espírito da Era da Informação*. Rio de Janeiro: Campus.

COCCO, Giusepe. (2012), "Trabalho sem Obra, Obra sem autor: a Constituição do Comum". In: BELISÁRIO, Adriano; TARIN, Bruno (Org.). *Copyfight: Pirataria e Cultura Livre*. Rio de Janeiro: Azougue.

FLUSSER,Vilém. (1985), *Filosofia da caixa preta*. São Paulo: Hucitec.

HIMANEN, Pekka. (2001), *A ética dos hackers e o espírito da era da informação: a importância dos exploradores da era digital*. Rio de Janeiro: Campus.

LYOTARD, Jean-François. (1986), *O Pós-Moderno*. Rio de Janeiro: Jose Olympio.

LESSIG, Lawrence. (1999), "Code and Other Laws of Cyberspace". *New York*: Basic Books.

LEVY, Steven.(2010), *Hackers: Heroes of the Computer Revolution*. 25th Anniversary Edition. Sebastopol: O'Reilly Media.

MACHADO, Murilo Bansi. (2013), *Anonymous Brasil - poder e resistência na sociedade de controle*. Bahia: EDUFBA.

MANOVICH, Lev. (2008), "Software takes command". Disponivel em:<http://lab.softwarestudies.com/2008/11/softbook.html>. Acessado em: 15 jul. 2014.

RAYMOND, Eric. (1998), "A catedral e o bazar". Disponível em: <http://www.dominiopublico.gov.br/download/texto/tl000001.pdf>. Acessado em: 15 jun. 2014.

_____. (1998), "Como se tornar um hacker". Disponível em: < https://linux.ime.usp.br/~rcaetano/docs/hacker-howto-pt.html>. Acessado em: 03 ago. 2014.

SAMUEL, Alexandra Whitney. (2004), *Hacktivism and the future of political particiption*. Tese (Doutorado em Ciência Política) – Departamento de Governo, Universidade Harvard, Cambridge, Massachusetts.

SENNETT, Richard. (2012), O Artífice. Rio de Janeiro: Record.

_____. (2006), A cultura do novo capitalismo. Rio de Janeiro: Record.

SILVEIRA, Sérgio Amadeu. (2009), Redes cibernéticas e tecnologias do anonimato. Comunicação & Sociedade, Ano 30, n. 51, p. 113-134.

_____. (2010), Ciberativismo, cultura hacker e o individualismo colaborativo. Revista USP, v. 1, p. 28-39.

_____. (2012), "Poder e anonimato na sociedade de controle". In: _____; JOSGRILBERG, Fabio B. (Orgs.). *Tensões em rede: os limites e possibilidades da cidadania na Internet*. São Paulo: Metodista.

TORVALDS, Linus. (2001), "O informacionalismo e a sociedade em rede". In: HIMANEM, Pekka. (Org.). *A Ética dos Hackers e o Espírito da Era da Informação*. Rio de Janeiro: Campus.

WONG H. Wend & BROWN Peter A. (2013), "E-Bandits In: Global Activism: WikiLeaks, Anonymous, and the Politics of No One". *Perspectives on Politics*, v. 11, p.1015-1033.

Recebido em: 19 de maio de 2015.
Aprovado em: 7 de dezembro de 2015.