UNIVERSIDADE FEDERAL DO ABC

POR DENTRO DOS ANONYMOUS BRASIL:

PODER E RESISTÊNCIA NA SOCIEDADE DE CONTROLE

MURILO BANSI MACHADO

DISSERTAÇÃO APRESENTADA COMO PARTE DOS REQUISITOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM CIÊNCIAS HUMANAS E SOCIAIS.

ORIENTADOR: PROF. DR. SERGIO AMADEU DA SILVEIRA

SANTO ANDRÉ

2013

CURSO DE PÓS-GRADUAÇÃO EM CIÊNCIAS HUMANAS E SOCIAIS

DISSERTAÇÃO DE MESTRADO

MURILO BANSI MACHADO

POR DENTRO DOS ANONYMOUS BRASIL:

PODER E RESISTÊNCIA NA SOCIEDADE DE CONTROLE

DISSERTAÇÃO APRESENTADA COMO PARTE DOS REQUISITOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM CIÊNCIAS HUMANAS E SOCIAIS.

ORIENTADOR: PROF. DR. SERGIO AMADEU DA SILVEIRA

SANTO ANDRÉ

2013

Universidade Federal do ABC

PÓS-GRADUAÇÃO EM CIÊNCIAS HUMANAS E SOCIAIS

FOLHA DE ASSINATURAS

Assinaturas dos membros da Banca Examinadora que avaliou e aprovou a Defesa de Dissertação de Mestrado do candidato **Murilo Bansi Machado**, realizada em 14 de maio de 2013:

Prof. Dr. Sérgio Amadeu da Silveira - Presidente (UFABC)

Prof. Dr. Claudio Luis de Camargo Penteado – Membro Titular (UFABC)

Prof. Dr. Henrique Zoqui Martins Parra – Membro Titular (UNIFESP)

Profa. Dra. Maria Gabriela Silva Martins da Cunha Marinho – Membro Suplente (UFABC)

Prof. Dr. Demi Getschko – Membro Suplente (PUC)

Este exemplar foi revisado e alterado em relação à versão original, de acordo com as observações levantadas pela banca no dia da defesa, sob responsabilidade única do autor e com a anuência de seu orientador.

Santo André, ____de _____ de 20___.

Assinatura do autor: _____

Assinatura do orientador: _____

A todos aqueles que, tal como eu, dedicam-se à
busca por e à pesquisa de métodos e
ferramentas que aspiram à
transformação social

AGRADECIMENTOS

Espaços como estes sempre se mostram deveras reduzidos quando comparados à quantidade e à intensidade de apoios que uma tarefa como esta demanda. Logo, qualquer tentativa de nomear todos aqueles que, direta ou indiretamente, contribuíram para esta caminhada seria por certo malfadada. Recebam todos, portanto, meu mais humilde e sincero agradecimento. Contudo, não poderia deixar de destacar:

(1) A todas as minhas referências no âmbito acadêmico, incluindo os educadores e professores que passaram por minha vida. Mesmo aqueles alheios às formas tradicionais de ensino foram decisivos em minha formação, tanto ao compartilhar seus saberes como ao servir de fonte inesgotável de inspiração. Deixo especiais agradecimentos aos professores que compuseram minha banca, Cláudio Penteado e Henrique Parra, e sobretudo ao amigo e orientador, Sergio Amadeu da Silveira.

(2) A todos os Anons que, de uma forma ou de outra, me auxiliaram no desenvolvimento deste trabalho. Um agradecimento especial para os *nicks* aletheia, AnonDev, Bile Day, Bruce Wayne e L. Sem vocês, esta pesquisa poderia se tornar uma mera especulação.

(3) A minha família, principal responsável por minhas referências em âmbito pessoal; a meus pais, a quem devo tudo, e a minha irmã, que em breve deverá me proporcionar o prazer de ler um agradecimento como este; aos que ficaram conosco e aos que, nestes últimos dois anos, nos deixaram momentaneamente;

(4) A minha companheira de trabalho e de vida, Daniella Cambaúva, sem a qual esta dissertação (e muitas outras coisas) jamais existiria.

RESUMO

Este trabalho discute o fenômeno do hacktivismo – ou ativismo hacker – como uma forma de resistência política sob o contexto das chamadas sociedades de controle. Para tanto, tem como objeto de estudo o coletivo Anonymous, com foco em suas facetas hacktivista e brasileira. Para responder à questão principal da pesquisa, que diz respeito ao modo como os Anonymous se engajam politicamente, este trabalho realiza, a princípio, um breve histórico do ativismo hacker em escala global para argumentar que, no final dos anos 2000, os Anonymous representaram uma reconfiguração dessa forma de ativismo político, observando, contudo, que o hacking sempre foi uma atividade intrinsecamente política e os hackers são atores políticos cuja relevância se agiganta na sociedade da informação. Em seguida, recorre à pesquisa bibliográfica para, primeiramente, alinhavar as fundações teóricas da sociedade de controle, tal como proposta pelo filósofo francês Gilles Deleuze, e as principais expressões acadêmicas dela decorrentes nos últimos anos, adaptando seu ferramental às sociedades contemporâneas. Em segundo lugar, destaca as principais perspectivas teóricas que já lançaram interpretações sobre o ativismo hacker, aqui divididas em (1) Desobediência civil digital; (2) Guerra da informação / ciberterrorismo; e (3) Hacktivismo por ele mesmo. Na sequência, este trabalho apresenta as origens e as principais ações do coletivo Anonymous, recuperando sua trajetória internacional para, assim, descrever suas principais faces e expressões no contexto brasileiro. Para corroborá-lo, analisa duas operações deflagradas por grupos e indivíduos alinhados aos Anonymous Brasil: as operações WeeksPayment e Globo, realizadas em 2012. Por fim, sugerem-se quatro formas principais por meio das quais os Anonymous se engajam politicamente (promovendo o anonimato; evangelizando; formando redes distribuídas; exibindo e possibilitando várias formas de ações políticas) para, em seguida, ressaltar sua posição de resistência política em meio à sociedade de controle.

Palavras-chave: Anonymous. Hacktivismo. Ciberativismo. Cultura hacker.

ABSTRACT

This dissertation discusses the phenomenon of hacktivism – or hacker activism – as a form of political resistance in the context of so-called control societies. For doing so, it studies the Anonymous collective, focusing on its hacktivist and Brazilian facets. In order to answer the main question of this research, which is related to how Anonymous engage politically, this dissertation shows, at first, a brief history of hacker activism on a global scale to argue that in late 2000, Anonymous represented a reconfiguration of this form of political activism, but highlighting that hacking has always been an inherently political activism and hackers are political actors whose relevance is increasing in the information society. Then it draws on the literature to, at first, baste the theoretical foundations of control society, as it was proposed by French philosopher Gilles Deleuze, and the major academic expressions based on this foundations in recent years, adapting its tools to contemporary societies. Secondly, it highlights the main theoretical perspectives that have studied hacker activism, here divided into (1) Electronic civil disobedience; (2) Information war / cyberterrorism; (3) Hacktivism by himself. Further, this dissertation presents the origins and main actions undertaken by Anonymous collective, mentioning its international course to describe its main faces and expressions in the Brazilian context. To corroborate it, examines two operations triggered by groups and individuals aligned with Anonymous Brazil: operations WeeksPayment and Globo, both conducted in 2012. Finally, it suggests four main ways through which Anonymous engage politically (promoting anonymity; evangelizing; forming distributed networks; displaying and providing various forms of political action) to then emphasize its position of political resistance in the control societies.

Keywords: Anonymous. Hacktivism. Cyberactivism. Hacker culture.

LISTA DE IMAGENS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

cDc	Cult of the Dead Cow
CAE	Critical Art Ensemble
CoS	Church of Cientology
DDoS	Distributed Denial of Service
EDT	Electronic Disturbance Theater
IRC	Internet Relay Chat
LOL	Laugh Out Loud
NSM	New Social Movement (Novo Movimento Social)
WITP	What is the plan (fórum)

SUMÁRIO

1 INTRODUÇÃO: A RECONFIGURAÇÃO DO HACKING POLÍTICO

Em tempos de crescente protagonismo das mais diversas redes digitais e interconectadas, inúmeros pesquisadores de várias áreas do conhecimento já chamaram a atenção para a emergência de uma nova forma pela qual o controle é implementados sobre as nossas sociedades contemporâneas (HARDT, 2000; GALLOWAY, 2004; LESSIG, 2006; SANTOS, 2003; COSTA, 2004; entre outros). Se, por um lado, essa reformulação na forma de se exercer o poder se mostra cada dia mais factível e totalizante, por outro, formas de resistência política a esse controle, em grande medida, começam a ganhar novos formatos e contornos, passando a operar sob um novo estilo de gerenciamento e em novas plataformas tecnológicas. Nesse cenário, certos atores políticos tradicionalmente relegados ao segundo plano passam a ganhar cada vez mais relevância na chamada era informacional (CASTELLS, 2009).

Por isso, este trabalho se propõe a traçar um mapa descritivo dessa nova forma de exercício do poder, aqui identificada com a chamada sociedade de controle, tal como formulada por Deleuze (1992), para tratar justamente de uma das expressões de um novo ativismo político: o ativismo hacker – ou hacktivismo. Este passa a se configurar, conforme apontou Sergio Amadeu da Silveira (2012, p. 110), como uma das inúmeras conformações de resistência ante a "voracidade do capitalismo cognitivo", ao lado, por exemplo, das práticas de compartilhamento de bens imateriais e das diversas manifestações culturais e étnicas disseminadas nas redes distribuídas.

Para tanto, tomou-se como objeto de pesquisa deste trabalho aquela que, em todo o mundo, certamente tem sido a maior expressão do ativismo hacker nos últimos anos: a rede hacktivista autointitulada Anonymous[1] – mais especificamente, os grupos e indivíduos identificados com tal rede no contexto brasileiro. Dessa maneira, o principal objetivo desta pesquisa é verificar como os Anonymous se engajam politicamente (seu modo de organização, seus ideais, a natureza de suas lutas, os atores que se identificam com elas etc.),

1 Como se poderá observar ao longo desta pesquisa, o coletivo Anonymous não é composto apenas por hackers. Ao contrário: entre os colaboradores desta ideia, há pessoas com diversas formações, profissionais de diversas áreas, além de estudantes oriundos dos mais variados cursos. Sem desconsiderar esse aspecto fundamental, este trabalho se foca principalmente na faceta hacktivista (e brasileira) deste coletivo. A opção por essa delimitação do objeto decorre do fato de que, ao menos no contexto brasileiro, as principais e mais expressivas operações deflagradas pelos Anonymous contaram com a fundamental participação de hackers ativistas, de modo que o pessoal não técnico, em grande parte dos casos, engajaram-se em ações em conjunto hacktivistas, ou então após a iniciativa destes.

tendo em vista a perspectiva segundo a qual o hacktivismo se configura como uma forma de resistência política no contexto das sociedades de controle.

Faz-se importante notar, antes prosseguir com os procedimentos formais desta pesquisa, que aqui nos debruçamos sobre um fenômeno que se mostrou responsável por uma nova etapa na história do hacking político, uma vez que deu início a uma verdadeira reconfiguração do hacking e do hacktivismo em escala global.

Para tratar dessa nova configuração, é importante observar que, embora o hacktivismo represente o hacking de computador em sua nuance mais transgressiva, não seria incorreto afirmar que o hacking de computador tem sido uma atividade carregada de traços políticos desde seu início, entre o fim da década de 1950 e o início da década de 1960. Voltemos, pois, às primeiras gerações de hackers.

1.1 HACKING: POLÍTICO EM SUA ESSÊNCIA

Esses traços políticos podem ser encontrados, por exemplo, no clássico *Hackers: heroes of the computer revolution*, em que Steven Levy (2010) desvela o código de ética, as motivações e o verdadeiro espírito que embasaram aquela que se tornou conhecida como a primeira geração de "hackers" – indivíduos que tinham como hábitat natural os laboratórios do MIT (Massachusetts Institute of Technology), no início dos anos 1960. Levy os qualifica como "pessoas muito fascinantes... sob seus exteriores frequentemente imponentes, eles eram aventureiros, visionários, pessoas correndo riscos, artistas... e aqueles que viram mais claramente por que o computador era uma ferramenta verdadeiramente revolucionária" (2010, on-line).

O autor mostra que, no cerne da chamada cultura hacker, está a noção de que as informações devem ser totalmente livres – isto é, que não sejam apropriadas ou controladas por ninguém – e de que o uso dos computadores, por seu potencial revolucionário de ação, deveria ser tão universal quanto possível. Ao tratar dos fundamentos de certa uma ética hacker, Levy pontuou vários de seus pontos-chave, cada um responsável por um subtítulo a ser explorado:

> O acesso aos computadores... deveria ser ilimitado e total.
> Todas as informações deveriam ser livres.
> Desconfie da autoridade – promova a descentralização.
> Hackers deveriam ser julgados por seus "hackeamentos", e não por falsos critérios, tais como graus de escolaridade, idade, raça ou posição social.
> Você pode criar arte e beleza em um computador.
> Os computadores podem mudar sua vida para melhor (LEVY, 2010, on-line).

Levy ainda constata que aqueles primeiros hackers de computador não se organizavam por meio de hierarquias; desconfiavam (e, por vezes, zombavam) da autoridade; promoviam ações colaborativas e descentralizadas; compartilhavam os resultados de seus trabalhos; e serviam, sempre que possível, ao restante da comunidade. Para eles, ainda, a habilidade (e não apenas o resultado final) também importava, e a prática era infinitamente superior às divagações teóricas.

De maneira semelhante, ainda de acordo com Levy, os hackers da chamada segunda geração – que marcou os anos 1970 e se tornou conhecida como a dos "hackers de hardware" – ansiavam por mudar as máquinas, tornando-as menores, mais usáveis, interativas e amigáveis. Em grande medida, um de seus objetivos era tirá-las do controle exclusivo dos técnicos especializados, levando-as ao máximo número possível de indivíduos, fomentando, portanto, um ato de empoderamento destes. Sem dúvidas, essa geração foi decisiva para a criação da microinformática e os desdobramentos dela.

Dessa forma, o relato de Levy nos permite observar que tanto os hackers da primeira quanto da segunda geração adotavam uma postura política diante das máquinas, das formas de autoridade e do acesso à informação.

Outras características políticas verificadas nas primeiras gerações do hacking de computador também podem ser identificadas na obra do finlandês Pekka Himanen *A ética dos hackers e o espírito da era da informação*. Himanen (2001) resgata o sociólogo alemão Max Weber[2] para argumentar – sob as influências principais da teoria da "era informacional", formulada pelo sociólogo Castells, e dos escritos e ações de Linus Torvalds, o criador do sistema operacional de código aberto Linux – que a ética hacker representa uma clara oposição à ética protestante e ao modo de vida dela derivado. Para tanto, divide sua obra em três partes, analisando três vertentes distintas (porém correlatas) da ética hacker: a ética do trabalho, a ética do dinheiro e a ética da rede.

A fim de realizar um contraponto, o filósofo elenca aqueles que seriam os sete valores

2 O próprio título da obra de Himanen dialoga com o ensaio *A ética protestante e o espírito do capitalismo*, escrito por Weber no início do século XX.

principais da ética protestante: dinheiro, trabalho, otimização, flexibilidade, estabilidade, determinação e contabilização dos resultados. Trata-se de uma ética sob a qual o trabalho deve ser encarado como um objetivo em si, não importando sua natureza ou o modo como é realizado; deve ser feito da melhor forma possível, otimizando tempo, monitorando os resultados, flexibilizando atividades para se obter maiores retornos; e deve ser visto como um dever incontestável à medida que gera lucro.

Paralelamente, Himanen trata dos sete principais valores da ética hacker: paixão e liberdade (referentes à ética do trabalho); valor social e abertura (referentes à ética do dinheiro); atividade e cuidar (em relação à ética da rede); e a criatividade, que permeia todos os demais valores.

Quanto à paixão, o autor argumenta que, para a cultura hacker, o trabalho não é um fim em si mesmo, tal como ocorre na ética protestante. Ao contrário: ele é algo instigante, motivador, que é apreendido e realizado, em muitos casos, de maneira divertida e apaixonada. Liberdade, por sua vez, diz respeito ao fato de que boa parte dos hackers não organiza sua vida e seu trabalho com base em dias úteis, rotinas mecânicas e otimizadas. Em vez disso, eles têm uma relação muito mais liberal diante do trabalho, o que nos sugere "um fluxo dinâmico entre trabalho criativo e outros prazeres da vida" (HIMANEN, 2001, p. 125). Com isso, a linha divisória que demarca os campos do trabalho árduo, de um lado, e do lazer despreocupado, de outro, é bem mais tênue do que para a maior parte das outras pessoas. Afinal, no protestantismo, segundo o filósofo, não há espaço para a diversão.

Quando ao valor social e à abertura, Himanen aponta que, para muitos hackers, o dinheiro não é apreendido como um bem em si mesmo. Isso significa dizer que o que guia o trabalho desses indivíduos não é a remuneração em si, mas seu valor social, o significado que ele representa para a comunidade. Além de criar algo valioso, é preciso que ele seja reconhecido, o que reforça o caráter meritocrático da cultura hacker. E, ao final de tudo, a "abertura" é crucial: não basta criar algo valioso se tal criação não puder ser usada, desenvolvida e testada por qualquer pessoa, de modo que todos possam se beneficiar do trabalho alheio, bem como aprender com ele.

A "atividade", por sua vez, envolve a defesa irrestrita da liberdade de expressão, sobretudo na Internet, e da privacidade – direitos que, para os hackers, são simplesmente invioláveis. Nesse aspecto, são absolutamente mal vistos (e, por vezes, incessantemente atacados) os governos ou empresas que sequer ameacem desrespeitar tais direitos. Já o

“cuidar” relaciona-se, segundo Himanen, com a preocupação diante do próximo, que culmina com “um desejo de libertar a sociedade virtual da mentalidade de sobrevivência que tão facilmente resulta de sua lógica” (2001, p. 126). Neste ponto, também se destaca o objetivo, defendido por muitos hackers, de levar cada vez mais pessoas a participarem da Internet e da cultura computacional, fazendo, assim, com que elas se beneficiem das informações nelas contidas e aproveitem todo o seu potencial de ação.

Por fim, os hackers que se portam segundo esses princípios fatalmente ganharão o respeito de seus pares, mas serão louvados como heróis caso consigam o último deles: a criatividade: “utilização imaginativa das habilidades de cada um, a surpreendente superação contínua de si mesmo, e a doação ao mundo e uma nova contribuição genuinamente valiosa” (2001, p. 127). E, geralmente, a criatividade é acompanhada de um humor sarcástico e penetrante.

Enfim, é também patente na obra de Himanen que há um caráter político que se encontra diluído nos próprios princípios e valores do hacking.

Mas, mesmo considerando políticos do hacking identificados por obras clássicas como as de Levy e Himanen, neste trabalho é preciso pontuar que o hacktivismo vai um pouco além disso. Enquanto as primeiras gerações estavam focadas nas políticas relacionadas a softwares e hardwares, os hacktivistas transpuseram mais claramente esse caráter político ao plano social, valendo-se dessas habilidades realizar atos concretos de protesto e de desobediência civil. Conforme se buscará conceituar em detalhes no próximo capítulo, o ativismo hacker pode ser definido como o uso de ferramentas digitais tendo em vista fins exclusivamente políticos, que não raro são logrados de maneiras especialmente transgressivas e/ou disruptivas. Ou, de forma mais ampla, trata-se da junção, por um lado, das ferramentas e conhecimentos técnicos encontrados no hacking e, por outro, de uma forma espeical de ativismo político – mais comumente realizado por meio das redes digitais de comunicação.

1.2 ORIGENS DO HACKTIVISMO

Pode-se afirmar, nessa conformação, que o hacktivismo tal como hoje o conhecemos tem uma de suas origens mais marcantes em meados da década de 1990, por meio do

engajamento na grande rede de colaboração com o apoio ao movimento zapatista – nas palavras de Castells (2002, p. 103), o "primeiro movimento de guerrilha informacional" da história.

De fato, Cleaver (1998) aponta que os zapatistas formaram uma grande teia eletrônica de luta em redor do Exército Zapatista de Libertação Nacional (EZLN), reunindo movimentos feministas, grupos de mídia independente, indígenas, ativistas de direitos humanos, ambientalistas, entre outros. Nesse sentido, em um interessante estudo realizado já nos anos 2000, os pesquisadores Garrido e Halavais (2003) elencaram os principais grupos que se engajaram nessa teia eletrônica, fazendo um mapeamento deles na rede por meio do cruzamento de links envolvendo seus websites e a página oficial do EZLN. E, além desses movimentos sociais tradicionais, que também se valeram massivamente da Internet e de demais mídias para se comunicar e chamar a atenção da comunidade internacional (ORTIZ, 2003), surgia um pequeno grupo de hacktivistas que resolveu levar o ativismo político a práticas mais transgressivas no campo virtual.

Quem conta boa parte dessa história é Stephen Wray, que aponta o ano de 1998 como o marco inicial para o surgimento dos termos "desobediência civil eletrônica" e "hacktivismo". Wray (1998) relata que, após o massacre de Acteal – confronto entre a comunidade zapatista e o exército mexicano que deixou um saldo de 45 mortos (na maioria, indígenas) –, um grupo chamado Electronic Disturbance Theater (EDT) criou um software pioneiro, o Zapatista FloodNet, e convidou diversos indivíduos para, por meio dele, participarem de protestos on-line em massa contra o governo mexicano. O aplicativo possibilitava a quem não tivesse conhecimento técnico a realização de ações distribuídas de negação de serviço (*Distributed Denial of Service*, ou DDoS).[3] Com isso, bastava que o internauta colocasse a URL dos sites-alvo[4] no FloodNet para que este começasse a inundar os servidores com pedidos de acesso. De acordo com Wray, entre os dias 9 e 10 de setembro

3 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 essa 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. Convém observar que 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).

4 Entre os alvos, destacam-se os sites da presidência do México, da bolsa de valores daquele país e do Pentágono, símbolos do capital internacional.

setembro de 1998, cerca de 20.000 pessoas utilizaram o aplicativo em uma ação de massa que reverberou em veículos de mídia de várias partes do mundo.

Além das experiências do EDT, Wray relata uma série de atos hacktivistas que ocorreram naquele ano na Grã-Bretanha, na Áustria, na Índia, na China, de forma que, em quase todos os continentes, houve relatos de "hacktividade".

Assim, tendo como um de seus pioneiros o EDT, ao longo dos anos o hacktivismo ganhou diversas roupagens, de forma que muitos grupos se tornaram conhecidos por suas ações – tais como interceptação de dados, desenvolvimento de aplicativos que permitissem furar bloqueios de censura na internet, ações de negação de serviço, paródias virtuais, desfiguramento de sites, entre outros.

O hacking e o hacktivismo, no entanto, sofreram um duro golpe no ano de 2001. Por um lado, Antoun (2011) observa que houve um racha no movimento hacker a partir dos ataques terroristas às torres gêmeas, ilustrado por uma série de desentendimentos entre os membros da lista de discussão do congresso Hope, da publicação *2600*. Enquanto parte do movimento queria atender ao apelo do departamento de Defesa dos Estados Unidos de "guerra ao terror", realizando, para isso, uma série de investidas contra países árabes e comunistas, levando a eles a liberdade de expressão, outra parte primou pela não agressão. Com isso, a lista se desfez e o movimento se viu dividido.

Por outro lado, após os atentados terroristas e a implementação do Ato Patriótico nos Estados Unidos, que despertou uma onda de vigilância naquele país e em todo o mundo, firmou-se em definitivo uma visão que imperava nos discursos dos governos e dos meios de comunicação desde pelo menos os anos 1980: a de que os hackers são perigosos cibercriminosos, ou até mesmo terroristas, e o hacking se configura como uma atividade antissocial e criminosa (VEGH, 2003).

Douglas Thomas (2002) aponta, por exemplo, que o filme *WarGames*, de 1983, foi um dos grandes responsáveis por influenciar de maneira desproporcional e negativa a representação dos hackers na mídia. Com isso, Galloway (2004, p. 153) também constata que, "depois de uma combinação de tecnofobia pública e agressiva legislação governamental, a identidade do hacker mudou, em meados dos anos 1980, de um hobista para um cibercriminoso".[5]

Dessa maneira, embora não tenham, em absoluto, deixado de existir, as ações

5 Para um estudo bem fundamentado acerca dessa deterioração quanto à imagem pública dos hackers, Cf. Sterling (1993).

hacktivistas mantiveram-se ainda mais ocultas e veladas, chamando pouca atenção e raramente chegando de forma marcante aos meios de comunicação de massa.

Esse cenário, no entanto, alterou-se no final dos anos 2000. Com a chegada dos Anonymous, a história do ativismo hacker ganhou um novo capítulo.

1.3 A LEGIÃO DOS ANONYMOUS

A partir do ano de 2008, o hacktivismo não apenas começa a renascer, mas o faz emergindo do espaço *underground* e criando imenso alarde, a ponto de preocupar governos e corporações do mundo inteiro. Pretensamente escondidos pela máscara de Guy Fawkes,[6] que se tornaria o símbolo principal dos Anonymous, centenas de indivíduos e grupos hacktivistas espalhados por todo o mundo sentiram-se à vontade para começar a realizar diversas ações, esforçando-se ao máximo para chamar a atenção da imprensa internacional.

Conforme apontaremos mais detalhadamente no capítulo III, seria incorreto dizer que "Anonymous" diz respeito um grupo ou a um conjunto unificado e formal de indivíduos. Trata-se, antes disso, de uma ideia e uma forma de ação compartilhados por uma ampla, difusa e heterogênea rede de grupos e indivíduos atuando em todo o mundo. Por se tratar de uma ideia, não conta com donos, liderança central e muito menos centro geográfico. Da mesma forma, para aderi-la, não é preciso pedir permissão ou passar por qualquer tipo de processo seletivo. Justamente por isso, muitos se dizem Anonymous, mas ninguém se diz *do(a)* Anonymous.

Originalmente, Gabriela Colleman (2011) observa que os primeiros registros de indivíduos agindo sob essa alcunha remontam ao 4Chan, um popular fórum de imagens para o qual é possível enviar mensagens de maneira anônima e no qual não se guardam quaisquer registros. Os primeiros atos desses indivíduos são realizados simplesmente *for the lulz*,[7] isto é, por pura diversão, e eram fundadas no princípio da trollagem[8] (chacota, provocação, uma espécie de *bullying* eletrônico). Escolhido um alvo, podendo ser uma pessoa ou organização,

6 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.

7 "Lulz" é uma corruptela de LOL, ou *laughing out loud* ("rindo alto", em tradução literal).

8 Diz respeito a chacotas, provocações, uma espécie de *bullying* eletrônico. Cf.: O que é trollar? Disponível em: <http://www.tecmundo.com.br/curiosidade/20149-o-que-e-trollar-.htm>. Acesso em: 4 abr. 2012.

ele se tornaria vítima de ataques bem humorados e sórdidos. No 4Chan, foram coordenadas ações como trotes telefônicos, sucessivos pedidos de pizzas para um endereço alvo, revelação de informações pessoais destes alvos, ações DDoS, entre outros. Pelo menos até o ano de 2006, indivíduos Anonymous realizaram várias dessas ações – unicamente *for the lulz*.

Dois anos mais tarde, em 2008, Coleman relata que os Anonymous passaram "do *lulz* à ação coletiva", transformando-se em um coletivo de ativistas políticos, e passando a lutar por diversas causas. O episódio que marcou essa transição, conforme observaremos, foi uma imensa onda de protestos contra a Igreja da Cientologia norte-americana, que passou a ser conhecida como Operação Chanology (#OpChanology). O ponto de partida foi a divulgação de um vídeo[9] (prática que se tornaria corriqueira nas próximas ações dos Anonymous) declarando guerra contra a instituição. Nele, já éramos apresentados a outro de seus símbolos – uma pessoa trajando terno escuro e sem um rosto, ressaltando o caráter anônimo do movimento – e àquela que se tornaria a assinatura virtual utilizada pela rede, algo que se faria presente em todos os seus comunicados futuros: "Nós somos Anonymous. Somos uma legião. Nós não perdoamos. Nós não esquecemos. Aguardem-nos".[10]

A partir de então, além de diversos ataques virtuais, foram produzidos inúmeros posts em sites, blogs e redes sociais chamando a atenção para o fato de que a Igreja estava violando o sagrado princípio da liberdade de expressão. Paralelamente, também foram investidas diversas ações de negação de serviço contra sites da Igreja. E, em 10 fevereiro daquele ano, diversos manifestantes envolvidos com a questão decidiram ir às ruas: em várias capitais do mundo, mais de 6.000 pessoas organizaram protestos, sobretudo em frente às sedes da Igreja da Cientologia na América do Norte, Europa, Nova Zelândia e Austrália.

Dois anos mais tarde, em 2010, os Anonymous mais uma vez chamaram a atenção de todo o mundo e entraram definitivamente na agenda pública ao deflagrarem uma maior e mais complexa operação – a #OpPayBack, que ganhou força com o imbróglio envolvendo a organização internacional Wikileaks e as empresas PayPal, Mastercard e Amazon, que atenderam aos pedidos do governo norte-americano de bloquear as doações monetárias destinadas ao site da organização (no caso das duas primeiras) e de bloquear o acesso a seu servidor no qual o site hospedava seu conteúdo (no caso da Amazon).

Naquela ocasião, os Anonymous não apenas militaram para registrar seu apoio ao Wikileaks, com quem trabalhariam em conjunto outras vezes, mas resolveram responder

9 Disponível em: <www.youtube.com/watch?v=JCbKv9yiLiQ>. Acesso em 7 dez. 2011.
10 Tradução para: "We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us".

diretamente às empresas em questão. Com isso, durante algumas horas, seus hackers, nesta ocasião também organizados por meio do IRC,[11] foram responsáveis por desabilitar os sites destas que são algumas das maiores corporações do mundo, inviabilizando seus serviços on-line e causando uma série de prejuízos.

Conforme apontaremos no terceiro capítulo, é precisamente na #OpPayBack que começam, ainda que de forma incipiente, as primeiras atividades dos Anonymous Brasil, o objeto de estudo deste trabalho, que se dedica a verificar como os Anonymous se engajam politicamente no contexto das chamadas sociedades de controle.

1.2 JUSTIFICATIVA

Como objetivo mais amplo e geral, esta pesquisa pretende contribuir para o estudo e a compreensão acerca dos novos movimentos políticos que surgem na aurora da chamada era informacional, aqui compreendida em um cenário hipermidiático e, vale ressaltar, hipercontrolado (GALLOWAY, 2004).

Tais movimentos, em sua maioria, atuam em rede, valendo-se das tecnologias digitais de comunicação e formando células independentes que operam de maneira distribuída. Com base na obra de Foucault, Silveira (2012) argumentou que, no mundo industrial, o controle disciplinar produziu formas específicas de resistência, como sindicatos e associações. Mas o pesquisador observa que, já na transição para um capitalismo cognitivo, pós-industrial, despontam novas formas de resistência, como o ativismo hacker. Ao passo que as primeiras foram vastamente contempladas pela literatura acadêmica em todo o mundo e nas mais diversas áreas, as últimas, incluindo o hacktivismo, permanecem em um terreno fértil no qual há muito a ser explorado.

Por isso, este trabalho se justifica, também, pela escassez de estudos relacionados ao ativismo hacker – sobretudo na academia brasileira –, mas, principalmente, pela inexistência de trabalhos publicados sobre os Anonymous brasileiros. No plano internacional, pesquisadores e escritores como Quinn Norton, Parmy Olson, Max Halupka, Alex Gekker e,

11 IRC é um protocolo de comunicação da Internet que pode ser utilizado para conversas e troca de arquivos leves. Quando as ações dos Anonymous passaram se tornar mais complexas, envolvendo grandes quantidades de pessoas, diversos servidores de IRC foram criados para que elas fossem minimamente coordenadas.

em especial, Gabriella Coleman se destacam no estudo e na descrição da rede hacktivista, mas suas análises se restringem aos contextos norte-americano, europeu e australiano. Portanto, no que diz respeito aos Anonymous no contexto brasileiro, até o momento, esta pesquisa se mostra inédita.

Para além disso, entendemos que compreender o hacktivismo e suas principais expressões nos ajuda a compreender as novas configurações dos processos de participação política na era informacional. À medida que nossas sociedades se veem permeadas por (e dependentes de) redes informacionais digitais, que os softwares se apresentam como sua principal mídia (MANOVICH, 2008), e que, por meio dessas redes trafegam nossas principais informações pessoais, culturais, políticas e econômicas, os hackers emergem como atores políticos de grande relevância.

Isso se dá porque, primeiramente, tais redes informacionais são seu hábitat natural: os códigos, protocolos, linguagens e formatos que as compõem lhes são tão familiares e facilmente manipuláveis como uma língua materna. "Por conhecerem o protocolo melhor do que ninguém, os hackers o empurram em direção a um estado de hipertrofia, esperando que saia do outro lado. Então, por um lado, os hackers são criados pelo protocolo, mas, por outro, os hackers são atores protocológicos por excelência", observa Alexander Galloway (2004, p. 158).

Em segundo lugar, em função de seu vasto conhecimento técnico em relação a estes sistemas, os hackers ativistas conseguem, como ninguém, interferir por meio deles no campo comunicacional – o local onde é travada a disputa pelo poder, segundo interpretação de Castells (2009). Por isso, segundo o autor, os hackers politicamente ativos são um elemento fundamental no movimento por justiça global:

> Sua capacidade tecnológica para utilizar as redes de computadores com propósitos distintos dos que haviam sido atribuídos pelas empresas colocou os hackers na linha de frente do movimento, liberando o ativismo das limitações à expressão independente impostas pelo controle empresarial das redes de comunicação (CASTELLS, 2009, p. 345).

Isto posto, este trabalho também se justifica na medida em que contribui, ainda que mínima e indiretamente, com os estudos sobre o futuro da participação política e das novas formas de mobilização à medida que identifica e resgata atores políticos cuja relevância se alarga na sociedade informacional. Expressão marcante vivenciada por parte desses atores, os

Anonymous atuam politicamente valendo-se de uma composição estrutural única, cujas características fizeram do coletivo um enorme agregador de ativistas. Na continuação deste trabalho, espera-se que seja possível traçar um mapa preliminar dessas características no contexto brasileiro, que auxiliarão nas discussões que a pesquisa se propôs a realizar segundo os procedimentos que se seguem.

1.3 PROCEDIMENTOS METODOLÓGICOS

Tomando como ponto de partida o principal objetivo deste trabalho – a saber, investigar como a rede Anonymous se engaja politicamente, entendendo o hacktivismo como uma forma de resistência política nas sociedades de controle –, seria fundamental encontrar uma metodologia que permitisse observar a questão tanto por meio de ações práticas deflagradas por genuínos ativistas hackers brasileiros, envolvendo sua forma de organização e seus principais métodos, quanto pelas principais questões que permeiam o coletivo no Brasil, como sua origem, suas inspirações, sua forma de criar ideais etc. É dessa forma que se optou por realizar um estudo de caso descritivo da vertente brasileira da principal expressão do ativismo hacker nos últimos anos.

Robert Yin (2001, p. 32) define o estudo de caso como "uma investigação empírica que investiga um fenômeno contemporâneo dentro de seu contexto da vida real, especialmente quando os limites entre o fenômeno e o contexto não estão claramente definidos". O estudo descritivo, que, segundo o autor, deve traçar uma sequência de eventos ao longo do tempo, descrevendo uma subcultura e descobrindo seus principais fenômenos, difere do exploratório e do explanatório. Enquanto este propõe explanações concorrentes para o mesmo conjunto de eventos, indicando como essas explanações possam se generalizar para outras situações, aquele ocorre em situações nas quais o fenômeno avaliado ainda não é capaz de fornecer resultados simples e claros, mas sim uma exploração inicial.

Com isso, este trabalho se propõe descritivo por acreditar que ainda não se pode, dado o caráter incipiente do fenômeno analisado, propor explicações finais e generalizáveis acerca desse objeto. No entanto, é plenamente possível descrevê-lo por meio de seus principais traços e dos acontecimentos marcantes que o compõem.

Para tanto, foram empregadas diversas técnicas de pesquisa, a depender do desafio específico que se buscou alcançar. Elas foram combinadas em pesquisa primária, de um lado (documentação, pesquisa bibliográfica, leitura da cobertura realizada pela imprensa e, principalmente, entrevista com indivíduos identificados com os Anonymous Brasil), e da observação direta, de outro.

O ponto de partida se deu na busca pelas origens e pelas principais faces apresentadas pelo coletivo no contexto brasileiro. Isso se mostrou possível por meio de entrevistas com 22 indivíduos – em sua esmagadora maioria, hackers – que atuaram junto aos Anonymous no Brasil, sendo 20 delas via comunicador instantâneo on-line e outras 2 presencialmente. Este pesquisador, sempre se identificando como tal, teve acesso a tais indivíduos por meio das ferramentas de comunicação comumente usadas pelo coletivo, como canais em servidores de IRC, blogs e perfis em redes sociais. Além disso, tais entrevistas frequentemente nos remeteram à conversa com outros indivíduos de diferentes grupos também identificados como Anonymous brasileiros. Nessas abordagens, muitos se dispuseram a relatar suas experiências e, por meio da reconstituição de seus depoimentos, foi possível delinear os pontos tratados acima. E, de forma complementar às entrevistas realizadas, como se observará, foram utilizados diversos relatos feitos por grupos e indivíduos identificados com os Anonymous em sites, blogs, redes sociais, além de repositórios de vídeos (como o YouTube) e textos (como o Pastebin) na rede.

Em seguida, fez-se oportuno observar a presença do coletivo na rede. Para tanto, foram escolhidas duas operações pontuais deflagradas por diferentes grupos autoidentificados como Anonymous no Brasil: a operação WeeksPayment (#OpWeeksPayment) e a operação Globo (#OpGlobo). Observou-se especificamente o modo como foram propostas, seu método de ação, a comunicação do coletivo com o público externo, o recrutamento de apoiadores para os atos, os principais grupos neles envolvidos e as contradições explícitas entre estes e demais grupos Anonymous.

Para viabilizar essa análise, foram armazenados os registros de postagem dos dois principais canais de comunicação utilizados pelos grupos durante as operações: o Twitter e o IRC. O primeiro foi utilizado, entre outras coisas, para comunicação com o público externo a fim de expor os motivos para se realizar as operações e também para conquistar apoiadores. Por isso, foram armazenados por meio da ferramenta on-line myTwebo[12] todos tweets

12 Disponível em: <http://www.mytwebo.com>. Acesso em: 15 jan. 2012. Para armazenar os tweets de um perfil específico, basta fazer login com uma conta do Twitter e digitar o perfil em questão. Nos armazenamentos

postados pelos perfis que assumiram a responsabilidade pelas operações durante os dias em que estas ocorreram.

O IRC, por sua vez, tem sido utilizado com a finalidade, entre outras, de organizar as operações realizadas por grupos Anonymous em todo o mundo junto a ativistas que já estão nelas engajados. Trata-se mais de um canal interno de comunicação, portanto. No caso da Operação Globo, na qual o IRC foi utilizado sistematicamente durante todos os dias do feriado prolongado da Paixão de Cristo em 2012, quando a operação ocorreu, os logs do canal em que se discutia sobre a #OpGlobo, registrado na rede VoxAnon, foram coletados pelo próprio pesquisador, que acompanhou as ações em tempo real pela rede. Isso se deu por meio da simples habilitação da opção de registro de logs (de conversações em canais abertos e mensagens privadas) no software XChat, cliente de IRC que se utilizou.

A partir da análise e da observação direta dessas duas operações, foi possível entrar em contato com alguns dos indivíduos que se engajaram nelas. Com eles, este pesquisador também realizou repetidas entrevistas, que possibilitaram a coleta de mais informações sobre as referidas operações.

1.4 ESTRUTURA

O capítulo II, logo a seguir, apresenta-se com a finalidade de discutir o fenômeno do hacktivismo como uma forma de resistência política no contexto da sociedade de controle, mostrando as principais estratégias mais comumente utilizadas para este fim. Por isso, recorreu-se, no primeiro momento, à pesquisa bibliográfica para alinhavar tanto as fundações teóricas dessa sociedade, que remontam à obra de Deleuze (1992), quanto as principais expressões acadêmicas dela decorrentes nos últimos anos – como Costa (2004), Galloway (2004), Hardt (2000), Pelbart (2011), Santos (2003), Silveira (2012), entre outros. Em seguida, para dar sustentação às inferências aqui realizadas, a mesma técnica de pesquisa bibliográfica nos levou às principais perspectivas teóricas que já lançaram interpretações sobre o ativismo hacker, oriundas das mais diversas áreas do conhecimento. Nesta pesquisa, tais perspectivas foram divididas em (1) Desobediência civil digital; (2) Guerra da informação / ciberterrorismo; e (3) Hacktivismo por ele mesmo.

realizados para esta pesquisa, foram capturados até 1.000 tweets que antecederam o momento da solicitação.

O capítulo III, por sua vez, apresenta os principais resultados deste trabalho no que se refere à pesquisa empírica. Em primeiro momento, recorre a pesquisadores estrangeiros e a relatos na imprensa para identificar o início e as grandes ações do movimento em nível internacional. Logo depois, relatam-se as origens e as principais faces dos Anonymous no contexto brasileiro, em quatro etapas divididas em ordem cronológica: início, operacional, ápice e dispersão. Parte da operação global PayBack, em 2011, para, em seguida, proceder à análise de duas operações deflagradas por hacktitistas brasileiros – a Operação WeeksPayment e a Operação Globo, ambas ocorridas no ano de 2012.

No capítulo IV, recuperaram-se os elementos apresentados no capítulo III para refletir, ainda que de modo preliminar, acerca da questão central desta pesquisa – como os Anonymous se engajam politicamente? – e seus desdobramentos. Sugerem-se quatro formas de engajamento, que englobam as principais estratégias de ação relatadas ao longo do trabalho: promovendo o anonimato; evangelizando; formando redes distribuídas; e exibindo e possibilitando várias formas de ações políticas. Além disso, destacaram-se alguns breves apontamentos teóricos que, dadas as limitações deste trabalho, não puderam ser contemplados.

Por fim, as considerações finais discutem o coletivo Anonymous à luz da sociedade de controle, apontando as principais inferências realizadas ao longo da pesquisa. Nesse sentido, também pondera quanto às evidentes limitações deste trabalho, suas contribuições para eventuais pesquisas futuras relacionadas ao tema, além dos principais tópicos que ainda merecem ser estudados por pesquisadores da área.

2. CONTROLE E RESISTÊNCIA NAS REDES DIGITAIS

> "Nenhuma forma de poder parece ser tão sofisticada quanto aquela que regula os elementos imateriais de uma sociedade: informação, conhecimento, comunicação" (COSTA, 2004, p. 162-3)

> "A Rede poderia ter sido desenhada para revelar quem uma pessoa é, onde ela está, e o que ela está fazendo. E, se ela fosse assim desenhada, ela poderia se tornar o lugar mais regulado que o homem jamais conheceu" (LESSIG, 2006, p. 38)

À medida que as sociedades contemporâneas constroem e adotam novas tecnologias digitais de comunicação, despontam, por um lado, formas de comando e de controle cada vez mais precisas e sofisticadas e, por outro, formas inovadoras por meio das quais se resiste a esse controle. A crescente digitalização das informações pessoais, profissionais, culturais, financeiras etc. habilita um rápido e fácil manejo sobre esses dados, o que mantém os indivíduos potencialmente controlados a todo momento. Da mesma maneira, contudo, as ferramentas técnicas que possibilitam tamanho controle não raro são apropriadas com a finalidade de bloqueá-lo, transpô-lo e, frequentemente, hipertrofiá-lo.

A fim de discutir esse tema e sua relação com o objeto de estudo deste trabalho – o ativismo hacker, em geral, e a rede hacktivista Anonymous do Brasil, em particular –, recorrer-se-á, neste capítulo, à fundação teórica da chamada "sociedade de controle", tal como formulada pelo filósofo francês Gilles Deleuze no final da década de 1980. A partir dela, serão discutidas algumas de suas expressões e repercussões na literatura acadêmica, tendo em vista o papel fundamental das tecnologias digitais de comunicação nessa relação, para, em seguida, identificarmos as principais perspectivas teóricas que se dedicam ao estudo do hacktivismo.

2.1 SOCIEDADE DO CONTROLE

Ao situar a chamada sociedade de controle, Gilles Deleuze opera na esteira de uma periodização da história levada a cabo pelo também filósofo francês Michel Foucault e

sistematizada pelo próprio Deleuze (2005). Foucault identificou as denominadas sociedades disciplinares entre os séculos XVIII e XIX, de modo que estas se seguiriam às sociedades de soberania. O ponto de transição entre ambas (soberania e disciplina) seria representado, ainda segundo Foucault, na figura de Napoleão Bonaparte (1769-1821). Inúmeras são as diferenças entre esses dois mapas sociais (de agora em diante, "diagramas"), mas, tendo em vista o escopo deste trabalho, cabem aqui algumas considerações imprescindíveis sobre o exercício e os mecanismos de poder existentes em cada um deles.

As sociedades de soberania podem ser caracterizadas pela existência de um poder absoluto concentrado nas mãos do soberano. Este, em nome da soberania do Estado, vale-se de um poder de morte: o poder de fazer morrer e de deixar viver. "O súdito deve sua vida e sua morte à vontade do soberano. Mais do que a vida, porém, é a morte que ele deve ao soberano", conforme aponta Peter Pál Pelbart (2011, p. 55-56): "O poder, no fundo, é mais um mecanismo de retirada, de subtração, de extorsão, seja da riqueza, dos produtos, bens, serviços, trabalho, sangue. É um direito de apropriar-se de coisas, de tempo, de corpos, de vida, culminando com o privilégio de suprimir a própria vida". Ou seja, trata-se de um poder negativo, restritivo, calcado na expropriação. No limite, o soberano tinha plenos poderes para apelar à suprema restrição: minar a vida.

Na passagem às sociedades disciplinares, tal poder de fazer morrer e deixar viver sistematicamente dá lugar ao poder de fazer viver e deixar morrer. Trata-se de um poder sobre a vida, sobre a gestão de vidas – em suma, um biopoder. Este é tomado por duas formas principais, a saber: a disciplina e a biopolítica (e, na articulação entre ambas, está o sexo). Por um lado, há as regulações, o adestramento dos corpos, a otimização das forças da vida e sua integração a sistemas de controle – sistematizados em instituições disciplinares como a fábrica, a escola, a família, o quartel e a prisão. Por outro, observa-se a gestão da vida tendo em vista não somente o indivíduo, mas toda a espécie. A população torna-se um problema biológico, científico e estatístico. Aqui têm início as políticas de controle e gestão das taxas de natalidade e mortalidade, do nível geral de saúde, da longevidade etc. Enfim, o poder investe-se sobre a vida:

> Um sistema geral de vigilância-reclusão penetra por toda a espessura da sociedade, tomando formas que vão desde as grandes prisões, construídas a partir do modelo do Panopticon, até as sociedades de patronagem e que encontram seus pontos de aplicação não somente nos delinquentes, como também nas crianças abandonadas, órfãos, aprendizes, estudantes, operários

> etc. (FOUCAULT, 1997, p. 38).

Ainda em relação à natureza do poder: a fim de formular a análise sobre as sociedades disciplinares, Foucault também considerou que seria preciso relegar a teoria clássica sobre o poder. Isso porque a imagem das sociedades disciplinares e, acima delas, do soberano suscitou uma série de representações unicamente jurídico-discursivas. Isto posto, o modo de manifestação e a forma de aceitabilidade do poder tomariam forma exclusivamente no direito. Daí se apreende que há um foco, um pouco central, uma fonte da qual o poder emana e arrebata a tudo e todos. Antes qualquer coisa, ele tem um local: o Estado. Para Foucault (1988, p. 100), portanto, é preciso libertar-se dessa representação jurídico-discursiva para proceder a qualquer análise:

> Se é verdade que o jurídico pôde servir para representar, de modo sem dúvida não exaustivo, um poder essencialmente centrado na coleta e na morte, ele é absolutamente heterogêneo com relação aos novos procedimentos de poder que funcionam não pelo direito, mas pela técnica, não pela lei mas pela normalização, não pelo castigo mas pelo controle, e que se exercem em níveis e formas que extravasam do Estado e de seus aparelhos. Entramos, já há séculos, num tipo de sociedade em que o jurídico pode codificar cada vez menos o poder ou servir-lhe de sistema de representação.

E, ainda, em outra passagem:

> Seria preciso tentar estudar o poder não a partir dos termos primitivos da relação, mas a partir da própria relação, uma vez que é ela que determina os elementos dos quais trata: mais do que perguntar a sujeitos ideais o que puderam ceder deles mesmos ou de seus poderes para se deixar sujeitar, é preciso procurar saber como as relações de sujeição podem fabricar sujeitos (FOUCAULT, 1997, p. 71)

Dessa forma, era preciso assumir outra teoria do poder, compatível com os novos mecanismos, não redutíveis à pura representação do direito. Assumir o poder como um não-lugar; como a multiplicidade de correlações de força existentes no campo social; como a relação entre as lutas e afrontamentos, além dos apoios adquiridos em cada um deles; como as estratégias de dominação; enfim, como o infinito jogo de poderes verificado nas sociedades. Afinal, "o poder está em toda parte […] porque provém de todos os lugares" (FOUCAULT, 1998, p. 103). Por conseguinte, as formas de controle também se verificam descentralizadas. Os indivíduos são controlados em seus lares, nas escolas, nas fábricas. À medida que se deixa

uma instituição disciplinar, rapidamente já se chega a outra, iniciando um novo ciclo de controle.

Ao lançar as bases da sociedade de controle, Deleuze afirmou que Foucault sabia da brevidade do modelo disciplinar, cujas instituições (novamente, a família, a escola, a prisão etc.) mostram-se em permanente crise. “Novas forças se instalavam lentamente e se precipitariam depois da Segunda Guerra Mundial: sociedades disciplinares é o que já não éramos mais, o que deixávamos de ser” (DELEUZE, 1992, p. 223-4). Deleuze segue Foucault ao tratar o poder como algo desprovido de centro de comando, mas indica que a sociedade de controle apresenta mecanismos ainda mais sofisticados para implementar o poder, que passa a ser exercido ao ar livre, de modo totalmente distribuído, ao contrário das antigas disciplinas, que dependiam da arquitetura de sistemas fechados de confinamento.

Dessa forma, nas sociedades disciplinares, a linguagem comum a todos os meios de confinamento é analógica. Ao deixar uma instituição para adentrar outra (ex: da fábrica para a família), supõe-se que o indivíduo comece do zero; já na sociedade de controle, a linguagem que une os comandos é completamente numérica.

O confinamento disciplinar opera como uma moldagem, literalmente moldando e disciplinando os indivíduos. Assim, um mesmo molde fixo pode ser aplicado a diversas formas sociais. Os controles, em contrapartida, são representados por uma modulação, isto é, uma moldagem autodeformante, adaptável, flexível, altamente mutante. A disciplina pode ser representada pela fábrica: tal como inseridos em uma moldagem, os trabalhadores realizam todos o mesmo trabalho, recebem o mesmo salário e até mesmo negociam coletivamente. Já o controle é marcado pela empresa: em diferentes modulações, colaboradores desempenham trabalhos distintos, recebendo valores distintos, e estimulados pelos mais variados tipos de prêmios, bonificações etc.

Se, na disciplina, começa-se do zero a todo momento, na sociedade de controle, nunca se termina nada. A mesma modulação autodeformante interpenetra a formação educacional, o trabalho na empresa, a vida em família. Se as sociedades disciplinares implementavam o controle por meio do confinamento, ou seja, em espaços fechados, o controle permite e incentiva uma verdadeira interpenetração dos espaços, tornando os indivíduos prisioneiros em campo aberto, sempre rastreáveis.

Nesse sentido, dois polos caracterizam as sociedades disciplinares: a assinatura (signo maior da identidade pessoal produzida pelo indivíduo) e o número de matrícula (indicador da

posição do indivíduo na massa). Afinal, o poder massifica (constituindo um só corpo de domínio) e individualiza (moldando cada indivíduo). Já na sociedade de controle, a assinatura e a matrícula são muito menos importantes do que a cifra: uma senha (ou código) que autoriza ou desautoriza o acesso a determinada informação, localidade, fonte etc. Munidos de uma senha, os seres passam a ser dividuais, isto é, divisíveis: são aceitos em determinadas situações, mas recusados em outras. Segundo Laymert Garcia dos Santos (2003, p. 151):

> Traduzido informação digital e genética, o indivíduo torna-se divisível, ou, para usar o termo empregado por Gilles Deleuze, "dividual". O sujeito não é mais modelado de uma vez por todas, mas sim permanentemente modulado, segundo uma nova lógica de cominação que nos faz passar da sociedade disciplinar para a sociedade de controle.

Dessa forma, para determinadas funções, uma senha ou código serve ao sujeito dividual. No entanto, para outras, ela lhes é completamente inútil. A modulação, contudo, é contínua: o código, que identifica o indivíduo, acompanha toda a sua mobilidade pelo espaço.

Por fim, acompanhando as mudanças pelas quais passou o capitalismo, as tecnologias de que se valeram as sociedades disciplinares (máquinas energéticas, termodinâmicas) passam, paulatinamente, a dar lugar a máquinas de informática, que também cumprem com o papel de auxiliar no controle dos indivíduos sem que estes precisem estar dentro dos limites das fronteiras de determinados espaços físicos. "O controle é de curto prazo e de rotação rápida, mas também contínuo e ilimitado, resume Deleuze (1992, p. 228).

Tabela 1 – Disciplina x controle

Sociedades disciplinares	**Sociedade do controle**
Linguagem analógica	Linguagem numérica
Confinamento: molde fixo aplicado a diversas formas sociais	Controle: modulação, uma moldagem autodeformante que muda continuamente
Fábrica: indivíduos em um só corpo	Empresa: indivíduos dividuais
Não se para de recomeçar do zero	Nunca se termina nada
Dois pólos: a assinatura e o número de matrícula	O essencial é a cifra: uma senha
Par massa/indivíduo	Indivíduos tornam-se dividuais
Máquinas energéticas	Máquinas de informática e computadores
Capitalismo de concentração, voltado para a	Capitalismo de sobre-produção. Foco em

produção. Foco em produtos	serviços e ações
Família, escola, exército, fábrica são espaços analógicos distintos que convergem para um proprietário (Estado ou potência privada)	Família, escola, exército, fábrica são figuras cifradas, deformáveis e transformáveis
Disciplina de longa duração, infinita e descontínua	Controle de curto prazo e duração rápida, mas contínuo e ilimitado

O ensaio em que Deleuze apresentou e (minimamente) descreveu a sociedade de controle, intitulado "Post-scriptum sobre as sociedades de controle", tem pouco mais de 6 páginas. Outras considerações a respeito desse novo diagrama de poder encontram-se espalhadas por fragmentos de textos e entrevistas concedidas pelo filósofo, como aquela intitulada "Controle e devir", em que conversa sobre o assunto com o teórico italiano Toni Negri. Embora profética e inspiradora, essa formação teórica apenas nos indica, conforme apontou Michael Hardt (2000), "uma simples imagem dessa passagem [das sociedades disciplinares à de controle], uma imagem sem dúvida bela e poética, mas não suficientemente articulada".

Por razões evidentes, Deleuze não pôde relacionar integralmente o controle distribuído com o uso maciço, nos tempos atuais, das mais diversas tecnologias digitais de comunicação, nem às novas práticas que emergiram em resistência a essa forma de controle. Tampouco foi possível observar o crescente predomínio, na comunicação contemporânea, do arranjo midiático de massa mais controlado (e controlador) de que se teve notícia: a Internet (GALLOWAY, 2004). Dessa forma, Deleuze semeou as bases teóricas para um pensamento no qual uma vasta gama de autores se apoiaria a fim de interpretar certos fenômenos vigentes nas sociedades contemporâneas. A seção que se segue pretende discutir o trabalho de parte desses teóricos.

2.2 COMANDO E CONTROLE NAS REDES DIGITAIS

No mundo contemporâneo, é possível afirmar que as tecnologias digitais de comunicação tornaram-se algumas das principais ferramentas da sociedade de controle, sendo que a Internet passou a ser uma de suas maiores expressões e os hackers, um de seus principais atores políticos. Afinal, as novas tecnologias de comunicação e as redes

informacionais são, antes de qualquer coisa, tecnologias e redes de controle. Permitem, cada uma a seu modo, um controle horizontal, disperso, distribuído, impessoal. Portanto, de maneira muito simples, com a crescente e irreversível digitalização das informações, combinada ao uso irrefreável de tecnologias de comunicação em um cenário hipermidiático, todo e qualquer (ciber)cidadão é passível de ser controlado a todo momento – e em campo aberto.

Isso ocorre, por exemplo, quando se utiliza qualquer aplicação web: acesso à conta de e-mail, atualização do perfil em determinada rede social, visita a um site de compras, download de um documento, leitura de um texto etc. À medida que usuários navegam na rede, invariavelmente deixam rastros que são, mais do que depressa, manipulados, quantificados, relacionados. O mesmo acontece quando se faz uma operação financeira, quando se realiza uma chamada telefônica, ou mesmo quando alguém porta consigo um telefone móvel. Enfim, as redes sociotécnicas são abundantes (e crescem cada vez mais): comércio, transporte, telefonia, telecomunicações, água, luz, computação etc. Todas atividades realizadas nessas redes são rastreáveis e geram um conjunto de dados e padrões de comportamento que são muito caros e rentáveis às instituições típicas do capitalismo pós-industrial – ou imaterial, na formulação de Gorz (2005).

Nessa sentido, Rogério da Costa (2004, p. 164) observa que a sociedade de controle acarretou uma mudança em uma das formas de controle – a vigilância:

> Há aqui uma modificação no sentido de vigilância, que passa da sociedade disciplinar à sociedade de controle. Na primeira, a ideia de vigilância remetia ao confinamento e, portanto, à situação física que caracterizava as preocupações dessa sociedade. O problema era o movimento físico dos indivíduos, seu deslocamento espacial. Vigiar era, basicamente, regular os passos das pessoas, era olhar. Com a explosão das comunicações, uma nova figura ganha força: a vigilância das mensagens, do trânsito de comunicações […] Vigiar passou a significar, sobretudo, interceptar, ouvir, interpretar […] O que parece interessar, acima de tudo, é como cada um se movimenta no espaço informacional. O modo como nos deslocamos por entre informações revela muito do como pensamos.

Na mesma linha, Santos (2003, p. 136) argumenta que essa nova forma de vigilância, mais "sutil e perversa"...

> … prescinde da instalação de câmeras no ciberespaço domiciliar e até mesmo do consentimento do vigiado que se encontra superexposto. Trata-se do cruzamento e processamento de dados que cada um de nós gera ao entrar,

> sair e transitar nos diversos sistemas informatizados e nas diversas redes que compõem a vida social contemporânea.

Esse movimento no espaço informacional – por natureza, altamente controlado – gera padrões de comportamento de todos os cibercidadãos. Mas o controle por meio das redes digitais apenas não é exercido no nível dos rastros de navegação e do bloqueio aos conteúdos. Ele se manifesta também (ou, acima de tudo) na infraestrutura lógica da rede.

Tendo isso em vista, Silveira considera a Internet como a maior expressão da sociedade de controle, de forma que esta representa uma nova "biopolítica da modulação": para o autor, tanto a grande rede como as tecnologias digitais desempenham o papel de modular a espécie na vida social, "em um cenário de múltiplas ambivalências que constituem as sociedades em rede" (2012, p. 112). Indo além das tecnologias disciplinares, a nova biopolítica traz outros elementos regulamentadores.

Nesse sentido, Silveira destaca e classifica os principais tipos de controle nas sociedades informacionais: além dos rastros de navegação e do controle de acesso, aponta os os formatos, as linguagens de programação e os protocolos.

Formatos dizem respeito ao modo como as informações são armazenadas e, portanto, como serão acessadas e modificadas no futuro – com isso, também dizem respeito à memória cibernética. A existência de um formato proprietário implica que só se poderá acessar as informações digitais por ele protegidas caso o software responsável por fazê-lo saiba as especificações contidas nesse formato. Como tais especificações, em um formato proprietário, não são amplamente conhecidas, a forma como as informações nele contidas serão acessadas dependerá unicamente da vontade dos desenvolvedores desse formato. Em última instância, isso representa uma forma absoluta de controle sobre certas informações.

O ciberespaço é dependente de linguagens de programação, que são a matéria-prima para a construção dos softwares. Sem estes, em uma sociedade informacional, é cada vez mais difícil criar e acessar conhecimento. A forma como um programa de computador é arquitetado pode, perfeitamente, limitar os processos de comunicação, controlando-os, impedindo-os de serem usados para uma ou outra finalidade. É por isso que, na sociedade informacional, "o software assume o comando", conforme apontou Manovich (2008, p. 7), referindo-se aos programas de computador como uma "uma camada que permeia todas as áreas da sociedade contemporânea".

Por fim, os protocolos, que são decisivos para o argumento central deste trabalho, são

os grandes responsáveis por controlar a comunicação em rede e as arquiteturas da informação. Eles "definem como uma rede deve receber um dado, utilizá-lo e enviá-lo. Podem ampliar ou restringir nosso modo de comunicação em rede" (SILVEIRA, 2012, p. 116).

O teórico norte-americano Alexander Galloway (2004) classifica o protocolo como um elemento decisivo da sociedade de controle deleuziana (para além disso, o protocolo é seu "tipo de administração"). Seguindo os autores já discutidos nessa seção, Galloway argumenta que nossas sociedades estão imersas em um novo aparato de controle – ou melhor, em um novo diagrama de poder. O diagrama em questão são as redes distribuídas; a tecnologia que o permeia, o computador; e o tipo de administração que rege esse cenário, controlando-o à exaustão, é o protocolo.

Por implementar um estilo de comando difuso, distribuído e sob o formato de rede, Galloway se propõe a analisar o protocolo (e o diagrama da distribuição) para explicar a lógica sociopolítica de nossa era. 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" – um 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, p. 7).

De maneira geral, o sistema de gestão dominado por protocolos permite que exista um alto grau de controle em um ambiente bastante heterogêneo. Galloway 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).

Em seu livro *Protocol*, o autor 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. Mas, antes disso, a própria existência do protocolo já representa uma forma expressa e totalizante de controle. Por exemplo, só existe a possibilidade de um indivíduo navegar na Internet caso aceite compactuar com um de seus principais protocolos, o conjunto TCP/IP (*Transmition* ***Control*** *Protocol/Internet Protocol*). Outras funções básicas, por sua vez, demandam novos protocolos, que também exigem ampla e restrita aceitação.

Em uma analogia deveras elucidativa, Galloway exemplifica o controle "protocológico" por meio da resolução de um problema de excesso de velocidade em

determinada rua. Em vez de instalar radares fotográficos, seria muito mais eficiente, do ponto de vista do protocolo, implantar lombadas nessa via. Ao contrário dos radares, as lombadas modulam a fundo o comportamento dos usuários do local (assim como protocolos de rede modulam o comportamento de quem trafega pela infovia). É inevitável: diferentemente dos radares, que inibem, mas não impossibilitam o tráfego em alta velocidade, com as lombadas, caso os motoristas insistam em dirigir velozmente, simplesmente se acidentarão e danificarão seus veículos. O protocolo, nesse sentido, é como a gravidade: aqueles que quiserem investir contra ele terão pouco ou nenhum sucesso.

Assim sendo, se é inútil lutar contra o protocolo, como seria possível realizar uma resistência minimamente eficaz a essa sofisticada forma de controle? "Não cabe temer ou esperar, mas buscar novas armas", apontou-nos Deleuze (1992, p. 224). Nas seções que se seguem, será apresentada uma das formas mais crescentes e proeminentes de enfrentar o controle na sociedade contemporânea.

2.3 RESISTÊNCIA E ATIVISMO HACKER

Para Silveira (2012), as sociedades disciplinares, aliadas ao capitalismo em seu estágio industrial, implementaram formas bastante estagnadas – embora descentralizadas – de controle. Em contrapartida, surgiram focos de resistência como sindicatos, associações de indivíduos, partidos políticos etc. Se, por um lado, um meio de confinamento como a fábrica constituía os indivíduos em um só corpo, tendo a vantagem de se negociar com e vigiar uma única massa de modo geral, a resistência sindical aproveitou-se disso para mobilizar uma massa conjunta para realizar os embates junto ao patronato.

Em uma etapa posterior, o capitalismo cognitivo – também chamado de informacional, tardio, imaterial, pós-industrial etc. – implementou, nas sociedades de controle, formas de controle distribuídas, difusas, em rede. Logo, conforme observou o grupo de artistas ativistas Critical Art Ensemble (2001), as táticas políticas de resistência devem se adequar a este novo cenário para que não incorram no anacronismo. Da mesma maneira, Alexander Galloway (2004) defende que, nesse novo diagrama de poder, a resistência passa, necessariamente, pelo engajamento com formas distribuídas de administração protocológica. "Eu sugiro que viver

na era do protocolo requer táticas políticas projetadas de dentro da esfera do protocolo", afirma Galloway (2004, p. 151).

> … 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 (Idem, p. 160).

Entre essas táticas, Silveira (2012, p. 110) destaca três delas – duas pontualmente e uma de forma genérica:

> A voracidade do capitalismo cognitivo aplainou o terreno para o surgimento de inúmeras conformações de resistência, entre as quais o ativismo hacker, as práticas de compartilhamento de bens imateriais e diversas manifestações culturais e étnicas disseminadas nas redes distribuídas.

O ativismo hacker, enquanto forma de resistência política nas sociedades de controle, é capaz de empregar as mais variadas táticas para, de acordo com Deleuze (1992) – sem se referir ao hacktivismo, evidentemente –, "iludir o controle". Para discutir esse ponto, tomar-se-ão como exemplo as formas de controle acima descritas por Silveira: rastros de navegação, acesso, formatos, linguagens de programação e protocolos.

Os hacker são capazes, de forma muito simples e rápida, de ocultar e embaralhar seus dados de navegação. Além de isso os tornar imunes a essa forma de controle, é capaz de causar prejuízos às empresas que se dedicam a coletar, organizar e analisar esses dados, mapeando o comportamento dos internautas. Isso é ainda mais pernicioso ao controle imposto pelo capital à medida que grupos de hacktivistas – majoritariamente identificados com o movimento cypherpunk – experts em criptografia programam aplicações que permitem aos internautas sem conhecimento técnico fazerem o mesmo (apagar e embaralhar seus dados de navegação). Talvez a mais conhecida aplicação nesse sentido seja o projeto Tor – anonimato online.[13]

Em relação ao acesso às informações, o hacking politicamente motivado também se mostrou uma arma ameaçadora a corporações e governos espalhados por todo o mundo. Parte dos dados divulgados pela organização internacional Wikileaks foram obtidos dessa forma.

13 Cf. <www.torproject.org>. Acesso em 19 set. 2012.

Um dos grupos mais marcantes nesse aspecto é o *Cult of the Dead Cow* (cDc), que, ao final dos anos 1990, associou-se a dissidentes chineses para colaborar com técnicas de criptografia a fim de construir aplicações que furassem o bloqueio implementado pelo governo chinês na Internet. Conforme observaremos na seção seguinte, o acesso amplo e irrestrito à informação é um dos preceitos intocáveis da chamada ética hacker, de forma que quaisquer mecanismos elaborados com essa finalidade são extremamente bem-vindos.

Formatos – sobretudo os proprietários – também são objetos de grande preocupação da comunidade hacktivista em todo o mundo. Nesta área, o empenho dos hackers tem sido principalmente o de empregar técnicas de engenharia reversa para se obter acesso às informações protegidas pelos formatos em questão. É dessa forma, por exemplo, que documentos protegidos pelos formatos padrão de um dos pacotes de escritório mais utilizados no mundo – o *Office*, da Microsoft – podem ser acessados por pacotes que se valem unicamente de softwares livres, como é o caso do LibreOffice. Vários embates já foram travados no campo dos formatos e, invariavelmente, os hackers são atores mais que relevantes nessas disputas.

A linguagem de programação, por sua vez, é como um língua materna para os hackers. Se, por um lado, ela condiciona a comunicação, limitando-a e modulando a forma como é praticada, por outro, ela emancipa aqueles que a conhecem e sabem manejá-la. Nesse sentido, na sociedade de controle permeada por redes digitais de comunicação, os hackers são decisivos à medida que dominam a arte de manipular os códigos presentes nessas redes. Para Galloway (2004, p. 167), "a relação estreita que os hackers têm com os códigos expõe o poder do protocolo, particularmente sua habilidade de incitar atores autônomos em direção a um estado mais vital ou afetivo dentro de seu meio particularmente distribuído".

Chega-se, portanto, ao protocolo. Conforme observamos, é sumariamente inútil fazer uma resistência *strictu sensu* aos protocolos de controle, uma vez que, fora deles, pouco ou nada se pode fazer. Neste caso, portanto, "resistência" não pode nem deve significar "recusa" ou "abstenção". Ainda seguindo Galloway, a maneira mais eficiente de resistir a um protocolo de controle deve-se dar *por meio* deste protocolo, e não *fora* dele. Nesse sentido, o hacking de computador representa uma alteração na própria natureza da resistência, pois os hackers não ignoram ou desejam a morte do protocolo, mas, em vez disso, são os arautos das principais possibilidades apresentadas por ele. "São atores protocológicos por excelência", diz Galloway (Idem, p. 158).

Portanto, hackers ativistas sabem que resistir ao protocolo não significa recusar as tecnologias digitais, mas redirecionar essas tecnologias a outros propósitos, ou "hackear" essas tecnologias. Resistir de forma apropriada ao protocolo significa levá-lo a um grau de máxima saturação, ou "hipertrofia", para citar termo empregado por Galloway. Com isso, o hacktivismo remaneja o protocolo para um novo sentido, sempre motivado por causas políticas.

A fim de explorar como isso ocorre, em parte, na prática, o próximo capítulo se foca no estudo descritivo da rede hacktivista Anonymous. Antes, porém, para tentar compreender esse fenômeno e buscar novos exemplos, faz-se importante abordar algumas das principais perspectivas teóricas que lançam interpretações sobre o fenômeno do hacktivismo na literatura acadêmica.

2.4 HACKTIVISMO: PERSPECTIVAS TEÓRICAS

Pode-se dizer que o fenômeno do hacktivismo, embora um tanto recente, já foi estudado com propriedade por pesquisadores oriundos das mais diversas áreas do conhecimento. Em um panorama geral, observa-se que a literatura concernente a ele se desdobra em contribuições, no mínimo, da sociologia, antropologia, comunicação, direito, filosofia, engenharia e estudos de segurança da informação.

Tomando o devido cuidado para não incorrer em uma sistematização grosseira, identificaram-se, nesses estudos, três principais perspectivas teóricas que buscam interpretar o hacktivismo à luz de preceitos relativamente familiares às respectivas áreas de estudo. Neste trabalho, a fim de melhor organizar essas perspectivas, identificá-las-emos como (1) desobediência civil eletrônica, (2) guerra da informação e (3) hacktivismo por ele mesmo.

A primeira perspectiva vê o hacktivismo no contexto da desobediência civil eletrônica e tende a valorizar (ou ao menos a levar em conta) os aspectos sociais, culturais e políticos que estão no cerne da cultura hacker. Nesses estudos, encontrados abundantemente na literatura acadêmica, percebe-se a disposição dos pesquisadores em ver as ações hacktivistas como formas de ação política direta ou de protesto político. Rechaçam-se, aqui, as interpretações que tendem a criminalizar o hacking e o hacktivismo, associando-os ao

terrorismo cibernético. Para além de relatos sobre atos hacktivistas, da cobertura midiática e de livros, artigos e manifestos elaborados pelos próprios hacktivistas, pesquisadores desta perspectiva conferem especial atenção ao diálogo direto com os próprios hackers por meio de entrevistas a fim de melhor apreender suas motivações, seus métodos, sua ética de ação etc. Pelo fato de este trabalho pretender contribuir, embora infimamente – com essa perspectiva, é a ela que será conferida maior atenção.

A segunda perspectiva teórica, por sua vez, tende a posicionar hacktivismo no contexto da segurança computacional, da guerra informacional e do ciberterrorismo. Trata-se de uma abordagem que, conforme concluiu Sandor Vegh (2003), ganhou eco e apoio em boa parte da imprensa estadunidense, sobretudo após os atentados terroristas às torres gêmeas do World Trade Center, em setembro de 2001. Na academia, esse pensamento foi preconizado pelo trabalho da pesquisadora Dorothy Denning (2000, 2001) e dos amplamente discutidos pesquisadores da RAND Corporation David Ronfeldt and John Arquilla. Diante da primeira perspectiva teórica, essa abordagem concentrada apenas na segurança da informação se mostra demasiadamente limitada (e, por vezes, reducionista), pois desconsidera os aspectos sociais e políticos do hacktivismo ao conferir maior relevância apenas aos aspectos técnicos e legais relacionados a esse fenômeno.

Por fim, a terceira perspectiva teórica é aquela formulada pelos próprios ativistas. Nesses trabalhos, preconizados pelo coletivo de artistas ativistas Critical Art Ensemble e seguido por diversos indivíduos e grupos hacktivistas em todo o mundo, observa-se uma tentativa de elaborar bases teóricas para compreender o lugar do hacktivismo e da resistência em face a uma nova configuração do poder.

Feita esta breve introdução, passemos a alguns dos autores que compõem cada uma dessas perspectivas.

2.4.1 Desobediência civil eletrônica

Um dos estudos atuais mais abrangentes quanto ao ativismo hacker sob a perspectiva da desobediência civil eletrônica é assinado pela pesquisadora estadunidense Alexandra Samuel. Em sua tese de doutorado em Ciência Política, defendida no Departamento de

Governo da Universidade Harvard e intitulada *Hacktivism and the future of political particiption*, Samuel (2004) define o hacktivismo como o casamento entre o ativismo político e o hacking de computador, fazendo um uso não-violento e legalmente ambíguo de ferramentas digitais[14] para se alcançar fins políticos.

Ao afirmar que as ações hacktivistas não são violentas, Samuel as diferencia claramente das formas de ciberterrorismo, cujo objetivo central é levar ameaças reais a vidas de seres humanos ou a estruturas físicas computacionais. Ao dizer que são legalmente ambíguas, a pesquisadora também as diferencia de um simples ativismo on-line – como, por exemplo, disseminação de informações, publicação de cartas-protesto, envio em massa de e-mails, blogagem coletiva –, que raramente envolve as habilidades presentes no hacking de computador.

Dessa maneira, segundo Samuel, o hacktivismo não é um ativismo on-line qualquer por motivos (1) táticos: os hacktivistas adotam ferramentas e estratégias mais diretas e transgressivas do que as utilizadas no ativismo comum; (2) culturais: para os hacktivistas, o online torna-se mais poderoso frente às manifestações do offline; e (3) de princípios: hacktivistas não são ciberterroristas, pois respeitam, acima de qualquer coisa, a proteção à vida humana.

Segundo a pesquisadora, o hacktivismo tem suas origens, por um lado, no universo hacker e, por outro, no cenário artístico-ativista, de quem ele ainda hoje carrega profundas influências. A fim de desvendar as diversas facetas desse fenômeno em sua forma atual, formulando uma complexa taxonomia do hacktivismo, Samuel realizou 51 entrevistas com ativistas hackers de várias partes do mundo, além de analisar um conjunto de materiais de fonte primária e secundária.[15] Por fim, a pesquisadora aplicou essa taxonomia a três assuntos relacionados à participação política: democracia deliberativa, autonomia do Estado e ação coletiva.

Mas o que verdadeiramente nos interessa neste trabalho é esse detalhado conjunto de classificações acerca do hacktivismo. De maneira geral, são identificadas pela autora três de vertentes: (1) cracking político, envolvendo ações claramente ilícitas; (2) hacktivismo de performance, praticado por hacktivistas oriundos do mundo artístico-ativista e diz respeito a ações legalmente nebulosas, como paródias de sites e manifestações virtuais; e a (3)

14 Entre as várias ferramentas digitais listadas pela pesquisadora, estão: deformação de sites, redirecionamentos, negação de serviço, roubo de informações, paródia de sites, manifestações virtuais, sabotagens virtuais e desenvolvimento de softwares.

15 Trata-se do primeiro grande estudo empírico relacionado ao hacktivismo de que se tem notícia.

codificação política, isto é, o desenvolvimento de softwares com finalidade política.

Sobre essas três vertentes, encaixam-se as seguintes classificações:

• Desfiguração de sites: ocorre quando hacktivistas substituem uma página por outra contendo algum tipo de mensagem de cunho político. Geralmente, trata-se de uma crítica ao governo, empresa ou organização que administra o site em questão. Trata-se de uma das formas mais comuns de hacktivismo;

• Redirecionamento de sites: consiste em entrar em um servidor e alterar o endereço de determinado site, de tal sorte que seus visitantes sejam redirecionados a um site alternativo, que geralmente contém uma crítica ao site original;

• Ação de negação de serviço: nesse tipo de ação, o servidor para de prestar serviço aos usuários, pois deixa de ter conectividade. Nesses atos, os hacktivistas não pretendem ganhar acesso aos sistemas-alvo, mas apenas anular o trabalho de seus servidores. Para isso, podem ser usados computadores zumbis a fim de ajudar a sobrecarregar tais servidores;

• Roubo de informações: ocorre quando pessoas entram em uma rede privada e roubam informações sigilosas. Quando essa ação é publicizada, tem por objetivo constranger os administradores desse sistema quanto à falha de segurança ou protestar contra alguma conduta adotada por eles;

• Sabotagem virtual: atividades com objetivo de manipular ou prejudicar tecnologias de determinados alvos, podendo destruir dados pessoais ou equipamentos. Exemplos de sabotagens virtuais, para Samuel, são os vírus;

• Manifestações virtuais: ocorrem quando milhares de ativistas atualizam as páginas dos servidores-alvos, sobrecarregando-os até que fiquem muito lentos ou simplesmente parem. Neste caso, o sucesso depende do grande volume de participantes, o que, para Samuel, o diferencia da ação de negação de serviço;

• Paródias: quando uma página é imitada em sua aparência, e sua geralmente URL é é muito parecida à da página-alvo;

• Desenvolvimento de software: ocorre quando hackers programam softwares com propósitos políticos – por exemplo, os embaralhadores de IPs, que ajudam internautas a manterem seu anonimato na Internet e, com isso, acessar sites proibidos por governos que censuram a rede em seus países.

Tendo por base a perspectiva formulada por Galloway (2004), pode-se dizer que todas essas estratégias de ação configuram-se como formas de resistência à medida que iludem o

controle dos protocolos. Conforme verificaremos, os Anonymous utilizam com frequência algumas dessas estratégias.

*****

De maneira mais ampla, é possível dizer que o trabalho do húngaro radicado nos Estados Unidos Sandor Vegh – *Hacking for democracy: a study of the internet as a political force and its representation in the mainstream media* (2003) – busca tratar do impacto da Internet na democracia, além da luta de poder entre controle e resistência no ciberespaço. Mas seu foco de estudo diz respeito ao hacktivismo e ao papel político frequentemente exercido pelos meios de comunicação de massa ao retratá-lo.

Vegh argumenta que o controle sobre a mídia é fundamental e decisivo para a manutenção da hegemonia das elites políticas e econômicas, uma vez que permite a elas reprimir à sua maneira quaisquer narrativas alternativas de protesto e resistência – como, por exemplo, aquelas que são elaboradas, assumidas e propagadas pelos hacktivistas. O autor acredita que o hacking pode atingir o coração do atual sistema capitalista na medida em que "os dois maiores medos das corporações são perdas de rendimentos e deterioração da imagem pública, exatamente o que um ataque hacker pode fazer ao derrubar servidores ou expor informações" (2003, p. 153).

Portanto, segundo Vegh, esse controle exercido pelas elites sobre os meios de comunicação de massa faz com que estes naturalmente enviesem sua representação sobre as mais diversas atividades contra-hegemônicas, assumindo assim uma perspectiva favorável à manutenção do seu *status quo*. Dessa maneira, o autor se propõe a examinar a cobertura realizada pela mídia de massa quanto ao uso político da internet por parte dos hacktivistas, dada a capacidade que essa mídia inevitavelmente ainda tem ao influenciar a opinião pública e, portanto, a elaboração de diretrizes políticas.

Depois de fazer uma ampla análise da cobertura midiática realizada pelos cinco maiores jornais dos Estados Unidos durante um ano e meio – incluindo-se, neste período, os atentados cometidos contra as torres gêmeas do World Trade Center, em setembro de 2001 –, Sandor Vegh conclui que a elite econômica interpreta o hacking e o hacktivismo como uma atividade antissocial e criminosa. Essa visão extremamente negativa e obscura quanto aos hackers, defende o autor, é parte de uma estratégia midiática consciente cujo objetivo

explícito é ganhar apoio do público a fim de instar as autoridades a exercer um controle cada vez maior sobre a Internet – uma forma de limitar seu potencial como ferramenta de ação política de resistência. Trata-se de um jogo destinado a formar um consenso público no sentido de erradicar o hacking, uma atividade que pode, ao menos potencialmente, ameaçar a ordem dominante.

O autor também conclui que, após os atentados terroristas de setembro de 2001, esse discurso midiático sofreu alterações para pior, de modo que os hackers, que eram frequentemente apresentados como criminosos comuns, passaram a ser retratados como ciberterroristas em relatos cada vez mais sensacionalistas. Isso, por certo, influenciou de forma negativa qualquer ativismo político online, que agora precisa, antes de tudo, se defender contra o fato de ser rotulado como uma forma de ciberterrorismo.

Para Vegh, essa perspectiva, por conta de sua interpretação limitada, pouco ajuda a compreender de fato o fenômeno do hacktivismo, que deveria ser apreendido como uma questão social inserida na estrutura de uma luta dinâmica e constante de controle e resistência entre os grupos que detêm o poder e os que não o detêm.

Com isso, ao classificar o hacktivismo como uma questão social, o autor pode ser inserido entre aqueles que entendem esse fenômeno como um ato de desobediência civil, uma forma legítima de resistência. A própria definição de hacktivismo apresentada pelo autor – por sinal, bastante abrangente – nos permite confirmá-lo:

> Hacktivismo é uma ação online politicamente motivada, ou uma campanha de ações, realizada(s) por atores não-estatais em retaliação para expressar desaprovação ou para chamar a atenção a uma questão defendida pelos ativistas [...] hacktivistas são tanto "ativistas cabeados", ou seja, ativistas que adaptam a Internet às suas estratégias, ou "hackers politizados", ou hackers *per se* que agora adotam causas políticas como justificativa para suas ações (2003, p. 167).

Em síntese, o hacktivismo, como forma de resistência on-line, é parte de uma luta constante na qual o controle é decidido. E a mídia, por sua vez, desempenha um papel crucial nesse cenário. Embora as conclusões e ressalvas do autor – sobretudo em relação a essa postura exercida pela mídia – se apliquem exclusivamente a um contexto específico (o estadunidense) por conta do escopo de sua análise, elas nos chamam a atenção para um aspecto por vezes desconsiderado nos estudos sobre o hacktivismo. E, de forma irrefutável, tal análise parece mais atual do que nunca, a julgar pelos incansáveis esforços impetrados por

governos e empresas dos Estados Unidos e Europa em uma guerra insana e declarada contra a "violação dos direitos de propriedade intelectual".

Por fim, essa outra visão sobre o ativismo hacker, que constantemente o associa ao ciberterrotismo e que é alvo de críticas neste trabalho de Vegh, tem também sua representação na literatura acadêmica, conforme constataremos na próxima perspectiva teórica.

*****

Outra obra indispensável relacionada ao hacktivismo é aquela desenvolvida pelos pesquisadores britânicos Tim Jordan e Paul A. Taylor (2004). Em *Hacktivism and cyberwars: rebels with a cause?*, os autores continuam sua investigação sobre o ativismo hacker e sua origem, suas motivações, suas formas de ação, disputas internas etc. Para tanto, diferentemente de Sandor Vegh (2003), que fundamentou sua pesquisa na cobertura midiática acerca da questão, Jordan e Taylor valem-se – além de uma minuciosa revisão bibliográfica relativa à história do hacking – de manifestos, periódicos, entrevistas e relatos elaborados por ou feitos com os próprios hackers.

Decisivamente, os autores classificam o hacktivismo em termos de desobediência civil eletrônica e de novos movimentos sociais. E, para defenderem essa posição, apresentam uma detalhada história da evolução do hacktivismo, iniciando pelos raízes da cultura adotada pela primeira geração de hackers.

De acordo com sua definição, hacktivismo é...

> … a emergência da ação política popular, da autoatividade de grupos de pessoas, no ciberespaço. Ele é uma combinação protesto político de pessoas comuns com o hacking. Os hacktivistas operam dentro da estrutura do ciberespaço, lutando sobre o que é tecnologicamente possível em vidas virtuais, e alcançam o ciberespaço utilizando poderes virtuais para moldar a vida offline. Movimentos sociais e protestos populares são partes integrais das sociedades do século XXI. O hacktivismo é ativismo que se tornou eletrônico (2004, p. 1).

Em suma, trata-se de um fenômeno social e cultural, uma nova geografia de poder, em que as políticas de ação direta foram transportadas para o virtual. Sua origem, segundo os autores, está na intersecção de três correntes divergentes: (1) o hacking, (2) as sociedades informacionais e as (3) formas modernas de resistência e protesto social, sobretudo os

protestos contra a globalização de cunho neoliberal. Em função do escopo deste trabalho, dedicaremos atenção à primeira corrente.

Jordan e Taylor argumentam que os hackers, incluindo os ativistas, não existem fora de sua relação com seus pares, que, juntos, formam as comunidades hackers. Desde os anos 1950, essas comunidades passaram por mudanças deveras significativas, de modo que os autores identificam seis comunidades distintas – embora, em muitos aspectos, coincidentes – que, além de marcarem estágios históricos no desenvolvimento do hacking, são precursoras do hacktivismo e do uso explícito do "hack" para fins políticos. Evidentemente, trata-se de uma sistematização possível, mas não rigorosamente perfeita, de tal sorte que é provável, por exemplo, encontrar hackers que, mesmo fazendo parte de comunidades/gerações distintas, compartilhem determinadas características.

A primeira onda de hackers, apontam os autores, é constituída por três comunidades, sendo que a primeira diz respeito aos (1) "hackers originais", os pioneiros a emergir nos primórdios da computação. Foram eles que experimentaram as capacidades das grandes estruturas computacionais que havia em universidades como o MIT (Massachusetts Institute of Technology) durante as décadas de 1950 e 1960. Em seguida, estão os (2) hackers de hardware e os (3) hackers de software. Enquanto os primeiros foram os inovadores que, no início dos anos 1970, tiveram um papel crucial na formulação do computador pessoal e, com isso, disseminaram e democratizaram o acesso a essas máquinas, os últimos inovaram na criação e reformulação de programas úteis a elas. Essas três primeiras comunidades (cuja sistematização é profundamente influenciada pelo trabalho de Levy (2010), segundo Jordan e Taylor, formam o que seria a primeira geração de hackers, que seria seguida, imediatamente, por outras formas de hacking.

A quarta comunidade, por sua vez, seria representada pela dualidade (4) hacker/cracker, termos usados desde a metade dos anos 1980 para descrever pessoas que invadiam sistemas de computadores, mas nem sempre por razões maliciosas. Enquanto "hacker tende a ser usado por aqueles que estão fora do *underground* computacional, particularmente os *mass media*", dizem os autores, "cracker é usado por aqueles que estão imersos nos grupos de tecnologia, em uma tentativa de salvar o termo hacker" (2004, p. 11).

Já em meados da década de 1990, surgiram (5) Microserfs,[16] programadores que, ao mesmo tempo que carregavam consigo vários atributos da cultura hacker, foram cooptados

16 O termo é uma junção das palavras "Microsoft" e "serf" (em inglês, servo): ou seja, o servo de empresas como Microsoft.

pela estrutura de grandes corporações de tecnologia, tais como a Microsoft. E, por fim, vieram os hackers da comunidade (6) *open source*, com a responsabilidade de criar o melhor software software possível de forma colaborativa, contando com a ajuda dos pares ao escrever, modificar e utilizar os programas de computador.

Jordan e Taylor (2004) argumentam que a mistura de todas essas gerações e comunidades culminaram, em meados dos anos 1990, com a mistura de uma atividade hacker com um propósito político claro. A primeira geração teria influenciado o hacktivismo com suas motivações políticas voltadas à irrestrita liberdade de informação e ao desejo de universalizar o acesso aos computadores. Da mesma forma, os valores anticorporativistas, que também tiveram origem na primeira geração, estendendo-se às seguintes, deram o tom contrário ao *stablishment* e à autoridade, frequentemente encontrado nos hacktivistas. O movimento *open source*, por sua vez, também era dotado de um cunho político extremamente relevante, mas "frequentemente escondido sob as linhas de código" (2004, p. 16). Simultaneamente a este movimento, os hacktivistas surgiram com ações políticas abertas, declaradas, usando computadores para ações diretas – o que os torna, inevitavelmente, uma comunidade distinta. Portanto, o hacktivismo, segundo Jordan e Taylor, tem suas raízes em um turbilhão de correntes do hacking.

Assim como sua origem, as formas de ação adotadas pelos hacktivistas e identificadas pelos autores podem ser coincidentes, mas, a fim de estudo, são divididas entre (1) hacktivismo de ação em massa (*mass action hacktivism*, comparável ao "hacktivismo de performance", tal como formulado por Alexandra Samuel) e (2) hacktivismo digitalmente correto (*digitally correct activism*, comparável ao que Samuel chamou de codificação para fins políticos). O primeiro é caracterizado pela invenção da desobediência civil eletrônica, que leva ao campo virtual todas aquelas formas tradicionais de protesto. Essa forma de hacktivismo, segundo os autores, relaciona-se intimamente ao movimento antiglobalização, à teia de luta em torno do movimento zapatista, no México, e às manifestações contra a Organização Mundial do Comércio. Aqui se situam, por exemplo, as ações de negação de serviço (ou DDoS, *Distributed Denial os Service*), método comumente usado pelos Anonymous.

A segunda forma, hacktivismo digitalmente correto, é atribuída a hackers que radicalizam os preceitos da primeira comunidade hacker – os da liberdade de e acesso a todo tipo e qualquer de informação. Para tanto, esses hackers dedicam-se a criar e aprimorar

ferramentas que assegurem (ou ao menos caminhe para isso) que o ciberespaço seja um lugar no qual os fluxos informacionais corram livremente. Suas preocupações são geralmente com empresas ou governos que agem no sentido contrário a esse – ou seja, limitando o acesso à informação. Entre as ações que fazem parte dessa segunda forma de hacktivismo está, por exemplo, a codificação de softwares que têm como objetivo transpor bloqueios implementados por certos países a seus cidadãos, que não conseguem acessar, geralmente por motivos políticos ou religiosos, determinados sites.

Em comum, essas formas de hacktivismo têm a característica de representar formas modernas de resistência social. Para Jordan e Taylor, à medida que nossas sociedades se caracterizam por uma crescente desmaterialização da vida social e cultural por meio da mercantilização de nossos espaços íntimos e imateriais, o hacktivismo representa a politização de um domínio hacker quanto às tecnologias do espaço imaterial (2004, p. 171). Isso significa que o hacktivismo gera abstrações que combatem abstrações: se, por um lado, vidas são mercantilizadas em um espaço imaterial abstrato, as ações de desobediência civil eletrônica contam com corpos abstratos para agir, mesmo que respaldados por uma presença física. Ao passo que se criam novas formas de tecnologia, mais os hackers são capazes de propagar meios de produção virtual, aprimorando suas abstrações e, por conseguinte, sua resistência. Por conta disso, para os autores, os "hacktivistas são o primeiro movimento social da virtualidade" (2004, p. 172).

*****

Mark Manion e Abby Goodrum (2000), em *Terrorism or civil disobedience: toward a hacktivistic ethic*, seguem na tradição de posicionar o hacktivismo no campo da desobediência civil. Os autores narram várias ações hacktivistas para argumentar que esses atores representam, na verdade, uma nova "espécie de hacker": aquele que é claramente motivado por preocupações éticas e que acredita seus atos devem ser considerados um uma forma legítima de desobediência civil.

Ao investigar essa forma de desobediência, Manion e Goodrum traçam princípios básicos que formam, ao mesmo tempo, as condições necessárias e a justificação ética para atos do gênero. Assim, na visão dos autores, se determinada ação (1) não causar dano a

pessoas ou propriedades; (2) não for violenta; (3) não for desempenhada visando ao lucro pessoal; (4) tiver uma motivação ética, isto é, a convicção de que a lei, norma ou conduta contra a qual se protesta é injusta; e (5) tiver, por parte dos agentes, uma vontade de assumir as responsabilidades pessoais para eventuais consequências, essa ação pode ser considerada uma forma de desobediência civil eletrônica.

Ou seja, é preciso que haja justificativa moral por trás de ações dos hacktivistas. Esse quadro já exclui do espectro do hacktivismo, sem qualquer possibilidade de dúvidas, o trabalho de hackers curiosos que, mesmo com habilidades avançadas, realizam ações no ciberespaço apenas em nome do desafio técnico; ou também o trabalho de pessoas que, mesmo sem tanto conhecimento técnico, quebram sistemas para lucro pessoal, vandalismo ("crackers", segundo os autores) ou com a intenção de causar danos como destruição de infraestruturas ou ameaça a vidas ("ciberterroristas").

Essa distinção entre o que pode ser tratado com desobediência civil ou não é crucial para o debate entre as duas primeiras perspectivas teóricas tratadas neste trabalho. Isso porque "se o hacktivismo pode ser definido como um ato de desobediência civil eletrônica, então as consequências punitivas devem ser alinhadas às outras formas de desobediência civil", apontam Mark Manion e Abby Goodrum (2000, p. 16). No entanto, os autores também observam que, na maior parte dos casos, os atos de hacktivismo têm sido tratados de forma igual a ações claramente ligadas à guerra da informação e ao terrorismo – que, por sua vez, são rechaçadas por hacktivistas.

Diante disso, por que, cada vez mais, governos, empresas e analistas de segurança da informação se recusam a fazer a distinção entre (hack)ativismo e (ciber)terrorismo? Segundo Manion e Goodrum (Op. cit., p. 17):

> Pode ser que, descrevendo hacktivistas como criminosos, ajude a fortificar uma certa concepção de, e controle sobre, propriedade intelectual, obscurecendo a crítica mais ampla sobre controle da informação, e da necessidade dos sistemas legais de proteger os poderosos interesses econômicos das corporações que tentam dominar e comercializar completamente a Internet. Mais do que isso, classificando os hacktivistas como uma ameaça à segurança nacional fornece maiores legitimações para entregar a privacidade individual nas mãos dos Estado de Segurança Nacional, que compila e armazena vastos bancos de dados de centenas de milhares cidadãos a cada ano.

Enfim, seguindo Vegh (2003), os autores observam que o ativismo hacker, seu modo

de ação e sua ética fatalmente entram em choque com o complexo comercial-financeiro-industrial que deseja controlar a Internet. Se, por um lado, em toda a história do ativismo político, as táticas de resistência nunca tiveram à sua disposição o conjunto potencialmente infinito de possibilidades existentes nas redes de comunicação interconectadas, isso pouco ajuda se o direito de protestar legitimamente, valendo-se de formas de desobediência civil eletrônica, é solapado e criminalizado.

*****

No Brasil, apesar de diversos pesquisadores já terem se debruçado sobre a ética e a cultura hackers – como Malini (2009), Lemos (2002) e outros –, há poucos trabalhos que tratem propriamente do hacktivismo como forma de resistência política.

Um desses trabalhos é *Ciberativismo, cultura hacker e o individualismo colaborativo*, de Sergio Amadeu da Silveira (2010), para quem o hacktivismo agigantou-se nos primeiros dez anos deste século e tem variado em suas formas de ação – que, além de seus modos tradicionais, vão desde atos em favor da maior transparência nos dados públicos até mesmo a elaboração de *machinimas* políticos.[17] Depois de realizar uma extensa revisão bibliográfica contemplando autores e ativistas alinhados a esta perspectiva da desobediência civil eletrônica, o pesquisador conclui que, no pensamento hacker, pode-se encontrar uma forte influência liberal na defesa das liberdades básicas dos indivíduos – como acesso livre à informação, direito à privacidade, à liberdade de expressão etc. Essa defesa, por sua vez, dá origem às diversas formas de ativismo que relatamos até então.

Além disso, no ideário hacker, incentiva-se a emancipação individual pelo conhecimento – "tudo indica que um pensamento típico-ideal do hackerismo passa por considerar que o custo da liberdade é o conhecimento. [Por exemplo,] ninguém pode ser autônomo em uma rede lógica se não sabe quem está no controle e o que estão fazendo com o seu computador" (2010, p. 38). Nesse sentido, observa o autor, os hackers também são dotados de um comportamento absolutamente meritocrático, de forma que são mais reconhecidos à medida que mais se dedicam pela comunidade. A cada vez que enfrentam desafios diante dos códigos e estes são solucionados, os resultados devem ser informados a todos – afinal, o conhecimento deve ser livre para que outros indivíduos também se

17 Machinima é a combinação das palavras "machine" e "animation". São pequenos games elaborados de forma a transmitir uma mensagem política a seus jogadores.

emancipem e ganhem autonomia.

Para Silveira, portanto, por um lado, o hacking é composto por um hiper-individualismo de seus membros; mas, por outro, tal hiper-individualismo é constituído em processos colaborativos. No ativismo hacker, isso não é diferente. Como consequência, esses atores realizam “um novo modo de resistência que passa pelo conhecimento e pela auto-formação de indivíduos autônomos e colaborativos. Isso porque os hackers exploram as falhas dos protocolos, suas propriedades e suas formas de controle”.

Para o autor, no universo hacker, para resistir, é preciso emancipar-se e, para tanto, o caminho é a busca pelo conhecimento.

*****

Outro trabalho brasileiro nesse sentido é assinado por Rodrigo Morais (2005). O pesquisador insere o fenômeno dos hackers no novo paradigma informacional, tal como formulado por Castells (2007). Qualifica-os como atores cuja ética estabelece uma nova relação com o trabalho e cuja existência alude à "fonte cultural da inovação tecnológica em que se baseia o informacionalismo" (MORAIS, 2005, p.3). Defende, ainda, que a ética hacker propõe uma nova perspectiva, constituindo-se como uma linha de fuga à lógica do capitalismo informacional – assim como apontou André Gorz, para quem os hackers são "os dissidentes do capitalismo digital" na medida em que se opõem "à privatização dos meios de acesso a esse 'bem comum da humanidade', que é o saber sob todas as suas formas" (GORZ, 2005, p. 63).

Já em relação ao hacktivismo, para Morais, à medida que ele é compreendido como uma atividade política que traz em seu bojo tanto movimentos sociais como especialistas em computação, faz-se sumariamente importante na resistência ao Império, na concepção de Negri e Hardt (2001), uma vez que pode contribuir para a construção de uma organização política alternativa e independente. O autor estabelece relação entre os diversos fluxos de poder imperiais, ainda com base na chave de pensamento de Negri e Hardt, e as interpretações do coletivo Critical Art Ensemble (2001), conforme se abordará a seguir, para quem as elites do capitalismo inventaram um novo e nômade modelo de poder a partir do ciberespaço – um local pleno de fluxos invisíveis e ininterruptos. Por conta disso, sugere o coletivo que a resistência política deve ocorrer não mais nas praças, avenidas ou monumentos públicos

físicos, mas sim com base e por meio do ciberespaço. Nesse cenário, as ações dos hackers mostram-se como a maneira ideal de combater o poder nômade das elites – as garras onipresentes do Império.

Morais conclui que o hacking constitui-se em uma novidade que tem papel relevante sobretudo em dois aspectos. Primeiramente, na formulação de novas formas de resistência política, alinhando-se, portanto, à desobediência civil eletrônica. Em segundo lugar, os hackers envolvem-se em um tipo de produção imaterial que não se submete à lógica do capital – o que não deixa de ser uma forma de resistência, mesmo que cultural. "Seu grande mérito, creio, está em ultrapassarem a mera contestação, a recusa, e em serem portadores de uma ética de cooperação e compartilhamento que propõe novos modos de encarar o conhecimento, o trabalho, o tempo, o dinheiro, em suma, a própria vida" (MORAIS, 2005, p. 98).

*****

Outra pesquisadora, a antropóloga Gabriella Coleman, muito tem contribuído com relatos etnográficos importantíssimos quanto ao hacking e ao hacktivismo. Trata-se, seguramente, da pesquisadora que mais tem acompanhado a rede hacktivista Anonymous desde que o coletivo revelou sua face política, no início de 2008. Em momentos seguintes, será necessário recorrer às publicações da autora que tratam da história, da ética e das formas de ação do coletivo. Por ora, interessam alguns de seus apontamentos quanto à cultura hacker e os gêneros morais.

Em *Hacker practice: moral genres and the cultural articulation of liberalism*, Coleman e Golub (2008) criticam os estudos acadêmicos que representam os hackers de maneira dicotômica: para alguns, são jovens visionários cujo modo de vida utópico e tecnológico teria o potencial para romper com as patologias apresentadas pelo capitalismo e pela modernidade; para outros, são adolescentes nada saudáveis que se envolvem em atividades de intrusão em ambientes protegidos. Neste primeiro grupo, a autora inclui os trabalhos de Levy (2000) e Himanen (2001), já trabalhados neste trabalho.

Mais recentemente, Coleman (2011) argumentou que visões dicotômicas como essas tendem a utilizar uma abordagem e uma terminologia inadequadas para compreender o fenômeno do hacking, sua fonte e seu significado. A autora defende que há uma vasta pluralidade de experiências digitais e, por isso, é necessário usar uma terminologia que dê

conta dessas diferentes formas de experiência, incluindo os vários graus e tipos de saturação tecnológica a que os hackers são submetidos. E tais formas de experiência, por sua vez, modelam (mas não simplesmente determinam, vale ressaltar) os públicos, as opiniões políticas e os compromissos éticos dos hackers. Afinal, eles não existem isoladamente, mas estão sempre envolvidos em redes institucionais e culturais, bem como em processos econômicos. Portanto, convém investigar as principais características que marcam as sensibilidades políticas e táticas dos hackers.

Assim, ao examinarem o que chamaram de "natureza heterogênea da socialidade hacker, a fim de retratar mais adequadamente a complexa topografia da moralidade hacker" (2008, p. 255), Coleman e Golub distinguem e analisam três gêneros morais concernentes à prática hacker para demonstrar que não há uma única "ética hacker". Para além disso, os autores argumentam que os hackers continuamente reformulam e criticam uma vasta gama de valores liberais em suas vidas cotidianas, o que reforça seu caráter plural.

Os três exemplos de gêneros morais são, precisamente, (1) a cripto-liberdade e as políticas da tecnologia; (2) o software livre e as políticas de inversão; e (3) as políticas de transgressão *underground*. Os três casos, por sua natureza, envolvem também as práticas hacktivistas.

O primeiro gênero diz respeito aos hackers que se envolvem com criptografia, em boa parte dos casos com a finalidade de promover uma navegação privativa ou anônima na rede, ou mesmo a fim de driblar mecanismos de censura impostos por governos. Aqui, articulam-se claramente os valores da autonomia individual e da liberdade diante da interferência governamental.

Já o segundo caso trata dos desenvolvedores de software livre/*open source*. Embora, de modo geral, eles também compactuem com essa cultura liberal presente no primeiro caso, é possível observar que, de um lado, o movimento de software livre, encabeçado em grande medida por Richard Stallman, foca-se em questões ideológicas quanto à liberdade do conhecimento; e, de outro, o movimento *open source*, capitaneado por Eric Raymond, prefere ater-se às questões mais técnicas, chamando a atenção para a superioridade do modo de produção em uma comunidade de software livre.

Por fim, para o *underground* hacker, a privacidade e a liberdade de informação são meros ideais que, na realidade, nunca serão alcançados de maneira absoluta. Dessa forma, esse gênero moral evita soluções liberais politicamente corretas, radicalizando completamente

as reivindicações morais do liberalismo. A crítica política desses hackers tem início com práticas de transgressão. "Este grupo considera o hacking como uma corrida armamentista constante entre aqueles com o conhecimento e o poder para erguer barreiras e aqueles com igual poder, conhecimento e, principalmente, desejo de desarmá-los", dizem os autores (Op. cit., p. 263).

Com isso, observamos que, na realidade, o hacking – e também o hacktivismo – contemplam uma vasta gama de subculturas:

> É evidente que alguns hackers se engajam livremente no comércio ilícito de arquivos, ao passo que outros não o fazem. Alguns hackers não se importam com aspectos técnicos e legais da criptografia, enquanto outros veem isso como algo constitutivo de sua identidade hacker. Muitos hackers são comprometidos com a filosofia ética do software livre, enquanto outros sentem que têm o direito individual de organizar a propriedade intelectual da forma como querem. Alguns hackers anunciam com orgulho suas façanhas ilegais, e outros admitem isso com relutância, um pouco envergonhados de sua incursão no mundo *underground* (Idem, p. 267).

Enfim, essa leitura equilibrada trazida por Coleman deve permear este trabalho, de tal sorte que a intenção, ao desenvolver esta pesquisa, não é pintar hacktivistas nem como benfeitores revolucionários nem como intrusos antissociais, mas sim como atores cuja relevância mostra-se cada vez mais decisiva quando se pensa nas novas formas de resistência política ao controle distribuído. Identificamos, sim, uma pontual ética hacktivista, como se observou acima, mas é sempre preciso ter em mente essa diversidade de facetas envolvendo a cultura hacker e, como se verá, o próprio movimento Anonymous.

2.4.2 Guerra da informação / ciberterrorismo

Conforme observamos, esta perspectiva teórica apreende o hacktivismo no contexto da segurança computacional, da guerra da informação e do ciberterrorismo. Ela tem seus expoentes nas pesquisas de Dorothy Denning e dos pesquisadores da RAND corporation David Ronfeldt e John Arquilla e se baseia principalmente em relatos de incidentes e na cobertura feita pela imprensa. Aqui se relegam, na maior parte dos casos, os aspectos sociais, econômicos e políticos do hacktivismo, de modo que esta literatura se faz valiosa no que diz

respeito a análises objetivas quanto às novas formas de conflito presentes no mundo contemporâneo.

Talvez o ponto de partida dessa visão esteja no artigo "Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy", em que se analisam as potenciais influências das práticas em rede em relação à política externa. Nele, a pesquisadora coloca, de um lado do espectro político, o ativismo on-line convencional, e, do outro lado, o hacktivismo e o ciberterrorismo. Segundo ela, "com respeito ao hacktivismo e ao ciberterrorismo, aqueles que se engajam nessas atividades têm menos probabilidade de conseguir seus objetivos na política externa do que *aqueles que não empregam técnicas destrutivas e disruptivas*" (2001, p. 242, grifo nosso).

Com isso, a autora trata o hacktivismo exclusivamente como uma questão de ameaça à segurança informacional – uma prática a que os governos devem prestar muita atenção a fim de combater. E, ao posicionar o hacktivismo como apenas mais uma das ameaças existentes no campo da segurança da informação, Denning acaba por, primeiramente, desconsiderar a vasta gama de ações hacktivistas, sobretudo as não disruptivas; e, por fim, rechaça qualquer significância política do hacktivismo.

Arquilla e Ronfeldt (1997), por sua vez, têm uma vasta obra em seu trabalho como pesquisadores militares ligados à RAND Corporation, uma das principais agências independentes de fomento à pesquisa sobre temas de interesse do Departamento de Defesa dos Estados Unidos. Segundo eles, os modos de ação política em rede têm como base um precedente fundamental: a chamada era da informação, que reforça as formas de organização em rede e altera a natureza dos conflitos. Para os autores, portanto, o aumento da ação em rede reflete (e está intimamente ligado à) revolução informacional.

Com isso, cunham o conceito de "guerra em rede" (*netwar*), em oposição à "guerra de controle" (*cyberwar*). Enquanto esta diz respeito à tradicional luta por meio da tecnologia militar travada por dois ou mais Estados (como as duas Grandes Guerras Mundiais, por exemplo), a guerra em rede se configura como um modo de conflito em níveis sociais, nas quais os protagonistas usam (e dependem de) formas de organização, doutrina, estratégia e comunicação em rede. Essa guerra, de baixa intensidade, é travada de modo assimétrico entre um Estado (por exemplo, o caso do México) e grupos organizados em rede (analogamente, o movimento zapatista), de modo que estes empregam tal rede para comunicação e controle operacional, podendo levar suas atividades para além do ciberespaço. Além disso, estes

grupos agem com frequência sem uma liderança central, de modo que a tomada de decisão pode ser deliberadamente descentralizada e dispersa.

"Portanto", dizem os autores, "a guerra em rede se diferencia dos modos de conflito e crime tradicionais, nas quais os protagonistas preferiam usar organizações, doutrinas e estratégias hierárquicas nos esforços de fomentar movimentos de massa grandes e centralizados sob contornos leninistas" (1997, p. 277). Como exemplos de movimentos que se valem das tecnologias digitais e das formas de organização em rede para promover guerras em rede, os pesquisadores citam grupos terroristas transnacionais, negociantes de armas de destruição em massa no mercado negro, movimentos fundamentalistas e etnonacionalistas, "piratas da propriedade intelectual" – notadamente, hackers –, contrabandistas de imigrantes e refugiados, entre outros.

Arquilla e Ronfeldt analisam esses movimentos justamente para desenvolver estratégias para que governos e empresas combatam as chamadas guerras em rede. Seu argumento é o de que, após a revolução informacional e as novas formas de organização em rede, o novo cenário favorece aqueles que dominam esse novo tipo de gestão. Portanto, é preciso atualizar as táticas de dominação.

Embora façam ressalvas em relação ao que denominaram "guerra em rede social" (*social netwar*), como no caso das mobilizações on e offline em torno da luta zapatista no México, à qual estratégias "antiguerra em rede" não deveriam necessariamente ser aplicadas – argumentando que a guerra em rede não é um fenômeno uniformemente adverso nem necessariamente uma forma de conflito que atrapalhe os objetivos dos governos –, o paradigma militarista, que percorre toda a obra dos autores, não é adequado para esta análise quanto ao hacktivismo. Afinal, sob esta perspectiva, é impossível compreender o ativismo hacker senão como uma forma de praticar o ciberterror e demais crimes virtuais. Essa visão, que, conforme observamos no trabalho de Vegh (2003), tem amplo respaldo na imprensa e é reducionista à medida que desconsidera por completo as os aspectos sociais, culturais e políticos presentes nas várias facetas do hacktivismo, em especial, e do ativismo em rede, em geral.

2.4.3 Hacktivismo por ele mesmo

Por fim, a terceira perspectiva teórica que lança interpretações sobre o fenômeno do hacktivismo é aquela que elaborada pelos próprios hacktivistas/ciberativistas. Escritos por indivíduos ou em nome de um coletivo, esses textos, em grande parte, tornaram-se peças clássicas de inspiração para novos hackers, além de fonte de influência e pesquisa para diversos trabalhos acadêmicos.[18]

Evidentemente, se fôssemos classificar os trabalhos que compõem esta terceira perspectiva teórica em um dos campos anteriores, ele seria o da desobediência civil eletrônica. No entanto, optamos por tratá-los de forma separada pelo fato de serem, em vez de trabalhos cuja finalidade é exclusivamente acadêmica, peças que descrevem motivações e compromissos ideológicos dos ativistas que os formularam. Contudo, longe de meramente representarem tais hackers em sua forma mais apaixonada e teórica, desvinculando-se de evidências empíricas a seu respeito, essas obras têm um papel fundamental porque, por um lado, nos fornecem uma fonte primária de estudo em relação ao hacktivismo e, por outro, influenciam muitos estudos acadêmicos a esse respeito – inclusive muitos dos autores acima citados.

Talvez o primeiro grande trabalho sob essa perspectiva tenha sido o seminal *Distúrbio eletrônico* (2001), de autoria do coletivo de artistas digitais e ativistas políticos Critical Art Ensemble (CAE). Posteriormente, o coletivo lançaria outros 5 livros, além de vários artigos, tendo parte de seus escritos traduzidos para mais de 18 línguas. Enfim, pode-se dizer que sua vasta obra opera propriamente como uma fundação teórica do hacktivismo.

Mas é em seu primeiro trabalho que os ativistas do CAE pontuam um dos argumentos que percorrerá boa parte dessa obra, bem como influenciará o discurso e a prática de hacktivistas até os presentes dias. Trata-se do argumento de que, em tempos de revolução informacional, a natureza e a estrutura do poder mudaram e, por conta disso, a natureza e a estrutura da resistência devem, obrigatoriamente, acompanhar essas mudanças, transferindo-se para os campos de batalha do ciberespaço:

18 Vale ressaltar que, nesta perpectiva, ainda estamos tratando de textos teóricos ou de manifestos fundantes. Quanto aos diversos textos comuns publicados por hacktivistas em todo o mundo, apesar de abundantes e consistentes, fogem ao escopo deste trabalho. Como também analisaremos, em capítulo seguinte, o discurso característico dos hackers do Anonymous e, levaremos em conta textos publicados em nome do coletivo.

> As regras da resistência cultural e política mudaram radicalmente. A revolução tecnológica causada pelo rápido desenvolvimento do computador e do vídeo criou uma nova geografia das relações de poder no Primeiro Mundo. Uma nova ordem que há cerca de vinte anos só poderia existir na imaginação: as pessoas estão reduzidas a dados, a vigilância ocorre em escala global, as mentes estão dissolvidas na realidade da tela do monitor. Surge um poder autoritário que floresce na ausência. A nova geografia é uma geografia virtual, e o núcleo da resistência política e cultural deve se afirmar nesse espaço eletrônico (CAE, 2001, p. 11).

Essa nova "geografia de poder" a que o coletivo se refere é a de um poder nômade,[19] cuja sede se vê em uma zona ambígua, sem fronteiras, sem delimitação precisa. À maneira dos citas – descritos por Heródoto em *As guerras pérsicas*, um povo sem cidades ou territórios fixos, usando seu constante movimento para promover sua autonomia e atacar outros povos sem que sua sede pudesse ser algum dia capturada –, o capitalismo tardio apoia-se na abertura tecnológica vigente no ciberespaço para reinventar um poder arcaico nômade, a fim de forjar um meio sustentável de (continuidade de) dominação.

Nesta nova modalidade de poder, os nômades militarizados sempre estão na ofensiva. Afinal, sua presença é pervasiva, suas "casamatas"[20] estão por toda parte e, como não são localizáveis, não têm a necessidade de se defender. Dessa forma, "a elite contemporânea se desloca das áreas urbanas centralizadas para o ciberespaço descentralizado e desterritorializado" (Op. cit., p. 27).

Diante disso, como ficam as vozes da resistência?

Segundo o CAE, esse poder nômade, potencialmente inexpugnável, praticamente emudeceu a voz da contestação, trazendo à cena tempos de desilusão. Por isso, de acordo com o coletivo, face a essa nova geografia de poder, as estruturas "sedentárias" de resistência – protestos em ruas, ocupações, movimentos trabalhistas, sindicatos etc. – tornam-se, inevitavelmente, servas das estruturas nômades. A fragmentação do mundo e os fluxos difusos de poder as tornam inermes, inócuas, sem sentido algum. A que a resistência pós-moderna deve recorrer, então?

De acordo com o CAE, "o vocabulário da resistência deve ser expandido para incluir meios de distúrbio eletrônico. Assim como a autoridade localizada nas ruas era combatida por

19 Essa noção, como podemos perceber no decorrer do relato, é muito semelhante à ideia de Império, tal como formulada por Hardt e Negri (2001).

20 "Espaços públicos privatizados que servem a várias funções particularizadas, tais como a continuidade política (repartições governamentais ou monumentos nacionais), ou áreas para orgias de consumo (shopping centers)" (CAE, 2001, p. 35). Há também a casamata eletrônica: a mídia, que tenta colonizar a residência particular.

meio de manifestações e barricadas, a autoridade que se localiza no campo eletrônico deve ser combatida através da resistência eletrônica" (Idem., p. 33). Ou seja, a resistência ao poder nômade deve se dar no e por meio do ciberespaço.

Enfim, permeado por citações que vão de Heródoto a Duchamp, passando por Wright Mills, Baudelaire e André Breton, *Distúrbio eletrônico* cumpre o papel de abrir o caminho teórico sobre o qual se sustentariam as bases então incipientes do hacktivismo.

*****

Em 1998, quatro anos após a publicação de *Distúrbio eletrônico*, Ricardo Dominguez, um dos mais conhecidos integrantes do Critical Art Ensemble, encabeçou a criação de um grupo hacker. Ele conta que deixou o CAE porque se frustrou com o fato de o grupo não se esforçar para colocar em prática suas teorias de desobediência civil eletrônica. Para criar seu novo coletivo, uma razão em específico o moveu: no calor dos acontecimentos envolvendo o Exército Zapatista de Libertação Nacional (EZLN) e o governo mexicano, à época liderado havia mais de seis décadas pelo Partido Revolucionário Institucional (PRI), uma violenta ofensiva do exército mexicano sobre comunidades zapatistas deixou 45 pessoas mortas no vilarejo de Acteal.

Em *Digital zapatismo*, texto-manifesto publicado naquele ano por Dominguez, o ativista relata como, após aquele massacre, ocorrido em dezembro de 1997, os ciberativistas – hacktivistas incluídos – envolvidos na grande rede de colaboração formada em apoio ao movimento zapatista precisaram responder com um nível mais intenso de desobediência civil, para além da retransmissão de informações e do envio em massa de e-mails aos governantes mexicanos, práticas que já vinham sendo adotadas até então.

Tendo isso em vista, Dominguez fundou o Electronic Disturbance Theater (EDT), grupo de hacktivistas que criou, duas semanas depois de se organizar, uma "ferramenta de protesto virtual": o software Zapatista Floodnet. Antes dessa ferramenta, já havia grupos de ativistas tentando realizar ações de negação de serviço. Eles eram convocados para clicar à exaustão, durante 1 hora, no ícone "atualizar" de seus navegadores, fazendo com que determinados servidores que hospedassem sites "símbolos do neoliberalismo mexicano" (como os da Bolsa Mexicana de Valores, do Banco de México e do Banamex) saíssem do ar. Posteriormente, o EDT facilitou o trabalho desses ativistas, pois o Zapatista Floodnet, quando

instalado em seus computadores, fazia tal trabalho automaticamente, enviando vários pedidos de atualização por segundo aos referidos servidores.

Ainda em *Digital Zapatismo*, Dominguez observa que, além de realizar ações como essa, qualificadas por ele como ações Beta – que, na linguagem dos programadores, significa algo ainda não acabado, em fase de testes –, boa parte das pessoas que estavam envolvidas nesses atos começaram a fazer uma análise mais focada em quais métodos de desobediência civil eletrônica poderiam funcionar de verdade. "Especulações quanto às implicações tecnológicas sobre essas ações começaram a se focar em questões como: Quem é mais provável que seja prejudicado com esse movimento?", questionavam-se (DOMINGUEZ, 1998, on-line).

Se, por um lado, os governos, para lidar com a crescente vulnerabilidade apresentada pelas infraestruturas eletrônicas, tiveram de redefinir as formas de tratar o comando, o controle e a inteligência, implementando, para isso, grandes redes de hipervigilância, as formas de resistência também deveriam se modificar. Dominguez observa que todo o movimento do Digital Zapatismo usou o sistema mais básico de troca de informações da cultura digital, como os e-mails, para perturbar esse "Estado Informático" e vigilante. E propôs-se a fazer um grande exercício de inventar outras formas de desobediência civil eletrônica, desenvolvendo métodos inventivos de ação política, apesar da incerteza em relação a essas ações.[21]

Enfim, Dominguez e o movimento de ciberativistas em torno dos zapatistas são, verdadeiramente, pioneiros em muitas das questões práticas associadas ao hacktivismo. Neles vemos o início do esforço de agir politicamente valendo-se de formas inovadoras das teias do ciberespaço e, além disso, pensar criticamente acerca dessas formas. Sua ação pioneira na coordenação de acessos em massa a determinados sites-alvo pode ser considerada uma precursora das hoje tão disseminadas ações distribuídas de negação de serviço (DDoS). Por conta disso tudo, é fundamental revisitar textos publicados pelo EDT e seus membros, mesmo porque, conforme observou Samuel (2004, p. 83), "as atividades do Electronic Disturbance Theater tem sido cruciais ao definir as atividades e a cultura da cena dos hacktivistas de performance". Ou seja, seu legado é seguido até os dias atuais.

21 Como, em 1998, ano da publicação deste texto-manifesto, a Internet não havia chegado a grande do planeta, apostar nesse meio como forma de ação ainda era algo, no mínimo, incerto. No entanto, já se notava que ele não passaria despercebido. "Neste ponto, é difícil saber quão perturbadores esses atos de desobediência civil eletrônica especificamente são. O que nós realmente sabemos é que o poder neoliberal está extremamente preocupado com eles", afirma Dominguez (1998, on-line).

***

Um desses textos foi publicado por outro integrante do EDT, o escritor e profissional de mídia digital Stefan Wray, também em 1998.[22] Em *Electronic civil disobedience and the world wide web of hacktivism: a mapping of extraparliamentarian direct action net politics*, conforme vimos na introdução deste trabalho, Wray estabelece o ano de 1998 como o marco inicial para o surgimento de dois termos: "desobediência civil eletrônica" e "hacktivismo". Ele descreve e aponta, além das experiências do EDT com o Zapatista FloodNet, uma série de atos hacktivistas que ocorreram, naquele ano, na Grã-Bretanha, na Áustria, na Índia, na China, de forma que, em quase todos os continentes, houve relatos de "hacktividade ".

Tomados em seu conjunto, esses atos, que envolvem desde ações mais simbólicas de desobediência civil quanto os eventos hacktivistas que mais se aproximam da ação política direta, são classificados por Wray como "ação política direta, em rede e extraparlamentar" (*extraparliamentarian direct action net politics*). Já naquela época, ele observava a repercussão desses atos no campo midiática.

O autor divide essa ação política direta, em rede e extraparlamentar em cinco subcategorias, ou tendências. São elas: (1) ativismo de computador (computerized activism); (2) guerra informacional (grassroots infowar) ; (3) desobediência civil eletrônica (electronic civil disobedience); (4) hacking politizado (politicized hacking) ; e (5) resistência à guerra futura (resistance to future war). Para Wray, essas tendências se constituiriam como um ponto de partida para pesquisas sobre a convergência do ativismo, da arte, e da comunicação e mídia computadorizados.

O (1) ativismo de computador diz respeito às redes de solidariedade informacionais via e-mails, fóruns, listas de discussão etc. Elas deixaram de ser marginais à medida que a Internet comercial se populariza, no início dos anos 1990, e com a chegada do navegador (*browser*) com interface gráfica, em meados da mesma década. O autor define esse ativismo como o simples uso da infraestrutura da Internet como um meio a partir do qual ativistas se comunicam uns com os outros. Trata-se da forma menos ameaçadora ao poder quando

22 Além de Ricardo Dominguez, compuseram o EDT Carmin Karasic, que trabalhava como assistente em um laboratório do Massachusetts Institute of Technology (MIT); Brett Stalbaum, artista digital, assim como Dominguez; e Stefan Wray, a quem Dominguez conheceu quando o entrevistou sobre seus escritos acerca do papel do exército estadunidense na guerra às drogas implementada pelo governo mexicano. Em comum, eles tinham o desejo de ajudar, de alguma forma, a luta zapatista.

comparada com outros usos, nos quais a infraestrutura da rede se fortalece como um objeto ou um campo de ação, e não apenas um meio. É também a forma que conhecemos há mais tempo e, por ser menos comprometedora, muitos atores políticos da rede se sentem mais confortável nela.

Já a (2) guerra informacional, aqui entendida como uma guerra de palavras, discursos, propaganda etc. é uma forma que intensifica o ativismo de computador, sendo o primeiro passo da mudança de perspectiva de que a Internet é apenas um campo para comunicação. O paradigma da guerra informacional foi elaborado pelos pesquisadores da RAND, conforme observamos na seção anterior deste capítulo. Wray observa que, após o massacre de Acteal, que pode ser tomado como um ponto de partida, passou-se a aceitar a infraestrutura da Internet tanto como um canal de comunicação quanto como um campo de ação. Neste caso, o exemplo zapatista também nos serve. Em boa medida, pesquisadores que se debruçaram sobre o movimento, como Ortiz (2003) e Cleaver (1998), observam que os zapatistas deveram sua sobrevivência à guerra de palavras – uma guerra de propaganda que tem foi propagada de forma bem-sucedida por líderes zapatistas como subcomandante Marcos, bem como por apoiadores não-zapatistas em todo o mundo todo. Uma grande diferença positiva da guerra informacional é a de que ela vem com um desejo de incitar a ação, e com a habilidade de fazê-lo em uma escala global .

(3) Desobediência civil eletrônica, por sua vez, remete à tradição da ação direta não violenta e à desobediência civil. É a primeira forma de transgressão eletrônica. Neste caso, os ativistas emprestam táticas de transgressão e bloqueio de movimentos sociais tradicionais, aplicando-os, muitas vezes de maneira experimental, na Internet, como em manifestações ou bloqueios virtuais – um bom exemplo são as ações de negação de serviço. Antes de 1998, observa Wray, a desobediência civil eletrônica existia apenas em teoria. O termo, como observamos acima, foi cunhado pelo CAE.

Fazem parte do (4) hacking politizado as ações hackers que geralmente alteram páginas web, inserindo nelas mensagens políticas. É outro tipo de ação política transgressiva, mas que não requer mobilização nem participação de massa – basta que um ator com habilidades técnicas se mobilize e envie sua mensagem. Nestes casos, ao contrário dos ativistas da desobediência civil eletrônica, os atores escondem seus nomes, uma vez que são ações claramente ilegais (no caso da desobediência, eles operam em uma zona ambígua da legislação).

(5) Resistência à guerra futura é uma categoria que funciona mais em sua forma potencial e trata da resistência que pode se dar, de maneira coordenada, entre hackers de todo o mundo. Se, por um lado, alguns classificam a Guerra do Golfo (1990-1991) como a primeira guerra da informação em razão da dependência do aparato militar das tecnologias de comunicação e informação – envolvendo satélites, radares, rádio, telefone etc. –, essas mesmas tecnologias propiciaram uma robusta resistência aos esforços da guerra. Opositores a ela usaram amplamente e-mail para se comunicar e se informar sobre a resistência em outras cidades por meio de sistemas de boletins e grupos de notícias. Com isso, diz Wray (1998, on-line), se os Estados Unidos decidirem entrar em uma guerra impopular, "com que o hacktivismo se pareceria nas condições de uma resistência mais generalizada? Ou, dito de outra forma, com que a resistência generalizada se pareceria nas condições do hacktivismo?".

Entre a desobediência civil eletrônica e a resistência à guerra futura, as transgressões movem-se em direção a uma Internet que, cada vez mais, deixa de ser uma simples esfera pública global para se transformar em um território conflituoso no qual o poder está em disputa. Com essa incipiente taxonomia, elaborada quando o hacktivismo mostrava suas primeiras faces, Stefan Wray tenta estabelecer bases teóricas e classificativas em relação a este fenômeno. Para isso, o autor captou o exato momento em que as redes comunicacionais estavam deixando de ser meros instrumentos de ação.

***

Por fim, mas não menos importante, cabe voltarmos atenção a outro clássico frequentemente apropriado pelo ativismo on-line e pelo hacktivismo. Trata-se do ensaio *TAZ: zona autônoma temporária*, assinado por Hakim Bey em meados dos anos 1980. Historiador e teórico libertário associado ao anarquismo (chegou a referir a si mesmo como um "anarquista ontológico" em diversas ocasiões), Hakim Bey é, na realidade, o pseudônimo de Peter Lamborn Wilson.

Bey inicia seu ensaio tratando das redes de informação globais de piratas e corsários no século XVIII, redes estas compostas por ilhas e esconderijos distantes, muitos abrigando comunidades fora-da-lei temporárias. Se, para o autor, as tecnologias modernas acabaram por inviabilizar esse tipo de autonomia, possibilitou a existência de outros tipos de enclave s livres.

O autor prioriza as formas de levante (de caráter temporário) em detrimento da revolução (de caráter permanente). Experiências de pico extraordinárias e de alta intensidade, comumente relacionadas à festividade, os levantes seriam uma saída para confrontar o Estado de novas formas, num tempo em que falar de revolução – ou até mesmo desejá-la – não faz mais sentido. "Nada, além de um martírio inútil, poderia resultar de um confronto direto com o Estado terminal, esta megacorporação/Estado de informações, o império do Espetáculo e da Simulação. Todos os seus revólveres estão apontados para nós" (BEY, 2001, on-line), argumenta, fazendo alusão às práticas revolucionárias. Para além disso, não há como guerrear com o Estado armados de modo miserável e, mesmo que assim não fosse, não se teria nem mesmo em que atirar senão numa forma estatal que se constitui "numa histerese, num vazio rígido, num fantasma capaz de transformar todo lampejo num ectoplasma de informação" (Idem, on-line).

Dessa forma, Bey nos apresenta a TAZ (sigla para *temporary autonomous zone*, ou zona autônoma temporária), uma forma de rebelião que tem a destreza de não confrontar o Estado diretamente. Trata-se de uma operação anárquica de guerrilha que torna livre uma área, podendo esta se de terra, de tempo, ou mesmo de imaginação. A TAZ é ágil o suficiente para se dissolver e se refazer noutro lugar e noutro momento, de modo que o Estado não consiga atingi-la, ou nem mesmo saber de sua existência. A TAZ "ocupa" clandestinamente uma área, um tempo ou uma forma imaginativa, realiza-se e se esvai. Sua principal característica é a invisibilidade, pois o Estado não pode reconhecê-la e, com isso, destruí-la. Assim que desaparece, surge novamente noutro lugar, novamente invisível, novamente livre.

Em uma época em que esse Estado é onipresente e todo-poderoso, de um lado, mas repleto de rachaduras e fendas, por outro, a TAZ, para Bey, é uma tática perfeita. Tanto em suas formas de ataque quanto de defesa – que podem variar de acordo com as necessidades postas –, a TAZ não faz nada além de evadir a violência estatal. Por sua natureza, ela ataca as estruturas de controle, sobretudo as ideias dominantes.

O autor observa que o mapa mundial está fechado: nenhuma área do planeta está livre da polícia ou dos impostos. Afinal, a última parcela de terra não reivindicada por um Estado-nação foi assim apropriada ao final do século XIX. Mas, ao mesmo tempo em que o mapa está fechado, a zona autônoma temporária está aberta, pois ela se desdobra em dimensões que são invisíveis à cartografia do controle. Neste momento, Bey apresenta o conceito de "psicotopologia", "uma 'ciência' alternativa àquela da pesquisa e criação de mapas e

'imperialismo psíquico' do Estado". Apenas essa "ciência" seria capaz de representar mapas fiéis à realidade, em escala 1:1, uma vez que apenas a mente humana é complexa o bastante para representar o real. E essa ciência, da mesma forma, é incapaz de controlar um território, uma vez que um mapa em escala 1:1 é idêntico a esse mesmo território. Com isso, a psicotopologia favorece a busca de espaços geográficos, sociais, culturais ou imaginários com potenciais para se configurarem como zonas autônomas temporárias.

O que poderia dar suporte a uma TAZ?

Neste ponto, apesar de se mostrar um cético tecnológico, colocando sempre em dúvida as benesses que tecnologias como o computador pessoal supostamente nos trariam, Bey afirma que a web[23] fornece à TAZ um apoio logístico, ajudando a criá-la. Ela, a web, funcionaria como um sistema de suporte, que pode, por exemplo, defender a TAZ – tornando invisível ou proporcionando a ela garras – ou transmitir informações rapidamente de uma TAZ a outra. Além disso, por ser sempre um acampamento nômade, a TAZ poderia contar com a web para criar coletivamente seus épicos, suas canções, suas lendas: "A contra-net assume a promessa de ser um aspecto integral da TAZ, uma adição que irá multiplicar o seu potencial, um salto quantum, um salto enorme em termos de complexidade e significância" (Ibidem, on-line).

Enfim, a "contra-net" de Hakim Bey é um meio, e não um fim si. O objetivo de uma zona autônoma temporária é mostrar resultados, atacando a realidade consensual, conquistando patamares de vida melhores e mais intensos. Para o autor, a grande rede só tende a facilitar esse processo, mas, caso assim não se faça, ela se torna dispensável.

A noção de zona autônoma temporária, desde que formulada, foi apropriada por diversos grupos sociais, desde frequentadores de raves até ciberativistas e hacktivistas, para quem *TAZ* é como um texto clássico fundador. Como bem pontuou Ricardo Rosas, no texto "Hakim Bey: o profeta anarquista do caos eletrônico": "A TAZ ou ZAT, em português, é livro de cabeceira (ou de tela, se preferir) de nove entre dez ativistas eletrônicos".[24] A ideia de um bando auto-organizado (em detrimento de uma estrutura hierárquica organizada), nômade, independente de fronteiras geográficas, que implementa ações diretas localizadas, dinâmicas, e que acontece invisível, de forma a não deixar rastros, é encarnada não apenas por teóricos

23 Bey (2001, on-line) diferencia os termos "web" e "contra-net": "Empregaremos a palavra web para designar a estrutura aberta, alternada e horizontal de troca de informações, ou seja, a rede não- hierárquica, e reservaremos o termo contra-net para indicar o uso clandestino, ilegal e rebelde da web, incluindo a pirataria de dados e outras formas de parasitar a própria net".

24 Texto disponível em: <http://pt.protopia.at/index.php/Hakim_Bey:_O_Profeta_Anarquista_do_Caos_Eletr%C3%B4nico>. Acesso em: 30 mar. 2012.

do hacktivismo, mas também pelos próprios hacktivistas. Não seria exagero sugerir que um coletivo hacktivista forja, a cada ato de desobediência civil eletrônica, uma zona autônoma temporária que, depois de cumprir seu objetivo político e passar sua mensagem – em atos que se assemelham a um microlevante festivo –, rapidamente se desfaz, invisível, já em busca de uma nova zona autônoma a ser ocupada.

*****

Enfim, essa pequena amostra que selecionamos sobre a terceira perspectiva teórica aqui abordada nos ajuda a compreender a força motriz do pensamento dos hacktivistas de outrora, além de auxiliarem no entendimento quanto ao campo da desobediência civil eletrônica. Ela, combinada às perspectivas anteriores, traz muitas das características que observaremos nos dois capítulos seguintes, sobretudo no que tange à estrutura, à organização, ao ideário e aos modos de ação dos Anonymous brasileiros.

3 OS ANONYMOUS

> "O *Anonymous* é sustentado – e por vezes amplificado – não apenas pelo uso eficaz de tecnologias de comunicação, mas por uma cultura que floresce na tensão entre a ordem e a desordem, entre o frio e o quente, a seriedade e o *lulz*, o anonimato e a transparência"
> (COLEMAN, 2012, p. 103)

Até o momento, este trabalho apresentou os principais objetivos de pesquisa e argumentou, no primeiro capítulo, que o hacktivismo se mostra como uma reconfiguração no hacking político, tendo em vista as diversas gerações de hackers desde os anos 1960. No capítulo anterior, discutiu-se como o fenômeno do ativismo hacker pode representar uma forma de resistência política na chamada sociedade de controle, apontando as principais estratégias comumente utilizadas para tal. Para isso, recorreu, em primeiro lugar, à fundação teórica da sociedade de controle e apresentou algumas de suas principais expressões na literatura acadêmica contemporânea. Em um segundo momento, discutiu as principais perspectivas teóricas que se dedicam ao estudo do hacktivismo, recorrendo a autores de diversas áreas do conhecimento.

Dando sequência a esta linha narrativa, este capítulo traz os principais resultados da pesquisa empírica, caracterizando o coletivo Anonymous, principalmente em suas vertentes hacktivista e brasileira. Nesse sentido, para realizá-lo, identifica as origens e as principais ações do movimento em nível internacional – inequívocas fontes de inspiração para os brasileiros – para, em seguida, apontar as principais faces do coletivo no Brasil. Por fim, realiza uma breve análise de duas operações deflagradas por hacktivistas brasileiros: a Operação WeeksPayment e a Operação Globo.

3.1 DAS ENTRANHAS DO 4CHAN À AÇÃO COLETIVA

Uma legião, um coletivo, uma ideia, uma rede, uma comunidade virtual, uma forma de ação, uma marca, um pressuposto, um conceito ou um movimento? Em meio a uma infinidade

de outras caracterizações possíveis, todas essas designações já foram utilizadas por pessoas que, de alguma forma, estão relacionadas ao imenso conjunto heterogêneo e distribuído de grupos e indivíduos que agem politicamente, em conjunto ou de forma descoordenada, valendo-se do termo "Anonymous" em várias partes do mundo. E todas elas, de alguma forma, mostram-se apropriadas.

Por se tratar de um objeto tão *sui generis*, as dificuldades em pesquisá-lo começam por sua própria definição. Quem são os Anonymous? E, mais especificamente, o que eles são? De fato, conforme observou Coleman (2011), os Anonymous resistem a uma definição mais direta e pontual. Isso porque, ao menos em tese, trata-se de um nome frequentemente utilizado por diferentes grupos, munidos de diferentes ideais, em diferentes partes do mundo. Tais grupos, por sua vez, não raro se engajam em operações desconectadas umas das outras, promovendo, em determinados ambientes virtuais, uma verdadeira celeuma, regada sobretudo com ações diretas que vão desde a mera trollagem[25] até protestos políticos mais sérios.

Este capítulo se dedica a traçar uma caracterização, ainda que mínima, da vertente brasileira dessa autointitulada legião. No entanto, para fazê-lo de modo apropriado, é indispensável recorrer aos fatos mais marcantes desse coletivo em seu âmbito internacional, do qual surgiram os primeiros nichos genuinamente brasileiros.

O início dessa história, se é que é possível identificá-lo, está no polêmico fórum de imagens norte-americano 4chan,[26] pois é nele que emerge boa parte da base cultural e social sob a qual os Anonymous se mantêm. Criado em 2003 pelo também norte-americano Christopher Poole, então identificado apenas como *moot*, seu *nickname*, o 4Chan rapidamente se tornou um dos espaços mais esdrúxulos, ofensivos e plurais da rede mundial de computadores. Atualmente, conta com mais de 5 dezenas de subfóruns, cobrindo tópicos que vão desde desenhos japoneses, passando por cuidados com saúde e até material adulto. Seu principal fórum – o /q/ ou "aleatório", que serviu como a "casa" não oficial dos Anonymous – é freneticamente alimentado com humor negro, insultos de toda sorte e uma boa dose de pornografia.

Uma das principais características do 4Chan é justamente o anonimato. Ao contrário de uma infinidade de sites que fomentam a comunicação identificada e autentificada entre seus visitantes, no 4Chan não se exige que os usuários se cadastrem, utilizando seus nomes, e-mails ou fotos verdadeiros. Ao contrário, a cultura criada por seus frequentadores desencoraja

25 Cf. nota 8.
26 O fórum pode ser acessado por meio do endereço: <http://4chan.org>. Acesso em: 11 nov. 2011.

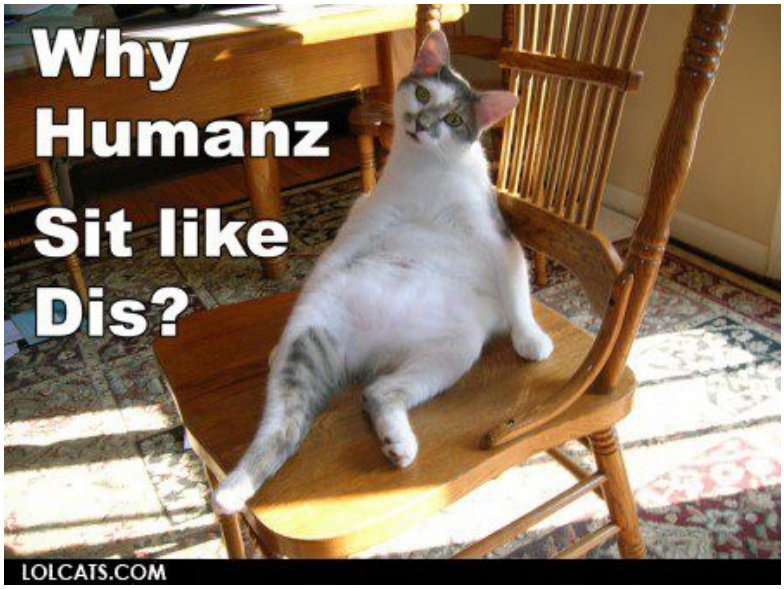
qualquer um a fazê-lo. Tanto que, por padrão, ao enviar qualquer mensagem, o nome sugerido para quem o faz é justamente "Anonymous" (anônimo). Daí o termo que passou a ser adotado pelo coletivo.

Assim, sem qualquer barreira de entrada, uma infinidade de Anonymous inunda o 4Chan a cada minuto com postagens que, dali a algumas horas, serão totalmente removidas do servidor do site. Ou seja: além de não pedir que os usuários se cadastrem, o fórum tampouco mantém qualquer registro do que houve ali. Isso levou a uma característica muito venerada entre os Anonymous: quaisquer que fossem as ações, estas seriam avaliadas com base em seu próprio conteúdo, sem que se levasse em conta quem as realizou ou a posição deste em meio aos demais (LANDERS, 2008) – influência de um dos traços mais eminentes da cultura hacker: a meritocracia. Com isso, à medida que o fórum crescia, seus membros cada vez mais abdicavam de suas identidades pessoais, passando sistematicamente a adotar uma personalidade compartilhada. Assim, "Anonymous", enquanto pseudônimo, prevenia seus membros de serem taxados individualmente como ridículos ou de serem acusados por quaisquer de suas ações (HALUPKA, 2011).

Esse ambiente de comunicação pretensamente livre aos poucos impulsionou a adoção de uma linguagem "que parece haver reduzido o inglês a um monte de epítetos maldosos, zombarias e mensagens de texto abreviadas" (COLEMAN, 2012, p. 92). Esse léxico facilmente distinguível levou à criação e propagação de uma infinidade de memes,[27] que rapidamente se somaram à base cultural dos Anonymous – talvez os mais conhecidos até o momento tenham sido os *lolcats*, imagens que combinam uma fotografia de um ou mais gatos em poses engraçadas ou constrangedoras com uma frase escrita em um inglês macarrônico, tal como observado por Coleman e conforme exemplo abaixo:

27 Termo criado por Richard Dawkins em seu livro *O gene egoísta*, argumentando que o meme está para a memória assim como o gene para a genética: trata-se da mínima unidade.

IMAGEM 1 – Exemplo de Lolcat



Os *lolcats* encarnam vigorosamente o princípio do *lulz*, que se tornaria ao mesmo tempo, ainda de acordo com Coleman (2012), o *ethos* e o objetivo dos Anonymous. Corruptela da abreviação LOL (*laugh out loud* ou "rir em voz alta", em tradução literal), o *lulz* é a máxima expressão da zombaria, da perversão e do espírito brincalhão que impera entre os habitantes do 4Chan (NORTON, 2011). Por sua vez, intimamente ligado ao *lulz*, está a arte de trollar (do inglês *troll*), uma espécie de bullying cibernético. Entre os mais eméritos exemplos de trollagem no 4Chan, destacam-se: sucessivos e não pagos pedidos de pizza para a casa de determinada pessoa-alvo; trotes telefônicos; vazamento de informações pessoais, frequentemente comprometedoras; ações de negação de serviço (DDoS), tirando sites do ar; ameaças não cumpridas de bomba etc.

Essas ações, conhecidas como *raids* – ataques sucessivos e coordenados contra determinado alvo – se davam principalmente em retaliações bem humoradas e sórdidas a organizações ou pessoas que, de alguma forma, incomodavam os habitantes do 4Chan. O *lulz* atuava como um princípio norteador dessas trollagens, que pelo menos desde 2006 são orquestradas de modo mais ou menos coordenados no fórum por indivíduos identificados como Anonymous.

Para Underwood (2009), os Anonymous se basearam fortemente nessa cultura dos memes e do *lulz*, que se tornou uma linguagem comum e passou a servir como uma indicação funcional do status dos seus participantes – uma espécie de capital cultural. Nesse mesmo

sentido, Halupka (2011, p. 37) afirma que o conhecimento dos memes e dessa linguagem comum permitiu que indivíduos interagissem efetivamente com o coletivo mais amplo dos Anonymous. "Essa base cultural dos Anonymous contribuiu para um senso comum de solidariedade, apesar das características centradas no anonimato". Isso porque, não muito tempo depois, o *lolspeak* e os memes passariam a se popularizar paulatinamente, chegando a outros espaços da rede.

Depois de um bom tempo agindo dessa forma no 4Chan, em 2008, um ato que seria aparentemente como os demais – isto é, *for the lulz* – tomou proporções até então inimagináveis e transformou os Anonymous em um movimento também (ou principalmente) político, passando "do *lulz* à ação coletiva", conforme afirma Coleman (2011). Isso se deu em razão do Projeto Chanology[28] – ou Operação Chanology (#OpChanology) –, que consistiu em uma série de *raids* e protestos presenciais contra a Igreja da Cientologia norte-americana. Fato é que a #OpChanology alteraria permanentemente a natureza do coletivo Anonymous.

Underwood (2009) relata que tais *raids* se iniciaram como boa parte das ações que eram orquestradas pelo 4Chan. Neste caso, seguindo vários relatos de que a Igreja adotava uma postura muito rígida com seus ex-membros que se opunham abertamente a suas práticas doutrinárias, inclusive movendo processos judiciais contra eles, os Anonymous viram uma oportunidade para uma boa dose de entretenimento. Afinal, nada melhor do exercer o *lulz* provocando uma instituição que, por certo, reagiria com violência se acossada.

A ocasião perfeita não tardou a chegar. Um vídeo em que o ator Tom Cruise falava, entre outras coisas, sobre as suas bem-sucedidas experiências decorrentes das práticas da Igreja foi publicado por alguns sites norte-americanos. Alegando que o conteúdo[29] era destinado apenas à divulgação interna, os cientologistas ameaçaram processar os sites que não retirassem o vídeo do ar. Isso, em tese, violaria um dos princípios que os Anonymous forjariam a partir de então: a liberdade de expressão, sobretudo na Internet. Com isso, assim que a Igreja confirmou as ameaças, em janeiro de 2008, os Anonymous empenharam-se em uma "difamação ultracoordenada" (COLEMAN, 2012) envolvendo: ações DDoS para derrubar os sites da Igreja; diversos pedidos de pizza não pagos para as suas unidades localizadas nos Estados Unidos; envio de imagens pornográficas para seus faxes, congestionando suas linhas; uma infinidade de trotes telefônicos etc. Poucos dias após a

28 Junção das palavras "Chan" (de 4Chan) e "ology" (de Cientology).
29 Disponível em: <http://www.youtube.com/watch?v=fbTKHDyCdbE>. Acesso em 7 dez. 2011.

primeira onda de *raids*, em 21 de janeiro, membros do coletivo publicaram um vídeo[30] intitulado "Mensagem à Cientologia", no qual declararam guerra à instituição, atestando que suas práticas estavam em desacordo com os "princípios morais" do coletivo, conforme transcrição abaixo:

> Olá, líderes da Cientologia. Nós somos Anonymous. Ao longo dos anos, nós os temos observado. Suas campanhas de desinformação; sua supressão das dissidências; sua natureza litigiosa; tudo isso chamou a nossa atenção. Com o vazamento do seu último vídeo-propaganda em circulação *mainstream*, a extensão da sua influência maligna sobre aqueles que confiaram em vocês como líderes tornou-se clara para nós. Os Anonymous decidiram, portanto, que sua organização deve ser destruída. Para o bem dos seus seguidores, para o bem da humanidade, *e para a nossa própria diversão*, nós faremos com que vocês sejam expelidos da Internet e vamos desmantelar sistematicamente a Igreja da Cientologia em sua forma atual. Nós os consideramos como um sério adversário, e não esperem que nossa campanha seja finalizada a curto prazo. No entanto, vocês não prevalecerão para sempre contra as massas furiosas do corpo político. Sua escolha de métodos, sua hipocrisia, e a precariedade geral de sua organização fizeram soar seu sino da morte. Vocês não podem se esconder. Nós estamos por toda parte [...] (LANDERS, 2008, grifo nosso).

E finalizam com a clássica assinatura adotada até hoje pelas ações em nome do coletivo: "Nós somos Anonymous. Somos uma legião. Não perdoamos. Não esquecemos. Aguardem-nos!". Àquele momento, o coletivo já passava a contar com um sem-número de adeptos que se aproximaram dele em função dos protestos contra a Cientologia e, em sua maior parte, desconheciam as origens e as fundações culturais dos Anonymous. Independente disso, a mensagem se espalhou rapidamente.

Um novo vídeo, postado uma semana depois e intitulado "Chamada para a ação" tentava convocar os apoiadores (ou Anons) para uma primeira tentativa de protesto em massa que excedesse os limites do ciberespaço e ganhasse as ruas. Com isso, em 10 de fevereiro de 2008, cerca de 7.000 pessoas protestaram em frente a sedes da Igreja da Cientologia em mais de 93 cidades do mundo (Underwood, 2009). Embora em uma nova fase de engajamento político, o princípio do *lulz* permaneceu durante a operação Chanology. Além de estar presente na "Mensagem à Cientologia" (a operação também seria realizada "para nossa própria diversão"), ele acompanhou vários dos manifestantes nas ruas, que se vestiam de modo totalmente irreverente, com fantasias, máscaras e demais adornos. E, cerca de um mês depois, uma nova onda de manifestações foi convocada, levando entre 7 e 8 mil pessoas às

30 Disponível em: <http://www.youtube.com/watch?v=JCbKv9yiLiQ>. Acesso em: 11 nov. 2011.

ruas, à maneira do primeiro protesto (Landers 2008).

São nos protestos contra a Cientologia que o uso da máscara que imita o rosto de Guy Fawkes[31] passou a se tornar outra marca do coletivo. Aqueles que não a usavam, em um primeiro momento, não deixaram de cobrir seus rostos com lenços e máscaras de gás. Tudo para enfatizar o caráter anônimo e a identidade coletiva que, mais tarde, seriam sintetizados em outro slogan não oficial dos Anonymous: "Unidos como se fôssemos um; divididos por zero" (tradução literal para: *United as one; divided by zero*).

A #OpChanology, além de marcar a ascensão dos Anonymous como um movimento político – "o Anonymous havia emergido de seu santuário online e se disposto a melhorar o mundo" (COLEMAN, 2012, p. 97) –, também levou a dois outros fatos relevantes. Primeiro, com a onda de novos apoiadores, os ideais do coletivo ultrapassaram, e muito, os limites do 4Chan e ganharam vários outros espaços na Internet. Daí começam a se organizar as primeiras redes no IRC,[32] além do surgimento de vários sites e perfis em redes sociais identificados com os Anonymous. Estava claro que, ante um fenômeno em ebulição, o 4Chan se tornara pequeno demais.

Em segundo lugar, a entrada massiva de apoiadores que, em princípio, não tinham conhecimento das origens do coletivo levou a uma série de discussões internas em diversos canais de comunicação, com a emergência de duas grandes correntes em meio à infinidade de grupos identificados como Anonymous. Halupka (2011) os chamou de Puristas, por um lado, e Moralistas, por outro. Enquanto aqueles defendiam que o coletivo deveria voltar ao seu submundo da rede e seguir agindo unicamente *for the lulz*, eximindo-se das ações morais, estes reivindicavam a então incipiente veia política do coletivo, defendendo que os protestos não poderiam parar por ali. Como ocorreria em muitas das ocasiões vindouras, essa tensão foi encarada com naturalidade pelo coletivo, cujos apoiadores sempre respeitaram o uso extremamente variado, e para as mais distintas finalidades, da marca "Anonymous".

Após os dias mais fortes de protestos da #OpChanology, parte dos Anons seguiu lutando contra a postura da Cientologia, engajando-se com um movimento previamente estabelecido de ex-membros da Igreja que já realizavam campanhas contra ela. Outra parte voltou ao 4Chan e às habituais trollagens. E, ao mesmo tempo, muitos apoiadores que tiveram a primeira experiência em nome do coletivo se dispersaram por diversos espaços da rede, atuando em separado e, por vezes, em questões pontuais.

31 Cf. nota 6.
32 Cf. nota 11.

Dois anos após a #OpChanology, outra grande operação, de uma vez por todas, tornaria os Anonymous conhecidos mundialmente e os transformaria em um relevante ator político internacional, recebendo a atenção e a hostilidade de empresas, instituições e governos de várias partes do mundo.

Tal operação se forjou quando outra vertente dos Anonymous deflagrou uma retaliação, novamente sem muita previsão ou planejamento, quanto a ações DDoS do software Airplex contra vários sites de compartilhamento de *torrents*, em especial o Pirate Bay, a pedido de várias empresas da indústria cinematográfica indiana de Bollywood. A intenção primeira era atacar diretamente o Airplex, mas um grupo independente começou agindo antes da hora, derrubando o site prematuramente (HAPLUKA, 2011). Com isso, em setembro de 2010, os Anonymous mudaram seu alvo e passaram a atacar, em forma de protesto, sites de empresas e organizações que representavam, de alguma forma, a indústria do *copyright*, tais como: a Motion Picture Association of America (MPAA) e a International Federation of the Phonographic Industry.

Dois meses mais tarde, em dezembro de 2010, o alvo principal do coletivo mudaria. Isso se deu quando, cedendo a pressões do governo norte-americano, empresas como a Amazon, a PayPal, a MasterCard, a Visa e o banco suíço PostFinance pararam de prestar serviços à organização Wikileaks – capitaneada pelo jornalista e ativista australiano Julian Assange –, congelando sua conta bancária, interrompendo as doações endereçadas a ela e tirando do ar seus servidores. Diante disso, alguns hackers Anons passaram a chamar a #OpPayBack de Operação Avenge Assange e iniciaram uma onda de ações DDoS contra tais empresas, tirando alguns de seus sites do ar e causando prejuízos de alguns milhões de dólares. Naquele momento, "os Anonymous mostraram ao mundo que era um movimento que deveria ser levado a sério, e que poderia dar suporte às suas reivindicações com uma eficiência técnica devastadora" (HAPLUKA, 2011, p. 53).

Após a #OpPayBack, os Anonymous já atuavam como uma fluida, heterogênea e distribuída rede de células independentes que, ao agir, variavam em metodologia, alvos e ideais. Seu caráter múltiplo e diverso, a cada dia, fomentava novas formas de ação e de engajamento políticos. Após tal operação, a história do movimento em nível internacional seguiu seu curso, de modo que adeptos do coletivo se veriam envolvidos em vários dos grandes acontecimentos políticos vivenciados pelos Estados Unidos e por outros países do mundo – como, por exemplo, o vazamento de informações da empresa HBGary, cujas práticas

ilícitas motivaram um pedido de CPI no Congresso norte-americano; o movimento *Occupy Wall Street*, que teve repercussões em diversos cantos do globo, incluindo o Brasil; e a assim chamada Primavera Árabe, que levou à queda de vários regimes em países norte-africanos.

A partir desta etapa, no entanto, o movimento internacional fica a cargo dos analistas e acadêmicos que passaram a acompanhá-lo sistematicamente. Voltaremos nossas atenções, então, à vertente brasileira dos Anonymous, com suas primeiras apropriações, seu ápice e as principais expressões verificadas atualmente.

3.2 NO BRASIL: PRINCIPAIS APROPRIAÇÕES

Anteriormente às duas etapas da Operação PayBack, não era de todo incomum encontrar brasileiros – hackers de computador, em sua maioria – atuando em apoio à ideia Anonymous, muito em função de suas participações, eventuais ou sistemáticas, nos principais canais de comunicação ligados ao coletivo, sobretudo no 4Chan e em servidores internacionais de IRC. Por isso, quando se forjaram os primeiros coletivos genuinamente brasileiros identificados com os Anonymous no país, é possível afirmar que uma parte dos indivíduos que os compunham já atuavam, principalmente por meio do ativismo hacker, em operações deflagradas por norte-americanos ou cidadãos de outros países do mundo. Tal atuação, contudo, fazia-se mormente individual e esporádica, contribuindo sobretudo com ações pontuais.

A #OpPayBack é responsável por mudar este cenário. Por conta de sua expressão e repercussão, em especial após o envolvimento das retaliações à organização Wikileaks entre os motivos de protesto, vários brasileiros passaram a buscar informações sobre o engajamento em atos de apoio aos Anonymous em vários espaços da web. Um desses espaços privilegiados, que exerceu papel fundamental na criação da vertente brasileira do coletivo, foi o fórum *What is the plan* (WITP).[33]

O WITP ganhou força e inúmeros adeptos notadamente após a Operação PayBack, quando passou a funcionar como um meio de esclarecer dúvidas e centralizar o ingresso de novos participantes. Afinal, embora muitos apoiassem os protestos em massa deflagrados na

33 Originalmente, o fórum podia ser acessado pelo endereço <http://www.whatis-theplan.org>. Atualmente, não está mais ativo.

operação, boa parte das pessoas – incluindo brasileiros – ainda não trazia uma ideia clara de quem/que eram os Anonymous, ou em que/como atuavam. Neste trabalho, classificaremos essas primeiras movimentações de brasileiros identificados com o coletivo como uma fase de **Início**, que será seguida, no decorrer deste texto, pelas fases **Operacional**, **Ápice** e **Dispersão**.

Iniciada entre o fim de 2010 e o início de 2011, esta primeira fase se caracteriza pelas movimentações iniciais dos brasileiros. Ela não envolve, a princípio, nenhuma operação minimamente coordenada. Trata-se, antes disso, de um período de formação dos nichos nacionais, bem como do estabelecimento de suas principais características. Foi naquela época, por exemplo, que a maior parte dos entrevistados para este trabalho passou a se envolver, direta ou indiretamente, com a ideia Anonymous.

Além do fórum *What is the plan*, no qual se abriu uma seção que passou a ser frequentada por brasileiros, logo começaram a surgir os primeiros canais no IRC criados por eles. Inaugurados principalmente – mas não apenas – nas redes AnonOps (irc.anonops.com) e AnonNet (irc.anonnet.org), esses canais figuravam um misto de ações diretas, com grande número de operações e boa dose de hacktivismo, além de outras ações invasivas e não necessariamente políticas (caso, em geral, da AnonOps), e também canais cujos membros estavam também preocupados com a politização das ações e dos novos membros (caso, em geral, da AnonNet). Cabe salientar, no entanto, que tais redes são extremamente híbridas e, por isso, podem comportar espaços que fujam totalmente a essa sistematização.

Um dos locais emblemáticos que se forjaria nesta fase, permanecendo bastante ativo até o final de 2011 e no qual se pôde verificar, durante esse tempo, uma diversidade de atores deveras condizente com o caráter do movimento no Brasil diz respeito ao canal #planbr, pertencente à rede AnonNet. Esse canal tornou-se, em pouco tempo, um dos destinos mais comuns apontados no fórum WITP para aqueles que quisessem, para além de tomar conhecimento da ideia Anonymous, passar à ação: por exemplo, ajudando na difusão do movimento, participando de e promovendo debates, além de se engajar nas diversas operações que estariam por vir. Por conta de sua relevância nesse sentido, o #planbr foi um dos espaços privilegiados para a observação direta por parte deste pesquisador.

Após o período inicial, identificamos que a fase **Operacional** se inicia a partir de meados de julho de 2011. No dia 15 daquele mês, o movimento internacional lançou o vídeo "O Plano: fase 1",[34] no qual se diz que, "fartos com as injustiças e ataques à liberdade

34 Disponível em: <http://www.youtube.com/watch?v=8c1ua7szp1U>. Acesso em: 21 nov. 2011.

ocorrendo pelo mundo", os Anonymous declaravam oficialmente uma guerra contra o "sistema". Nele, o coletivo se apresenta como "uma ideia de liberdade real on-line, tal como na vida real, uma ideia de justiça em defesa dessa liberdade e de um mundo livre de opressão e intolerância". E finaliza o vídeo com um aviso: "A resistência está aqui". Conforme observaram alguns brasileiros que estavam iniciando suas atividades no fórum WITP e no IRC, o vídeo representou um objetivo comum a ser perseguido, e pode-se dizer que foi um dos pontapés iniciais para as atividades no Brasil. Assim, pouco mais de uma semana depois, indivíduos identificados como Anonymous já lançavam uma versão desse conteúdo traduzida para o português do Brasil.

"O Plano: fase 1" fez com que diversos simpatizantes procurassem pelos Anonymous. Pouco a pouco, o #planbr tornava-se cada vez mais populoso, recebendo tanto pessoas que já haviam se identificado com o coletivo, mas atuavam em outros espaços, como também indivíduos que ainda pouco conheciam sobre a ideia, mostrando-se ávidos por informações. Parte dessas pessoas, depois de permanecerem no canal durante certo período, simplesmente não voltavam mais. Outras, no entanto, mostravam seu engajamento e, com o tempo, ganhavam a confiança dos operadores do canal, sendo que algumas delas tornaram-se operadoras também.[35]

Toda a empolgação com "O plano" culminaria com uma das primeiras – talvez a primeira – operações organizadas por brasileiros. Trata-se da Operação Onslaught (#OpOnslaught), realizada em 30 de julho de 2011. A ideia também se deu pegando carona com um vídeo lançado pelo movimento internacional[36] chamando para a mesma operação, cujo objetivo era divulgar a ideia Anonymous tanto pelas ruas quanto nos espaços virtuais. "Diga ao mundo que nós estamos aqui e que nós somos Anonymous. Anuncie nossa posição distribuindo panfletos, adesivos, tags etc. por toda a sua cidade. Todos que estiverem participando nas Ops online irão postar no Twitter, Facebook, Youtube e no Myspace", dizia a voz do vídeo. Na chamada para as atividades, ainda se encorajou o uso de "comunidades e fóruns para se encontrar e se informar com outros membros do local ", uma vez que, "por meio desse esforço, nossa mensagem chegará a um número massivo de pessoas". Conforme algumas pessoas que participaram dessa operação relatariam mais tarde a este pesquisador, o caráter até então inusitado do movimento, combinado à falta de experiência de boa parte dos

35 No IRC, quem define os operadores e demais normas de determinado canal é seu fundador. Logo, cada canal tem seu conjunto específico de regras e seu sistema de reconhecimento e aceitação entre os usuários.
36 Disponível em: <http://www.youtube.com/watch?v=KaQ3ZHzKfbI>. Acesso em: 21 nov. 2011.

indivíduos quanto a ações como aquela fizeram com que as manifestações não atingissem o nível desejado de participação.

Contudo, a partir da #OpOnslaught, os Anonymous brasileiros se já passaram a se engajar em diversas e pequenas operações, deflagradas espontânea e individualmente por vários grupos e indivíduos independentes identificados com o coletivo. Sempre em contato com o movimento internacional, que por diversas vezes auxilou os brasileiros tanto com inspiração ou ideias para ações quanto na hospedagem dos servidores dos sites e do IRC, foram realizadas ações locais, regionais, nacionais e alguma até globais – como, por exemplo, a #OpMegaupload e as operações em apoio à chamada Primavera Árabe.

Também nesta fase, evidenciaram-se mais claramente as duas grandes faces que compunham os Anonymous Brasil. Estas, aparentemente excludentes, sustentaram uma permanente tensão que se faria presente em diversos momentos, tornando-se insustentável ao final de 2011, quando se acentuou o declínio da vertente brasileira do movimento.

A primeira das faces, responsável gerar grande repercussão na imprensa nacional e internacional, é formada apenas por hackers ativistas e tem um caráter mais belicoso. Focada sobretudo na ação, tem como objetivo realizar grandes operações, principalmente por meio do hacktivismo, almejando chamar a atenção dos meios de comunicação. Dessa forma, de acordo com os grupos e indivíduos identificados com essa face, é possível passar sua mensagem de protesto a um maior número de pessoas. Para seus seguidores, a preocupação com a politização das operações e de novos apoiadores não é de todo irrelevante, mas "dispensar muito tempo pensando demais", nas palavras de um Anon, equivale a incorrer em grave erro.

Esta face foi representada mais fortemente pela *LulzSec Brazil*,[37] que, embora não seja o foco deste trabalho, certamente mereceria um capítulo (ou uma dissertação) à parte. Ao contrário dos Anonymous, a *LulzSec Brasil* foi propriamente um grupo fechado de hacktivistas que planejava e executava suas ações de maneira independente. Sempre em contato com seu braço internacional (a *LulzSec*, cujo principal expoente era o hacker Sabu), os brasileiros, por conta de divergências internas, interromperam as atividades entre junho e julho de 2011, mas mantiveram em seu site[38] os *releases* com as principais ações até então realizadas. Dessa forma, parte dos hackers da *LulzSec Brasil* se dividiram entre os grupos *AntiSecBrTeam* e *iPirates*, que, poucas semanas depois, passaram a atuar conjuntamente integrando-se ao movimento dos Anonymous no Brasil. Por conta do caráter de suas

37 Nome derivado da junção das palavras *lulz* e *security*.
38 Ainda disponível em: <http://lulzsecbrazil.net>. Acesso em 6 mar. 2013.

operações, bem como de sua constante repercussão midiática, esta face foi uma das grandes responsáveis pela exposição da vertente brasileira do coletivo, que sempre suscitava o interesse de novos apoiadores.

Atuando paralelamente à primeira, a segunda grande face dos Anonymous brasileiros é formada também por hackers, mas se mostra mais inclusiva e dialógica que a anterior. Muito embora também tenham participado de várias ações hacktivistas, os nichos identificados com esta sempre se mostraram menos preocupados com grandes ações midiáticas. Seu foco, antes de tudo, consistia na constante educação e politização dos apoiadores do coletivo e das ações em que estes se engajavam. Por isso mesmo, uma vasta e heterogênea gama de indivíduos (não apenas hackers) passaram a orbitar em torno desta face. Se, por um lado, estes eram acusados pelos primeiros por "pensar demais", atrasando e, por conseguinte, perdendo o *timing* das ações, também aqui sobravam críticas aos ex-integrantes da *LulzSec Brazil* e seus apoiadores: suas ações seriam demasiadamente precipitadas, sem qualquer politização, e sua suposta necessidade de aparecer na mídia atrapalhava o movimento. Contudo, houve o reconhecimento de que esse tipo de hacktivismo cumpriu um papel fundamental ao divulgar o movimento no Brasil.

Apesar dessas evidentes diferenças de pensamento e metodologia de trabalho, representantes das duas faces conviveram uns com os outros e até realizaram ações conjuntamente pelo menos até dezembro de 2011. Um dos locais privilegiados dessa interação, o canal #planbr, da rede AnonNet, foi o meio de aproximação e, ao fim, de completo desmembramento entre essas duas faces, conforme se verá a seguir.

Passada a fase operacional, é possível afirmar, ao sistematizar o relato de boa parte dos Anonymous brasileiros, que o **Ápice** do movimento se deu em torno das manifestações que se realizaram durante a semana do dia 7 de setembro de 2011 – conhecidas sob os esforços da Operação #ODiaPelaIndependência. Com o intuito de questionar a "verdadeira independência" do povo brasileiro, tendo como mote principal a luta contra a corrupção no país, a operação foi organizada para se realizar pela rede mas, principalmente, fora dela. Com isso, contou com alguns dias de preparação e, durante sua execução, com uma enorme euforia.

Deliberadamente, o foco era promover uma conscientização em relação a estes temas. Em um dos mais acessados vídeos[39] que convocaram a operação, pedia-se que, "no dia da falta independência do Brasil, vamos fazer realmente acontecer essa independência". Noutra

39 Disponível em: <http://www.youtube.com/watch?v=iqn08ivMJZ8>. Acesso em: 11 nov. 2011.

passagem, bem à maneira espontânea que caracteriza a ideia Anonymous, dizia-se: “Se você está a fim de encabeçar o protesto na sua cidade, fique à vontade. Estará ajudando o seu país. Se quiser distribuir panfletos, colar cartazes, sei lá, fazer alguma propaganda desse manifesto em algum canto, você estará nos ajudando bastante”.

Parte do movimento dedicou-se a realizar oficinas para produção de camisetas, *flyers*, panfletos, cartazes etc. Outra parte preferiu atuar pela rede, divulgando informações em blogs e redes sociais. Também se montaram listas de e-mails e telefones com pessoas do meio público, da mídia, e também políticos, para os quais se enviaram diversas mensagens. Embora timidamente, alguns ações hacktivistas também ocorreram. E assim, no feriado de 7 de setembro, em boa parte das capitais brasileiras – e também em algumas cidades do interior – se realizaram marchas, manifestações e panfletagens, nas quais se divulgava o trabalho dos Anonymous, bem como alguns de seus canais de comunicação.

Como resultado, novos apoiadores aproximaram-se do movimento e o #planbr ganhou novos participantes. Um dos Anons que atuou pela rede durante #OdiaPelaIndependência observou que havia “uma euforia gigante. No dia 7 à noite, você só via a hashtag #muitofeliz”. Outra pessoa, que optou por participar dos protestos nas ruas, relatou: “A gente não sabia. Não tinha a menor noção de que ia ter tanta gente em tanta cidade assim. Foi um sufoco, uma emoção”. Posteriormente, diante da apropriação e do uso político desses protestos por parte de alguns partidos políticos – sobretudo conservadores –, algumas pessoas até pensaram em fazer retaliações, mas prevaleceu o consenso de que qualquer um poderia se apropriar da ideia Anonymous.

Se, por um lado, #OdiaPelaIndependência representou o ponto alto dos Anonymous no Brasil, também é possível dizer que, a partir dele, tem-se início uma fase de maior **Dispersão** do movimento, seguida por um declínio na intensidade das atividades. Segundo relatou um Anon que havia participado do movimento desde antes do fórum WITP, ajudando em ações pontuais dos norte-americanos, “nós não estávamos esperando o 8 de setembro. Foi um erro de estratégia. É importante, nesse tipo de ação, manter a poeira levantada. Não pode deixar as coisas caírem na rotina novamente. Uma revolução não é feita em um dia e muito menos em uma manifestação”. Outro Anon, que colaborou esporadicamente com várias das ações fomentadas no #planbr, acredita que “as pessoas começaram a sentir um desânimo natural. É complicado você enxergar que está tudo errado, mas ver que poucos estão se importando. Naturalmente, isso começa a gerar um certo cansaço. E as pessoas vão se desapegando do

movimento".

Com isso, depois de chegar a bater recordes de número de usuários durante #ODiaPelaIndependencia, a frequência no #planbr, aos poucos, caía. Durante os meses seguintes, vários grupos e indivíduos migraram para outras plataformas, formando novos nichos, atuando em outros projetos, e passando a agir de forma independente. Outros simplesmente deixaram de atuar. Fato é que o espírito de cooperação e ação forjado em meio ao 7 de setembro jamais retornaria com tanto gás.

Dois meses depois, a gota d'água para um fatal e derradeiro esfriamento de ânimos ocorreu no mês de dezembro. Mesmo em atrito, as duas faces dos Anonymous brasileiros, ora atuando em conjunto ora independentemente, conseguiam conviver no mesmo espaço, o #planbr. Não obstante, um desentendimento no canal envolvendo um representante de cada uma delas selou o fim de qualquer aproximação ou cooperação futura. Após uma série de retaliações, membros do *AntiSecBrTeam* e do *iPirates* saíram em definitivo daquele espaço, passando a atuar por meio de outras plataformas.

Quase um ano depois, um dos participantes do canal que acompanhou a cisão com certo distanciamento, afirmou: "A coisa, na minha visão, sempre foi bifurcada, as duas vertentes sempre foram bem distintas. Isso [a cisão] aconteceria de qualquer forma". Outro Anon, no mesmo período, expressou uma opinião semelhante: "Precisamos admitir que não dá para trabalhar com todo mundo. São pequenas redes e a gente tem que se ligar. A gente tem que se juntar por afinidade para coisas que são para todo mundo. Mas esse é um entendimento que vem depois. Aconteceu tanta coisa para a gente ter essa clareada!". A cisão, no entanto, mudou o canal. "Meio que o clima pesou. Os ânimos esfriaram. Daí para frente, muito mais gente foi saindo", afirmou um dos hackers indiretamente envolvidos no desentendimento. Com isso, nos primeiros meses de 2012, apenas pouco mais de uma dezena de usuários ainda frequentava o #planbr.

Apesar de terem se dispersado ainda mais, os Anons brasileiros não desapareceram nem tampouco deixaram de atuar. Àquele momento, uma rápida pesquisa nos principais buscadores, ou em redes sociais como Twitter e Facebook, ou mesmo em servidores de IRC permitiria observar ainda dezenas de blogs, sites, perfis em redes sociais, *nicknames* e canais com participação de brasileiros identificados com os Anonymous. E, até meados do ano de 2012, período em que finalizamos a coleta de materiais para este trabalho, ainda se realizariam algumas operações de relevância e grande repercussão, com o uso mais direto do

hacktivismo como forma de protesto.

Nas seções que se seguem, dedicaremos atenção a duas dessas operações: a #OpWeeksPayment e a #OpGlobo.

3.3 #OPWEEKSPAYMENT

A Operação WeeksPayment (ou "semana do pagamento", em tradução literal) foi planejada, organizada e executada pelos grupos *AntiSecBrTeam* e *iPirates*, compostos por boa parte dos ex-membros da vertente brasileira do grupo *LulzSec*, a *LulsSec Brazil*. Reunidos em torno do perfil @AnonBrNews na rede social Twitter, estes hackers – que formariam, após a já referida cisão, um dos nichos mais proeminentes e ativos dos Anonymous Brasil – se engajaram em uma operação totalmente à sua maneira: grandes e vistosas ações de negação de serviço (DDoS), com mensagens veiculadas em diversos canais de comunicação e registros tanto na imprensa nacional como internacional. Embora tenha sido realizada, de fato, entre os dias 30 de janeiro e 3 de fevereiro de 2012, um membro deste nicho reportaria meses depois a este pesquisador que o desejo de realizá-la era algo de longa data. No entanto, antes da cisão, eram aconselhados por outros indivíduos a não realizá-la, alegando que ela carecia de maior fundamentação política e teria como principal feito atrapalhar os brasileiros justo na semana de seu pagamento.

Pois a #OpWeeksPayment consistiu justamente nisto: tirar do ar, entre outros, os sites de 5 dos maiores bancos brasileiros de segunda a sexta, durante a semana do pagamento, quando tradicionalmente ocorre um grande número de operações financeiras por parte dos bancos e seus clientes. Com isso, a cada dia da semana, um banco viu seu servidor inundado por requisições de acesso e, por consequência, tornou-se impossível acessar sua página. Enquanto alguns sites permaneceram fora do ar durante algumas horas, outros voltaram às atividades, mesmo com dificuldades e lentidão, após alguns minutos.

Na segunda-feira, 30/01, o alvo dos hacktivistas foi o banco Itaú, cujo site ficou instável no período da manhã. Na terça-feira, foi a vez do Bradesco. Já na quarta e quinta-feira, os atingidos foram Banco do Brasil e HSBC, respectivamente. Na sexta-feira, o coletivo se responsabilizou por investidas contra os sites da Federação Brasileira dos Bancos

(Febraban), do Banco Central, das operadoras de cartões de crédito Cielo e Redecard, além dos bancos Citibank, BMG e PanAmericano.

Na sexta-feira (3/2), dia em que se encerrou a #OpWeeksPayment, os hacktivistas tornaram claros seus objetivos mais gerais em duas mensagens enviadas pelo referido perfil no Twitter: "Temos condições de causar um caos jamais visto, mas este não é o objetivo do movimento". E, em seguida: "O objetivo é alertar a população sobre o que acontece no país e como ela pode fazer algo para mudar a situação. Isso é ser Anonymous". Embora não se possa precisar se este objetivo foi plenamente atingido, pode-se afirmar que, ao menos quanto à repercussão, as ações chamaram para si bastante atenção. Ao longo da semana, os próprios hackers estabeleceram um contato direto com a imprensa, principalmente via e-mail, e divulgaram um comunicado em áudio,[40] que foi utilizado por diversos veículos de comunicação, incluindo os radiofônicos.

Para a #OpWeeksPayment, os Anons que a realizaram dispensaram qualquer ajuda de apoiadores nas ações hacktivistas. Antes do início da operação, duas postagens no Twitter, escritas em caixa alta, alertavam quanto a isso. No primeiro: "Pedimos a compreensão de todos, nesta missão apenas nosso grupo estará à bordo! Peguem suas pipocas e se acomodem num local confortável!" (sic). Em seguida, reforçou-se: "Por favor não façam qualquer ação para nos ajudar nesta missão! apenas acompanhem e divulguem! =)". Em entrevistas posteriores a este pesquisador, por mais de uma vez, um dos hackers mais ativos na #OpWeeksPayment afirmou que, embora ajude em operações internacionais dos Anonymous, nos atos hacktivistas empreendidos por este nicho, "não precisamos de ajuda, nem pedimos". No entanto, tal pedido restringe-se ao hacktivismo, uma vez que outras formas de apoio são bem-vindas e encorajadas. Por exemplo, espera-se que os apoiadores divulguem as operações e fomentem o debate político gerado por elas nos diversos canais de comunicação.

Nesta operação, ainda foi possível observar a presença marcante de dois dos princípios norteadores deste nicho. O primeiro diz respeito à mensagem de denúncia – frequentemente realizada de forma genérica e sem alvos determinados – da corrupção nos sistemas político e financeiro brasileiros. Não raro, o coletivo divulga nas redes sociais mensagens indignadas sobre atos de corrupção no país, denunciando situações precárias em diversas áreas, tais como saúde, educação, moradia, mobilidade urbana etc. Durante a #OpWeeksPayment, não foi diferente. No quarto dia de operação, por exemplo, ao comentar a opinião de analistas de

40 Disponível em: <http://blogs.estadao.com.br/radar-tecnologico/2012/02/01/ciberataques-continuam-hacker-diz-que-grupo-sera-conhecido-pelo-amor-ou-pela-dor>. Acesso em: 15 jul. 2012

segurança da informação e parte da imprensa, que classificaram a #OpWeeksPayment como uma série de atos criminosos, os Anons protestaram: "#OpWeeksPayment CRIME? Crime é a desigualdade social, é não ter onde morar, o que comer. OTÁRIOS! Porque não criticam os que te roubam?", fazendo referência à classe política e financeira.

O outro princípio norteador presente em peso nesta operação é o *lulz*, tal como descrito anteriormente neste capítulo. Apesar de se mostrar como um protesto coordenado com o objetivo de chamar a atenção para questões políticas e sociais sérias, a #OpWeeksPayment não prescindiu de um espírito brincalhão. Ao longo da semana, à medida que os sites saíam do ar, membros do grupo usaram novamente o Twitter para lançar mensagens provocativas às corporações-alvo. "Marujos venham ver a equipe de TI do @Itau andando na prancha! lol lol lol 'ItáOff' 'TangoPersonalite' 'Tango30H'", postou o coletivo depois de o site do Itaú sair do ar, brincando com dois dos slogans do banco ("Itaú Personalité" e "Itaú 30h") e a expressão "Tango Down", comumente usada pelos Anons no mundo todo depois de uma ação de negação de serviço bem-sucedida. Ao final da operação, dispararam: "Internet: R$150,00 PC: R$1.000,00. Derrubar as duas maiores operadoras de cartão de crédito do país: Não tem preço!", fazendo referência à mensagem publicitária da Mastercard.

Também foi na #WeeksPayment que, de maneira bastante polêmica, este nicho dos Anonymous no Brasil estampou aquele que se tornaria conhecido como um de seus lemas: o de que as pessoas conheceriam as suas ideias "pelo amor ou pela dor". Ainda no áudio divulgado durante a operação, um dos hackers sugeriu que as ações eficientes de protesto eram aquelas que fossem capazes de afetar diretamente a vida da população. "Nossos ataques eram direcionados a sites do governo. Mas isso não está surtindo muito efeito e vimos que a população não está reagindo. Então, decidimos tomar medidas mais extremas para isso. Irão nos conhecer pelo amor ou pela dor". Essa declaração causou certa celeuma entre quem, até aquele momento, estava apoiando a #WeeksPayment. Para estes, o foco da operação deveria ser um protesto contra os sistemas político e financeiro no Brasil, e não o fato de atrapalhar as pessoas durante semana do pagamento.

A principal crítica veio justamente de outros nichos Anonymous no Brasil, que, antes mesmo de seu início, já reprovavam a operação. Esta, aliás, foi incessantemente debatida em canais de IRC e por meio de perfis e páginas em redes sociais. Em função do caráter anônimo, disforme e espontâneo da ideia Anonymous, fatos como este não são de todo incomuns. Pelo

contrário. Não houve registro de nenhuma operação em que o planejamento, a organização ou o método de execução fossem unânimes. Durante a Operação WeeksPayment, a reação mais contundente veio do Plano Anonymous Brasil, um coletivo cujos membros se alinhavam mais à face inclusiva e dialógica dos Anonymous. À época, ainda mantinha ativos o perfil @PlanoAnonBr, no Twitter, e a página Plano Anonymous Brasil, no Facebook. Logo no segundo dia da Operação, o PlanoAnon divulgou um comunicado via Facebook:

> Anonymous não tem como alvo a sociedade, os prejudicados por esta ação, são única e exclusivamente os cidadãos, que estão na primeira semana do mês, semana de volta as aulas, semana de pagamento. […] Esta ação está sendo executada pelo @AntisecBrTeam, @iPiratesGroup e a @Lulzsecbrazil, grupos estes, que se declararam contra o Anonymous abertamente, e estão executando essa ação como tentativa de desmoralizar o coletivo ao qual dedicamos várias de nossas forças a quase um ano. Eles com toda sua necessidade doentia de atenção, decidiram assumir a postura, de que "se não nos respeitam pelo amor, vão nos respeitar pela dor" [sic].[41]

Meses após a operação, vários indivíduos que faziam parte do PlanoAnon relataram a este pesquisador que, embora fosse de comum acordo que qualquer um pudesse se valer da marca Anonymous, isso não o isentaria das mais variadas críticas oriundas do próprio movimento. E foram muitas: “Eu não tenho nada contra nenhuma operação. Se quer atacar o governo, beleza. Quer atacar o banco, beleza. Mas cara, atacar bancos no dia de pagamento prejudica apenas o cidadão. Isso tem nome: burrice”, opinou um dos hackers que se opuseram à operação. Nesse mesmo sentido, outro indivíduo, que colaborou com o movimento brasileiro desde o início, mas em ações que fugiram ao hacktivismo, afirmou: “Alguém acredita que derrubar o site de um banco por 4 min vai realmente trazer pessoas para a nossa causa? Eu diria que é o contrário... Mais e mais pessoas vão nos enxergar como moleques... desordeiros... ”.

No entanto, os responsáveis pelos protestos valeram-se de sua prerrogativa anônima e continuaram com as ações. E, se parte do movimento se opunha a elas, isso não representava sua totalidade. No terceiro dia de operação, por exemplo, outra página no Facebook, identificada como Anonymous Rio, se contrapôs as críticas à #OpWeeksPayment:

> [Anonymous] é uma ideia ou um conjunto de ideias sempre em construção,

41 Comunicado disponível em: <https://www.facebook.com/PlanoAnonymousBrasil/posts/291464640918163>. Acesso em: 15 jul. 2012.

> transformação, mutação e adaptação. Não existem cartilhas, centros, grupos, pessoas ou qualquer outra coisa que possa falar por Anonymous, todos podem falar por si. Ninguém pode falar por todos. Não existem lideranças e TODOS TEM QUE SER LÍDERES. Em resumo, você pode ser Anonymous, mas JAMAIS vai ser da Anonymous, pois isso não é um grupo [...] O que valida uma Op é pura e simplesmente adesão. Não existem operações oficiais, reais, verdadeiras nem nada do gênero. Existem pessoas que concordam e pessoas que discordam. […] Somos contra o sistema vigente? Acho que sim. Uma coisa é certa, se vamos atacar o sistema e se estamos imersos nele TAMBÉM VAMOS SER AFETADOS! Então se é isso que queremos temos que arcar. [...] E os bancos vão continuar a cair essa semana! [sic][42]

Enfim, o debate sobre a #OpWeeksPayment exalta ânimos de grupos e indivíduos identificados como Anonymous até a data de finalização deste trabalho, após mais de um ano do ocorrido.

3.4 #OPGLOBO

A Operação Globo, realizada entre os dias 2 e 10 de abril de 2012, sobretudo entre o feriado da Paixão de Cristo e o domingo de Páscoa, forjou-se bem à maneira Anonymous: um pequeno grupo de pessoas teve uma ideia, lançou uma operação e esperou por possíveis adesões de grupos e indivíduos Anons espalhados pela rede. E, tão logo foi declarada encerrada, viu seus apoiadores dissiparem pela rede e seus canais de comunicação serem descontinuados.

Durante as ações que compuseram a #OpGlobo, dois desses canais irrefutavelmente se sobressaíram: de um lado, a rede social Twitter, por meio do perfil criado especificamente para a operação (@OpGlobo), bem como de outros vários perfis dos realizadores ou apoiadores dela – por exemplo, @Havittaja, @AnonIRC e @AnonopsPB, entre outros; por outro, o IRC, principalmente por meio do canal #OpGlobo, criado apenas para essa operação na rede VoxAnon (irc.voxanon.net).

Entre as postagens no Twitter, boa parte divulgava os sites que haviam sido derrubados (ver abaixo) e, em sua maioria, apontavam para o canal no IRC onde as conversas estavam sendo realizadas. Outras, ainda, esforçavam-se para politizar as ações por meio da divulgação

42 Comunicado disponível em: <https://www.facebook.com/permalink.php?story_fbid=310540125663009&id=231139103603112>. Acesso em: 15 jul. 2012.

de links que direcionavam, por exemplo, para o documentário “Muito além do Cidadão Kane” – produção britânica assinada por Simon Hartog – ou para cartazes e manifestações de rua contra a TV Globo, frequentemente com as frases: “O povo não é bobo”, ou ainda “Você está sendo manipulado”, ao lado do logotipo da emissora. Ainda por meio do Twitter, foi possível observar o apoio de perfis internacionais com altíssima influência e número de seguidores, tais como @YourAnonNews, @Anon_Central e @AnonymousWiki. Cada um dos três divulgou a operação ao menos uma vez e mencionou os sites que estavam sendo derrubados naquele momento.

O número massivo de tweets que direcionavam os Anons apoiadores para o IRC levou ao canal #OpGlobo bem mais que uma centena de pessoas, um número considerável tendo em vista que o canal fora criado havia pouco tempo e que se estava em meio a um feriado prolongado. Mesmo assim, o canal fervilhou de mensagens de todo tipo – tanto é que os *logs* (registros) de atividades, apenas nos três principais dias da Operação, entre 5 e 7 de abril, preencheram nada menos que 150 páginas de um editor de texto nas configurações padrão.

Ao chegar ao #OpGlobo, a primeira mensagem que o usuário recebia, tal como em qualquer canal do IRC, era seu tópico. Nele, os organizadores das ações colocavam os sites-alvos (a serem derrubados) do momento, de modo que, quem quisesse ajudá-los a manter as páginas fora do ar, já poderia se guiar apenas por aquela mensagem. Já aqueles que quisessem apenas divulgar a operação ou conversar com quem estava envolvido nela, podia se juntar ao chat público do canal, ou mesmo enviar mensagens privadas.

Aqueles que chegavam ao canal por meio de uma mensagem Twitter, sem ter acompanhado previamente a operação, logo se deparavam com uma avalanche de mensagens de todo tipo. Nos dias mais ativos da #OpGlobo, era possível observar desde indivíduos totalmente perdidos, pedindo “eu kero ser um rarcker”, até mesmo hackers estrangeiros perguntando pelos detalhes da operação e oferecendo ajuda. A madrugada entre os dias 5 e 6 de abril, por exemplo, foi tomada por uma rara euforia. Mesmo os Anons que frequentavam o IRC havia mais tempo se surpreenderam com a quantidade de usuários frequentando o canal. Antes da meia-noite, quando seria divulgado o próximo alvo, pululavam várias mensagens ansiosas, com perguntas ou sugestões aos participantes do #OpGlobo. “Preparem os canhões!”, exclamou um dos Anons, seguido por diversos outros.

Assim, quando se optou pela ação contra os sites da Fundação Roberto Marinho (http://www.frm.org.br, http://www.fundacaorobertomarinho.com.br e http://www.fundacao-

robertomarinho.org.br), ONG pertencente às Organizações Globo, novas postagens eufóricas se fizeram, ora conclamando a todos para o "ataque", ora reforçando os desvios supostamente praticados pela emissora, tais como manipulação deliberada da opinião pública e indevida dedução de impostos por meio do projeto Criança Esperança. Naquele dia, a página da Fundação esteve fora do ar até pouco depois das 4h. E, ao passo que outras ações se realizavam ao longo da semana, participantes do #OpGlobo propunham pequenas ações paralelas e, para isso, juntavam-se em pequenos nichos de hackers.

Ao final, a Operação Globo consistiu em uma série de ações de negação de serviço[43] contra diversos sites ligados às Organizações Globo, conforme um comunicado publicado em uma aplicação web de compartilhamento de textos:[44]

> Olá a todos Anonymous, simpatizantes, e qualquer outra classificação que possa existir. Iniciamos uma grande operação. Cansados da manipulação da Globo, estaremos lançado a #OpGlobo. Objetivo: Sites do subdominio: globo.com. Por isso contamos com a ajuda de todos que estão lendo essa mensagem, com divulgação ou até mesmo ataques aos websites. Deixando claro a oposição não queremos censurar a mídia. Os próximos passos da operação estarão sendo dadas no twitter […] O que precisara ser feito neste ataque: Ataques em massa. Organizações em IRC ou Similares. NÃO USEM botnets com pessoas infectadas (banalizamos esse tipo de ato). [sic]

No referido comunicado, os Anons ainda passaram a atualizar o texto à medida que as páginas saíam do ar, apontando as referidas páginas e o tempo em que haviam permanecido inacessíveis, conforme sistematizamos na tabela abaixo. Como, ao longo da semana, as atualizações não se tornaram regulares, outros sites que também saíram do ar, como o da Turma da Mônica e do canal Futura, não constam entre os demais.

TABELA 2: Sites derrubados na #OpGlobo

Página	**Tempo inacessível**
corp.editoraglobo.globo.com	1h30
editoraglobo.globo.com	1h30
telecine.globo.com	3h

43 Paralelamente às ações de negação de serviço, houve dois outros atos como pano de fundo da #OpGlobo. O primeiro foi um *defacement* realizado em um site da rede Record, em retaliação a uma notícia postada em um dos blogs do portal R7. Nessa notícia, dizia-se que a Internet mundial estava ficando mais lenta, e que isso, provavelmente, seria culpa dos Anonymous. A outra ação diz respeito ao vazamento de algumas mensagens do e-mails do jornalista Caco Barcellos, da TV Globo. No entanto, nenhuma delas teve grande repercussão.

44 Trata-se do "Paste HTML: free anonymous HTML hosting". O link do comunicado, que não está mais ativo, podia ser acessado pelo endereço: <http://pastehtml.com/raw/btg72yyul.html>. Acesso em: 15 abr. 2012.

telecine.com.br	3h
assine.globo.com	15 minutos
somlivre.com	4h
somlivreshop.com	4h
escute.com	4h
caldeiraohiphop.com	4h
kellykeypassaporte.com	4h
rge.com	4h
musiq.com	4h
stagerio.com	4h
globoir.globo.com	3h
bbbpayperview.globo.com	1h30
canaisglobosat.globo.com	1h30
envio.gnt.globo.com	1h30
globosatcomercial.globo.com	1h30
globosathd.globo.com	1h30
loki.canalbrasil.globo.com	1h30
megapix.globo.com	1h30
mundomega.megapix.globo.com	1h30
pfci.globo.com	1h30
sociopremiere.globo.com	1h30
movieboxbrazil.com.br	1h30
fundacaorobertomarinho.com.br	4h

A #OpGlobo também não prescindiu do espírito do *Lulz*. Tanto nos comunicados via Twitter como nas conversas pelo IRC, entre as mensagens de protesto, logo se viam chacotas de todo tipo. Por exemplo, no terceiro dia de Operação, um dos perfis postou no microblog: “Me chama de Rede Globo e me deixa te manipular todinha, sua linda!”. E, horas mais tarde: “A minha vó acabou de cair - TANGO DOWN!" :: Foram os Anonymous!”. Também no IRC, em plena madrugada de ataques, no dia 6 de abril, participantes do #OpGlobo perguntavam-se se não seria um pecado muito grande atacar alguém durante uma sexta-feira santa, conforme diálogo abaixo:

<AnonA> mano jesus morreu hj

<AnonA> dai ele renasce na páscoa
<AnonB> putz, eh mesmo. Não devíamos fazer DDoS em dia santo!!! Eh pecado
<AnonA> fazer mal a alguém num dia santo
<AnonC> kkk
<AnonA> tbm depende da religião da pessoa
<AnonB> ah eh verdade. Judeus podem fazer DDoS [sic]

Como é de praxe, a #OpGlobo não foi unânime entre os Anonymous brasileiros. Enquanto ela acontecia, um vídeo postado no YouTube, mas removido poucos dias depois, questionava os fundamentos morais e políticos da Operação. O maior questionamento entre os Anons baseou-se em um regra tácita, que já havia algum tempo era seguida pela maior parte do movimento internacional: a de que, independentemente do que houvesse, os Anonymous não atacariam meios de comunicação, até mesmo em países em que eles fossem controlados e manipulados pelo governo, uma fez que isso feriria a liberdade de informação, uma das clássicas (e também tácitas) bandeiras do coletivo. “Foi um monte de ataque sem sentido. Só ataca, sem passar nenhuma mensagem”, um Anon disse a este pesquisador alguns meses após a Operação. Sobre o preceito de não se atacar a imprensa, outro Anon opinou: “Inicialmente, seria burrice mesmo. A melhor arma da imprensa (ao contrário do que pensam muitos) é o desprezo. A imprensa pode queimar seus atos, porém te desprezar é muito pior. Então atacar a imprensa é burrice. Eles te ignoram e você sai perdendo”.

Por sua vez, os apoiadores da #OpGlobo lembraram que, em nenhum momento, voltaram-se contra os sites noticiosos da Globo, uma vez que os ataques foram investidos em páginas unicamente comerciais. Isso também foi debatido no IRC: após alguns dias de Operação, alguns Anons propuseram que as ações se tornassem mais ousadas, direcionadas, por exemplo, ao portal http://globo.com. Imediatamente, um dos hackers organizadores disse: “SEM ATAQUES À GLOBO.COM. Globo.com é um portal de notícias gente!” [sic]. Dessa forma, mesmo em meio a críticas, os protestos se seguiram, e o último registro de ação data de 10 de abril.

Pouco tempo após a realização da Operação Globo, o canal #OpGlobo, da rede VoxAnon, não existia mais, e parte dos perfis que o divulgaram no Twitter foram descontinuados – incluindo o próprio @OpGlobo.

*****

As duas operações aqui relatadas – a #OpWeeksPayment e a #OpGlobo –, aliadas ao breve histórico do movimento no Brasil, permitem-nos observar e traçar, mesmo que em linhas gerais, as principais formas por meio das quais os Anonymous brasileiros se engajam politicamente, bem como os desdobramentos disso. Passaremos a fazê-lo no próximo capítulo.

4 ENGAJAMENTO POLÍTICO

No capítulo anterior, este trabalho recuperou os principais fatos que compuseram o início da trajetória dos Anonymous em nível internacional, até o momento em que sua história cruzou com o princípio do coletivo no Brasil – no bojo da Operação PayBack (#OpPayBack), ao final do ano de 2010. A partir de então, traçou-se um breve histórico, dividido em quatro fases, apontando alguns dos principais atos envolvendo a imensa rede heterogênea e difusa de indivíduos e grupos brasileiros identificados com os Anonymous para, dessa forma, relatar e descrever, de modo mais específico, dois dos grandes episódios em que diferentes nichos se engajaram para planejar e executar atos políticos distintos: as Operações WeeksPayment (#OpWeeksPayment) e Globo (#OpGlobo).

Isto posto, acreditamos ser possível ter reunido informações, indagações e reflexões suficientes para esboçar, nas linhas que se seguem, alguns pontos que auxiliem na discussão da principal questão que motivou e guiou esta dissertação até o momento – a saber, o modo como o coletivo Anonymous se engaja politicamente. Para além disso, convém destacar algumas breves reflexões acerca de questões teóricas que, de um modo geral, a julgar pelas evidentes e ora intransponíveis limitações deste trabalho, naturalmente passaram à margem da pesquisa.

Caminhemos, portanto, cercando a questão central: como os Anonymous se engajam politicamente?

4.1 PROMOVENDO O ANONIMATO

Para o ideário Anonymous, a questão do anonimato é entendida, ao mesmo tempo e em diversas situações, sob diferentes aspectos: como um ideário, uma forma de se defender, um modo de se engajar coletivamente etc. Mas, acima de tudo, trata-se da melhor maneira que o coletivo encontrou para compartilhar efusivamente uma identidade coletiva capaz de angariar uma legião de colaboradores que não necessitasse de identificação, conhecimento prévio ou quaisquer credenciais formalizadas para agir politicamente.

Em certo sentido, tal caráter anônimo dialoga com um preceito fundamental da cultura hacker: o de que um *hack*, uma ação ou uma ideia, sejam quais forem, devem ser valorizados por aquilo que são, e não pelo gênero, etnia, credo, faixa etária ou posição social de quem os formulou ou realizou. Em suma: "vale o que você faz, não quem você é". Isso de mostrou evidente em diversos momentos desta pesquisa – desde o *underground* do 4Chan até as últimas operações analisadas. Em várias das discussões abertas nos canais IRC, cuja finalidade variava entre propor/avaliar operações ou até mesmo refletir sobre os rumos mais imediatos do movimento, muitos dos indivíduos ali presentes não tinham o menor conhecimento sobre quem estava por trás daqueles nicks e, portanto, só poderiam discutir unicamente com base em suas ideias. Além disso, para evitar que se fizesse qualquer identificação nesse e em outros sentidos, vários deles utilizavam múltiplos *nicks* não registrados para acessar os servidores IRC, variando a cada vez que acessavam determinada rede, ou então a cada período regular de tempo. Nesses casos, fazia-se impossível, portanto, utilizar qualquer reputação prévia para influenciar determinada discussão.

Além do mais, o caráter anônimo e frequentemente não identificável do coletivo expressa outra característica política dos Anonymous: a de que ninguém é sobressalente. Sempre que determinado nick tenta se expor mais do que a ideia ou a causa, tende a ser marginalizado pelos demais. O mesmo ocorre com as operações realizadas por usuários que as "assinavam" com seus nicks: são respeitadas, mas com muitas ressalvas. Assim, por acreditar que isso fere a totalidade do princípio de anonimato, boa parte do coletivo opta por simplesmente não trabalhar com pessoas que agem dessa forma.

Esse caráter particular dos Anonymous nos leva também a tecer algumas reflexões acerca do fator identitário. Em *A identidade cultural da pós-modernidade*, Stuart Hall aponta algumas das mudanças conceituais por meio das quais o sujeito Iluminista, pretensamente dotado de uma identidade una, fixa e estável, foi se descentralizando, culminando com o que o autor chamou de "identidades abertas, contraditórias, inacabadas, fragmentadas do sujeito pós-moderno" (2005, p. 46).[45] Um desses descentramentos teóricos diz respeito ao impacto do feminismo, aqui representando tanto uma crítica teórica quanto um movimento social. Assim

45 Nessa obra, Hall trabalha com três concepções de identidade: a do sujeito do Iluminismo, "baseado numa concepção da pessoa humana como um indivíduo totalmente centrado, unificado, dotado das capacidades de razão, de consciência e de ação, cujo "centro" […] essencial do eu era a identidade de uma pessoa" (2005, p. 10-11); a do sujeito Sociológico, que "refletia a crescente complexidade do mundo moderno e a consciência de que este núcleo do interior do sujeito não era autônomo e auto-suficiente, mas era formado na relação com 'outras pessoas importantes para ele', que mediavam para o sujeito os valores, sentidos e símbolos" (Idem, p. 11); e a do sujeito Pós-Moderno, "composto não de uma única, mas de várias identidades, algumas vezes contraditórias ou não-resolvidas" (Ibidem, p. 12).

como os chamados "novos movimentos sociais" – que também compreenderam, por exemplo, as lutas raciais, pela liberdade sexual, movimentos pacifistas e de meio ambiente –, o feminismo apelou, segundo o autor, para a identidade social de seus(suas) apoiadores(as), culminando com o nascimento de uma política de identidade e, por conseguinte, com a formação das identidades sexuais e de gênero. Assim, "o feminismo apelava às mulheres, a política sexual aos gays e lésbicas, as lutas raciais aos negros, o movimento antibelicista aos pacifistas" (Idem, p. 45). Isso resultou em uma politização da subjetividade, da identidade e, sobretudo, do processo de identificação.

Na forma Anonymous, por sua vez, nos é permitido dizer que opera uma política de identidade *sui generis*. Em grande medida, não se apela para a identidade social de seus apoiadores, que são os mais diversos possíveis. Ao contrário, à primeira vista, pode-se afirmar que, para os Anons, a identidade consiste em relegar momentaneamente a segundo plano sua identidade. Isso significa que a identificação com os Anonymous implica adotar uma identidade coletiva e pretensamente consensual em detrimento das próprias individualidades de seus apoiadores, que passam a ser ocultas. Exige que, por alguns instantes, se abra mão destas, às vezes de maneira radical – conforme observou Coleman (2012), a identificação pode se tornar um problema. Dessa forma, faz-se interessante notar que, por um lado, todos fazem parte da ideia Anonymous e, em tese, contam com uma voz ativa sobre ela. Por outro, no entanto, ninguém está habilitado a falar em nome dela, muito menos a representá-la de alguma forma.[46] Por isso, quando colocam a máscara que imita o rosto de Guy Fawkes, os rostos por trás dela são sobrepujados por todo o ideário por ela carregado. Não obstante, ela valeria muito pouco sem essa atuante multiplicidade de rostos.

É por isso que essa identidade se sustenta em uma dicotomia: ela é fraca e forte ao mesmo tempo. Faz-se fraca porque é fluida, flexível, tênue, e sua barreira de entrada é praticamente desprezível. Mas também se faz forte à medida que suas condições encorajam vigorosamente a adesão de novos partidários, mesmo que seja para uma ou outra ação pontual, e pare por aí. E, ao mesmo tempo que os indivíduos se aproveitam da potência de uma legião anônima para atacar, também o fazem ao se defender, uma vez que o anonimato facilita ainda mais a dispersão sem deixar rastros – muito embora se saiba que, em plena sociedade de controle cibernético, esta se mostra uma tarefa humana (e mecanicamente)

46 Na maior parte das entrevistas com este pesquisador, antes de responder a quaisquer questões, os Anons faziam questão de deixar claro que tudo o que diziam representava unicamente sua opinião pessoal, e que aquilo se fazia apenas em nome deles mesmos, e não dos Anonymous Brasil.

impossível. Assim, em uma era na qual os serviços online praticamente obrigam os usuários a se cadastrarem, escancarando as várias facetas de suas identidades para alimentar gigantescos bancos de dados publicitários, a opção pelo anonimato não deixa de ser uma forma de resistência.

Vale ressaltar que, embora essa identidade coletiva anônima frequentemente tente se colocar sobre as individualidades, é preciso ressaltar ela não é unificadora, uma vez que não é capaz (e nem tem o objetivo) de eliminar a diversidade que caracteriza o coletivo. Logo, as individualidades não são, de modo algum, suprimidas. Pelo contrário. Conforme pudemos observar no capítulo anterior, sobretudo à luz dos exemplos práticos no Brasil, os Anonymous não são uma ideia homogênea nem tampouco cegamente unida, mas sim um emaranhado de grupos e coletivos que possuem diferentes pensamentos e metodologias de trabalho, de modo que estes frequentemente são conflitantes uns com os outros. Para atestá-lo, basta ver as inúmeras reações que se sucederam às operações WeeksPayment e Globo. Uma vez propostas, enquanto alguns Anons se engajam em ações de apoio a elas, outros discordaram de seu ideal ou de seu *modus operandi*, passando a criticá-la abertamente e fomentando um debate que, em muitos momentos, parece não ter fim. Além do mais, nada impede que os que se mostram contrários criem seus próprios nichos, suas próprias ações e seus próprios métodos de trabalho. Nesse sentido, os Anons adotam a cultura do individualismo colaborativo, também muito própria à cultura hacker, tal como demonstrou Silveira (2010).

Ao mesmo tempo que optam por esconder suas identidades, colocando-as a serviço de uma identidade coletiva totalmente anônima e difusa, os Anonymous exigem transparência e rigor por parte dos mais variados governos e corporações espalhados pelo mundo – o que leva a outro de seus lemas não oficiais: transparência para eles; privacidade para nós. Nesse sentido, para os Anons, o anonimato é válido como ferramenta política unicamente para os que não estão no poder. Por sua vez, quaisquer Estados ou empresas que tentarem se valer dele para qualquer propósito serão alvos em potencial.

Dessa maneira, é por meio de uma renitente invisibilidade individual que os Anonymous conseguem, em diversos momentos, alcançar uma visibilidade coletiva imensa – o que sugere que, tendo em vista o ideário Anonymous, agir politicamente é, antes de qualquer coisa, agir anonimamente.

4.2 EVANGELIZANDO

Nos movimentos que se dedicam à produção, uso e divulgação de softwares livres, além dos programadores de códigos, dos tradutores (que permitem que uma distribuição ou aplicativo sejam utilizados por mais pessoas no mundo), dos documentadores (que se dedicam a elaborar manuais e tutoriais desses softwares) e mantenedores de sistemas, há uma figura que é fundamental para se captar novos usuários ou colaboradores: trata-se do que se convencionou a chamar de "evangelizadores". Em geral, tal "evangelização" é realizada por colaboradores que se saem bem ao falar em público ou têm um poder de convencimento acima da média. Por isso, são comumente escalados pelas comunidades de software livre para divulgar os trabalhos delas e do movimento em fóruns, congressos, *install fests* ou demais eventos. Via de regra, a chamada evangelização se estende pela rede, com a ajuda de vários membros dessas comunidades postando informações em seus blogs, redes sociais, ou mesmo ferramentas criadas por elas próprias a fim de divulgação.

Analogamente, a julgar pela experiência brasileira, é possível dizer que os Anonymous também se engajam politicamente valendo-se de algumas formas de evangelização – isto é, levando a ideia adiante com o objetivo de que mais pessoas se identifiquem com e trabalhem por ela. Mas, ao contrário dos evangelizadores das comunidades de software livre, estes não o fazem principalmente em eventos presenciais, ou em nome de um grupo. De modo sumariamente anônimo, este trabalho vai se realizando, paulatina e permanente, a cada operação lançada, mas também nas ações triviais do dia a dia do coletivo.

Fato é que, independentemente do nicho em questão, a preocupação com a evangelização parece fazer parte da própria ideia Anonymous. Seja qual for a natureza da operação, o ato de evangelizar invariavelmente estará entre seus objetivos – explícita ou implicitamente. E, de tão importante e decisivo, gera uma série de discussões. Conforme observamos, durante a #OpWeeksPayment, os nichos que se mostraram contrários às ações alegavam que seus realizadores não estavam "evangelizando" da maneira apropriada. Afinal, ao derrubar os sites dos principais bancos brasileiros durante a semana do pagamento, só sobrariam prejuízos à população, de modo que a mensagem que o coletivo transmitia estava inevitavelmente distorcida. Por outro lado, os apoiadores da operação ressaltaram que, sem chamar a atenção das pessoas e dos meios de comunicação, nenhuma evangelização se

mostraria eficaz.

Entre os Anonymous brasileiros, esse debate também se estendeu no tocante à metodologia dos protestos, uma vez que esta se mostra impreterivelmente relacionada à forma como a mensagem é transmitida – em uma palavra, à evangelização. Entre os hackers ativistas, muitos se disseram mais favoráveis aos *defacements* em detrimento das ações de negação de serviço, dado que, ao se desfigurar a página inicial um determinado site, é possível passar uma mensagem de modo muito mais prático e direto do que simplesmente tirando-o do ar. Outros, por sua vez, preferem trabalhar com o hacktivismo no nível dos vazamentos de informações de interesse público, pois estas, quando reveladas, supostamente teriam maior poder de chamar a atenção das pessoas e mobilizá-las. Conforme sublinhou um dos hacktivistas brasileiros que atua junto aos Anonymous desde 2009, quando questionado sobre a melhor forma de se evangelizar: "Todas as formas de ataque só fazem sentido se forem realizadas na hora e momento certo. Tudo tem que ser mensurado. Acho que, muitas vezes, os hacktivistas não planejam. Só fazem. Esse é o erro primário".

A preocupação com essa evangelização também pode ser observada nos diversos produtos midiáticos assinados por indivíduos que se identificam como Anonymous. No capítulo anterior, referimo-nos a vídeos, comunicados em texto e posts em redes sociais que ajudam a ilustrar esta questão. Em boa parte deles, o ato de evangelizar revela-se fundamental, sobretudo quando se está realizando uma operação. Não à toa, não raro apelam para a função emotiva da linguagem, que, combinada a uma pitada de *lulz*, tenta gerar bases comuns de identificação. Também não é à toa o número de perfis, brasileiros e estrangeiros, no Twitter e no Facebook, destinados apenas ao compartilhamento de notícias e comentários que suportem a ideia Anonymous. No Brasil, os mais seguidos são os já citados @AnonBrNews, @AnonIRC e @PlanoAnonBr.

Por fim, essa evangelização se fez notável também – ou sobretudo – em alguns dos canais IRC, nas redes utilizadas pelos Anonymous. Para tomar o exemplo do #planbr, na maior parte do tempo em que o canal ficou ativo, havia sempre alguns colaboradores que se dedicavam a receber os novos membros, explicar-lhes o que estava ocorrendo e também mostrar como poderiam ajudar, se assim quisessem. Foi um desses evangelizadores, por exemplo, que recebeu este pesquisador em meados de 2011, quando buscava por Anons brasileiros nos principais servidores internacionais. Conforme explicaria mais tarde um dos hackers que assumiu para si essa função, havia uma preocupação constante nesse sentido,

como, por exemplo, durante as manifestações do movimento *Occupy*: "Eu era um dos poucos que passavam um tempo considerável no canal (18 horas por dia, em media). Se todo mundo vai pra ocupação, não fica ninguém […]. A gente tinha um numero X de pessoas que realmente sabia como receber os novatos no canal, como tirar as dúvidas, quais vídeos mandar pra eles".

4.3 FORMANDO REDES DISTRIBUÍDAS

Além de promover o anonimato e se empenhar na dita evangelização, os Anonymous também se engajam politicamente por meio da formação de redes distribuídas independentes. Esta (des)organização não é à toa: reflete a multiplicidade de indivíduos, ideias e métodos envolvidos com o coletivo e o torna, por sua natureza, um ator político muito difícil (se não impossível) de ser abatido.

Entre todas as definições possíveis que diferenciam as redes centralizadas, descentralizadas e, como neste caso, distribuídas, este trabalho optou pelas atribuições a elas conferidas pelo teórico norte-americano Alexander Galloway:

> Uma rede distribuída se diferencia de outras redes – como as centralizadas e as descentralizadas – na disposição de sua estrutura interna. Uma rede descentralizada consiste em um único ponto de poder central (um *host*) ao qual os nós radiais são atraídos. O ponto central está conectado com todos os nós satélites, que se conectam entre si apenas por meio do ponto central. Uma rede descentralizada, por outro lado, tem múltiplos pontos centrais, cada qual com seu conjunto de nós satélites. A comunicação se dá geralmente de forma unidirecional tanto nas redes centralizadas quanto descentralizadas: a partir do tronco central em direção às folhas radiais. A rede distribuída é algo completamente diferente […]. Cada ponto em uma rede distribuída não é nem um *hub* central nem um nó satélite – não há troncos ou folhas […]. Como em um rizoma, cada nó em uma rede distribuída pode estabelecer comunicação direta com outro nó sem ter de se reportar a um intermediário hierárquico (GALLOWAY, 2004, p. 11-12).

Um emaranhado heterogêneo de nós diretamente conectados uns com os outros sem intermediários hierárquicos; sem centros de controle ou geográficos; em comunicação multidirecional e irrestrita – assim se dispõem os Anonymous, um projeto de rede distribuída que frequentemente conta com células que se dissipam, após uma determinada operação, com

a mesma velocidade com que se criaram, pouco tempo atrás – a #OpGlobo, conforme relatado anteriormente, é um eminente exemplo disso.

Nesse sentido, os Anonymous atuam à maneira dos nômades deleuze-guattarianos, responsáveis pelo desenvolvimento da chamada "máquina de guerra", paradigma naturalmente exterior e irredutível ao do aparelho de Estado. Dispostos sob a forma de um rizoma, em oposição à estrutura arborescente, que, com seus núcleos de controle, concentram os poderes sob a lógica do aparelho de Estado, os nômades se fundam na multiplicidade, promovem e alimentam uma "indisciplina fundamental do guerreiro, um questionamento da hierarquia, uma chantagem perpétua de abandono e traição, um sentido da honra muito suscetível, e que contraria, ainda uma vez, a formação do Estado" (DELEUZE; GUATTARI, 1997, p. 21). Essa estrutura nômade dos hacktivistas ainda atua, por meio de redes distribuídas, no "espaço liso" absolutamente heterogêneo da grande rede, um "lado de fora" tangível ao paradigma da forma Estado, e no qual a desterritorialização e a intensificação da velocidade levam os próprios nômades à constante tentativa de fuga à captura por parte desse paradigma.[47] No espaço liso, hábitat natural dos nômades, não há metodologia que se firme, nem forma que consiga se reproduzir com exatidão, mas sim um modelo totalmente turbilhonar, enredado, e fundado na distribuição de fluxos em um espaço aberto. Enfim, um espaço em que não há pontos de partida ou de largada, não há paradas obrigatórias, mas apenas movimento.

Assim, sob o espírito nômade, essa ação política em redes distribuídas permite aos Anonymous desenvolver múltiplas comunidades independentes, algumas vezes até isoladas, que podem variar em sua filosofia e metodologia de trabalho, objetivos específicos ou forma de realização das ações, mas respeitam-se mutualmente quanto ao uso da marca Anonymous e estão intimamente ligadas por essa identidade coletiva da qual fazem parte. Como se pontuou no capítulo anterior, não faltam exemplos dessas comunidades independentes interconectadas. Elas se formam em torno de redes de IRC, dos canais situados nessas redes, dos perfis em redes sociais, ou mesmo sob os esforços de operações específicas. Estas, por sua vez, são desenhadas e executadas de acordo com as necessidades e vontades mais urgentes daqueles nichos que estão por trás delas. Por exemplo, basta uma rápida visita à rede AnonOps, no IRC, para observar o espantoso número de pequenas operações ocorrendo simultaneamente,

47 Para Deleuze e Guattari (1997), a forma Estado, por sua vez, representa o próprio lado de dentro, num espaço estriado que se funda na homogeneidade, e que quer capturar a máquina de guerra e as estruturas nômades com a finalidade de estriá-las, regulá-las, e dispô-las sob suas regras e normas.

deflagradas por diferentes atores.

Dessa forma, a natureza do coletivo é condicionada pelo intrincado conjunto de relações – envolvendo junções, cooperações, mas também intrigas, atritos, tensões, contradições, rupturas etc. – que se dão entre esses diferentes nichos, assumidos como uma massa em constante interação. À medida que estes se movem, assumindo novas ações, propalando novas ideias, reivindicando novos modos de agir, o coletivo como um todo se transforma e se reinventa – passa do *lulz* à ação coletiva direta; move-se entre a rede e as ações de rua; e assim por diante.

O fato de fugir das formas institucionais tradicionais quanto à ação política, tanto nos protestos como mas tomadas de decisão, faz com que os Anonymous se tornem muito mal compreendidos pelas organizações que adotam estruturas hierárquicas de organização. Trata-se da velha tensão entre a catedral, de um lado, e o bazar, de outro, na conhecida analogia formulada por Eric Raymond ao caracterizar o modo de produção dos softwares livres (1998). Por exemplo, tornou-se cada vez mais frequente, nos noticiários da mídia de massa, apontar os Anonymous simplesmente como um "grupo" – ou, ainda, um grupo composto unicamente por hackers. Para responder a isso, um Anon ligado ao movimento internacional publicou, em agosto de 2011, um dos comunicados[48] que se tornaram clássicos entre o coletivo, chamado "Anonymous não é unânime" (*Anonymous is not unanimous*):

> Os Anonymous têm um problema de percepção. A maior parte das pessoas pensam que nós somos um grupo de hackers sombrios. Este é um erro fundamental. Anonymous são *grupos* de hackers sombrios, e é aqui que reside o problema. Os Anonymous fizeram uma série de benesses nos últimos 9 meses. Ajudaram, junto com outros grupos, a fornecer apoio a pessoas localizadas em países onde "democracia" é uma palavra ruim. A mídia *mainstream* precisa entender que Anonymous não é unânime […].

Outro exemplo que revela a falta de entendimento quanto ao funcionamento de um movimento político organizado em redes distribuídas: o governo canadense, que certamente compõe uma rede centralizada, convocou, em março de 2012, os "Anonymous" para depor na Comissão de Assuntos Internos da Câmara dos Deputados. O motivo? Supostos "membros do grupo" teriam ameaçado um ministro que trabalhava a favor da aprovação da lei C30, que trata da censura à internet. Diante da evidente inviabilidade de um depoimento "dos Anonymous", um dos perfis no Twitter associados ao coletivo respondeu: "Só vamos se

48 Disponível em: <http://pastebin.com/4vprKdXH>. Acesso em 15 nov. 2011.

houver poltronas estofadas para todos. Somos uma Legião".

Este talvez seja o principal desafio – e também o principal temor – das instituições hierárquicas que pretendem fazer frente aos Anonymous. Afinal, a quem culpar? A quem retaliar? Como capturar uma ideia? Como prender uma legião? A adoção de uma identidade coletiva que tenta, a todo momento, esconder suas individualidades é, por certo, um problema para essas instituições. Do mesmo modo que podem faltar poltronas estofadas em um Parlamento, certamente faltarão agentes para deter uma ideia disforme.

4.4 EXIBINDO E POSSIBILITANDO VÁRIAS FORMAS DE AÇÕES POLÍTICAS

Por último, e talvez mais importante, é possível dizer que os Anonymous exibem e possibilitam a existência e a execução de uma vasta gama de ações políticas. Por certo, isso se verifica como uma decorrência natural das características mais eminentes do coletivo, que se delinearam até então neste trabalho. Afinal, seu caráter anônimo, evangelizador, distribuído, desprovido de lideranças, diretrizes ou núcleo geográfico, faz dos Anonymous uma marca que engendra a participação de diversos grupos e indivíduos em várias ações possivelmente desconexas, mas que se abrigam sob o grande guarda-chuva capitaneado por uma legião sem rosto.

Conforme observamos, há poucas barreiras de entrada para que os atores políticos se identifiquem e atuem como Anonymous. Não é preciso preencher formulários, seguir regras regimentais, ou enviar dinheiro para quem quer que seja. Em grande medida, isso resulta em uma vasta multiplicidade de operações, que podem variar em objetivo, metodologia ou ideário, a depender daqueles que as propõem e, principalmente, daqueles que eventualmente aderem a elas.

Essa vibrante pluralidade faz com que não seja nada custoso para um indivíduo se identificar com uma das inúmeras células Anons distribuídas pela rede, ou com alguma das dezenas de operações sempre em curso. E, mesmo que isso se mostre difícil, tal indivíduo certamente será respeitado caso prefira dar início à própria célula ou à própria operação, buscando possíveis adesões *a posteriori*. Ou seja: os Anons são frequentemente empoderados com a capacidade de criar seu próprio canal, perfil, comunidade, operação, ou movimento em

meio à ideia Anonymous.

Como consequência disso, os Anonymous se tornam uma via concreta, informal e convidativa para o engajamento político, culminando com um alto nível de envolvimento ativista nas operações de maior repercussão. Isso porque, embora cada um dos nós dessa rede distribuída seja condicionado pelas vontades e necessidades de sua base de apoiadores, e se transforma à medida que ela o faz, de tempos em tempos, eles se unem em operações ditas globais que, conforme se pontuou, contam com o trabalho coletivo de diversos nichos independentes espalhados pelo mundo.

Portanto, os Anonymous também se engajam politicamente exibindo e possibilitando ações políticas de toda sorte – por exemplo, desde um simples ato de divulgação de ideias até uma complexa operação hacktivista de vazamento de informações sensíveis.

5 CONSIDERAÇÕES FINAIS

Antes de apontar as possíveis contribuições que esta dissertação pode oferecer aos estudos vindouros que contemplarem certas temáticas específicas e se realizarem sob as correntes teórico-metodológicas de algumas áreas do conhecimento, é preciso apontar, de modo claro e transparente, algumas questões relevantes, a começar pelas principais limitações deste trabalho.

A primeira delas diz respeito ao próprio objeto deste estudo. Por sua natureza, os Anonymous são de difícil apreensão. A ausência de lideranças, de um núcleo central – seja geográfico ou de decisões – e de qualquer ato ou produto que se apresente como "oficial" do coletivo tornou esta pesquisa, por diversas vezes, uma verdadeira corrida entre gato e rato, ou entre pesquisador à procura de suas fontes de trabalho. Além do mais, a disposição dos Anons em redes distribuídas, formando nós flexíveis e intermitentes, tampouco auxiliou esse processo que, por isso mesmo, mostrou-se exaustivo em diversos momentos. Afinal, uma investigação que se fundamentasse apenas em relatos de pesquisadores estrangeiros e de textos jornalísticos veiculados na imprensa nacional não seria capaz de responder à altura as questões que nos propusemos a analisar nesta dissertação. Este é, portanto, um dos motivos pelos quais se pode afirmar que este trabalho não apreendeu os Anonymous Brasil em sua totalidade, nem tampouco elaborou um completo e fidedigno mapa desse movimento. Conforme alguns pesquisadores que acompanham o coletivo em nível internacional já observaram, pela natureza dos Anons, esta é uma tarefa sumariamente impossível de se realizar com alguma propriedade.

Evidentemente, em uma pesquisa acadêmica, todo e qualquer tipo de recorte resulta em perdas e na adoção de um viés. Neste trabalho, não poderia ter sido diferente. Como os Anonymous são um coletivo que se expressa também por meio de grandes operações, não raro com o objetivo de chamar a atenção da imprensa, se analisaram entre várias outras, duas dessas ações, com clara orientação hacktivista. Várias razões levaram a elas – como, por exemplo, sua repercussão, o volume de participantes engajados e o fato de serem exemplares a ponto de evidenciar a maior parte dos traços mais característicos dos Anonymous Brasil identificados ao longo desta pesquisa. Mas, também, optou-se por elas porque, dados os prazos e as obrigações que envolvem a execução de uma dissertação de mestrado no Brasil,

este pesquisador pôde acompanhá-las mais de perto, ao contrário de outras. Evidentemente, a análise de um maior número de ações teria enriquecido este trabalho, revelando novas informações e demais materiais para análise.

Por outro lado, como os Anonymous também são um coletivo de planejamento e discussão de ideias, que se discute e se refaz enquanto acontece, fez-se necessária a realização de entrevistas com grupos e indivíduos identificados com essa ideia no Brasil. Definitivamente, não foi possível falar com todos os Anons brasileiros, nem mesmo com a maioria – muitos, inclusive, atuam de forma bem discreta, sem se expor a canais abertos de comunicação. Com isso, este trabalho reflete o caminho particular percorrido pelo pesquisador em meio às redes habitadas pelos Anonymous no Brasil.

Por fim, é certo que os resultados deste trabalho são também fruto de um ferramental teórico aqui adotado. Dadas as suas características, um objeto de pesquisa tão fértil e multiforme como os Anonymous poderia ser interpretado à luz de outras várias perspectivas teóricas – conforme verificamos no segundo capítulo, o ativismo hacker é um fenômeno contemplado por estudos de distintas áreas do conhecimento, sob diversos prismas. Muitos deles, aliás, podem e devem se configurar como fonte de inspiração para pesquisas futuras acerca desse objeto.

No entanto, a despeito dessas naturais e inevitáveis limitações, esta pesquisa pode fornecer, ainda que de modo preliminar e exploratório, algumas contribuições a diversos campos acadêmicos. A contribuição mais significativa deste trabalho é, sem dúvidas, para o entendimento acerca da rede Anonymous, principalmente em sua faceta brasileira. Nesse sentido, a despeito da expressão desse fenômeno, esta dissertação caracteriza-se como o primeiro estudo acadêmico que investiga especificamente os Anonymous Brasil. Suas conclusões, dessa maneira, podem-se mostrar úteis a pesquisas futuras que tratem dos próprios Anonymous, envolvendo seus traços culturais e sociais, bem como suas formas de engajamento político.

De modo mais amplo, este trabalho também pode contribuir para estudos que contemplem as características e as evoluções do ciberativismo, em geral, e do hacktivismo, em particular. Tal como se argumentou no primeiro capítulo, os Anonymous representam uma reconfiguração do ativismo hacker, reacendendo-o no plano internacional e levando-o a uma combinação com outras formas de ativismo político, bem como engendrando diversas formas de engajamento. E, ainda no plano mais geral, este trabalho também pode apresentar

contribuições para pesquisas que tratem de novas formas de participação política e de ativismo, sobretudo no que se refere, por um lado, a novas ferramentas e estratégias de ação e, por outro, ao angariamento de atores políticos – jovens, em sua maioria – que, desacreditados das formas institucionais de participar da cena política, encontraram em movimentos como os Anonymous modos de fazê-lo por meio de outras vias.

5.1 PESQUISAS FUTURAS E NOVAS ABORDAGENS

Apontadas as principais limitações e contribuições deste trabalho, também se faz relevante, neste espaço, lançar outros possíveis caminhos para futuras pesquisas acadêmicas concernentes ao tema aqui tratado.

Entre as outras diversas abordagens teóricas que podem auxiliar na compreensão de um objeto como os Anonymous, vêm ganhando destaque algumas perspectivas associadas às teorias de movimentos sociais. Nos últimos anos, certos pesquisadores passaram a se valer dessa abordagem para lançar caracterizações em direção a coletivos ativistas que, entre outras coisas, atuam de modo descentralizado/distribuído; acreditam no poder de mobilização e transformação da Internet; e se dispõem de forma a questionar as estruturas tradicionais vigentes nas principais organizações políticas da atualidade, como governos, partidos políticos e movimentos sociais tradicionais.

Jeffrey Juris (2004), por exemplo, dedica-se ao estudo do que chamou de "movimentos sociais em rede", notadamente os movimentos antiglobalização e por justiça global que, sob forte influência do Movimento Zapatista de Libertação Nacional, revelado ao mundo em 1994, teriam surgido após a série de manifestações e protestos ocorridas em Seatle, em 1999. O autor considera que, ao utilizar práticas e tecnologias em rede para se comunicar, coordenar ações e se auto-organizar, esses ativistas estariam construindo "novas formas organizacionais que são baseadas em redes, e que expressam e refletem a rede como um ideal político e cultural emergente" (Idem, p. 355).

Em outro texto, assinado com Carles Feixa e Inês Pereira (2009), os pesquisadores traçam um breve e amplo histórico dos movimentos sociais de maneira geral, classificando-os como velhos (*old social movements*), novos (NSM, ou *new social movements*) e novíssimos

(*new new social movements*). Os primeiros, surgidos na primeira metade do século XIX, estariam ligados à emergência da sociedade industrial, que suscitou lutas geralmente identificadas como masculinas, adultas e baseadas principalmente em fronteiras concretas de classe, nação e condição social. Além disso, são comumente relacionados aos movimentos trabalhistas. Seus exemplos mais emblemáticos seriam a onda revolucionária de 1848, a comuna de Paris, a Revolução Russa de 1917 e o movimento pela reforma universitária em Córdoba, Argentina, em 1918. Nesse sentido, seu foco residia em protestos de ordem econômica e política, mas também moral, sendo a greve e a manifestação suas ações mais visíveis. Entre as características culturais desses movimentos, podem-se citar a linguagem verbal, uma estética relacionada às lutas e a produção cultural em meios tradicionais, como jornais, panfletos e livros. Por fim, sua forma organizacional dominante é melhor representada pela metáfora do banco: grupos locais com grande coesão interna, além de símbolos e sinais de identidade que diferenciavam claramente quem pertencia ou não ao movimento.

Já os novos movimentos sociais, segundo os autores, nasceram principalmente na Europa e na América do Norte após a Segunda Guerra Mundial, entre os anos 1950 e 1970, e tiveram como ponto de partida os movimentos estudantis em Berkley (1964), Paris, Roma, Nova York e México (1968). A base social dos novos movimentos sociais fugiram à noção de classe, enfatizando agora outros critérios de identidade, tais como a geração, o gênero, a orientação sexual e o caráter étnico de minorias. Ao contrário dos velhos movimentos, estes transcenderiam seu caráter local, passando a lutas regionais e transnacionais. Seus movimentos mais característicos são o de meio ambiente, feminista, pacifista, contracultural e pela liberdade sexual. Entre suas ações mais visíveis, de roupagem mais lúdica, poder-se-iam citar ocupações e acontecimentos pontuais, mas atividades tradicionais, como assembleias, ainda continuaram a existir. Por fim, os novos movimentos sociais são identificados sobretudo com movimentos jovens, cuja participação deu origem a uma série de microculturas específicas que transcenderam fronteiras.

Por sua vez, os novíssimos movimentos sociais são aqueles que se estendem sobre as fronteiras dos espaços físicos e virtuais na virada do novo milênio. Destacando as transformações sociais associadas à consolidação do capitalismo informacional, esses movimentos têm como símbolos iniciais os acontecimentos em Seattle (1999), Praga (2000) e Genoa (2001). Além disso, suas bases sociais transcendem questões de geração, gênero, etnias e territórios, pois reúnem um coletivo extremamente heterogêneo e multifacetado em torno de

uma causa, e sua base social não é mais local, regional ou nacional, pois eles estão situados em um grande espaço global em rede. Tal como os novos movimentos sociais, estes movimentos combinam ações tradicionais, como marchas e manifestações, mas as chamadas para a ação geralmente se dão de forma distribuída pela Internet, e as ações são frequentemente orquestradas junto a várias formas virtuais de resistência. Muito embora boa parte de seus atores sejam jovens, tais movimentos são identificados como lutas intergeracionais. E ainda, conforme argumentam os autores, "uma diferença importante dos movimentos anteriores é que, pela primeira vez, os jovens não estão, por definição, em uma posição subalterna, especialmente em relação à mudança tecnológica" (JURIS, PEREIRA e FEIXA, 2009, p. 428).

Outro autor a utilizar abordagem dos movimentos sociais é o sociólogo espanhol Manuel Castells, o grande teórico da chamada sociedade em rede. Em seu livro *Networks of outrage and hope: social movements in the Internet age*, lançado em 2012, Castells se dispôs a analisar previamente a vasta gama de manifestações e movimentos que, iniciados por meio de chamados oriundos de redes sociais na Internet, culminariam com grandes ocupações do território urbano e com a queda de alguns governos totalitários em países árabes – a assim chamada Primavera Árabe. Esta, por sua vez, serviu de estopim para outros movimentos em rede que, voltando-se contra as elites políticas e econômicas em tempos de crise, realizaram diversos atos de protesto na Europa (principalmente na Espanha, Grécia, Portugal, Itália e Reino Unido) e nos Estados Unidos, promovendo várias ocupações, assembleias e ações de resistência virtual.

Castells analisa separadamente os casos da Tunísia, Islândia, Egito, Espanha e as ações decorrentes do movimento *Occupy Wall Street*, iniciado nos Estados Unidos e com repercussões em diversos lugares do mundo, incluindo o Brasil. O autor argumenta que os movimentos sociais em rede da era digital representam uma nova espécie de movimento social por conta das novas formas de comunicação existentes hoje:

> As características dos processos de comunicação entre indivíduos engajados no movimento social determinam as características organizacionais do próprio movimento: quanto mais interativa e autoconfigurável é a comunicação, menos hierárquica será a organização e mais participativo será o movimento (CASTELLS, 2012, p. 15).

Por fim, ao tratar de um padrão emergente de movimentos sociais em rede, o autor

identifica as seguintes características comuns entre eles: são em rede sob múltiplas formas (ação, estruturação, ausência de lideranças, organização on e offline etc.); tornam-se movimentos ocupando o espaço urbano (seu espaço de interação é no que o autor chamou de "espaço de autonomia": a intersecção entre o espaço de fluxos da internet e os significativos espaços físicos ocupados – "o espaço de autonomia é a nova forma espacial dos movimentos sociais em rede", p. 222); são locais e globais ao mesmo tempo (iniciam-se em contextos específicos e se conectam pelas redes da Internet); têm uma nova relação com o tempo (organizando sua vida como se ela pudesse a sociedade alternativa dos sonhos); são espontâneos em sua origem, geralmente deflagrados por uma faísca de indignação; são virais, segundo a própria lógica da rede; fazem suas deliberações nesse "espaço de autonomia", com a transição da afronta (*outrage*) para a esperança *(hope*); não têm liderança central (seus participantes não confiam em qualquer forma de delegação de poderes); sua condição de se aglutinar é fomentada pelas redes horizontais de comunicação; praticam constantemente a autorreflexão; não são violentos; são raramente programáticos, contando com múltiplas demandas e uma motivação quase ilimitada; almejam mudar os valores da sociedade, sem qualquer pretensão de assumir o poder; são deveras políticos no sentido de defender e adotar a democracia participativa; e compartilham uma cultura específica: a cultura da autonomia, a matriz cultural fundamental das sociedades contemporâneas.

Assim como Juris e Castells, outros autores se lançaram a interpretar essas novas mobilizações à luz das teorias de movimentos sociais. No também recente livro *Movimentos sociais na era global*, organizado por Maria da Glória Gohn e Breno Bringel (2012), duas autoridades acadêmicas no assunto, diversos pesquisadores levantam estudos de caso e sistematizações quanto aos novos e novíssimos movimentos sociais, para utilizarmos a terminologia de Jeffrey Juris (2004) – com destaque para os textos de Célia Regina Jardim Pinto, que lançou a hipótese de uma "nova forma de fazer política" diante dos movimentos ocorridos em 2011, notadamente no caso da Espanha e do Chile; e de Geoffrey Pleyers, que se focou no estudo do Fórum Social Mundial, argumentando quanto à existência de um novo padrão de "internacionalização sem institucionalização". Segundo Gohn e Bringel (2012, p. 8):

> No cenário do mundo globalizado a partir do final do século XX, observa-se: a rearticulação das formas de dominação, nova (re)divisão internacional do trabalho entre os Estados-nações operada pelas políticas econômicas contemporâneas e os novos mecanismos de ação dos mercados e agentes

> financeiros, novas políticas públicas nas quais o Estado passa a ser gestor/controlador e não promotor direto de bens e serviços. E novas práticas sociais em um mundo crescentemente moldado pela complexidade. Esta globalização assimétrica se beneficiará da importância crescente das redes e dos fluxos das novas tecnologias de informação e comunicação. Isto tudo levou a uma reestruturação das formas de organização e de protestos das ações coletivas e dos movimentos sociais nas últimas duas décadas.

Embora tratem das mais atuais mobilizações em massa percebidas pelo mundo nos últimos anos e, portanto, trazem um referencial de análise altamente relevante e, em alguns pontos, pertinentes a nosso objeto, essas teorias não tratam especificamente de coletivos que se valham do ativismo hacker como forma de protesto e resistência política. Por esta e outras razões, apesar de não terem feito parte do escopo deste trabalho, as teorias de movimentos sociais abrem-se como um dos campos de estudo mais profícuos em relação aos Anonymous e aos novos movimentos globais em rede. Por isso, para trabalhos futuros, explorações nesse sentido se mostram prementes.

5.2 CONCLUSÕES

Esta pesquisa argumentou que o ativismo hacker, de modo mais amplo, e que a rede Anonymous, de modo particular, configuram-se como uma forma de resistência política a um modo específico de como o controle é exercido nas sociedades contemporâneas. Partindo dessa premissa, propôs-se a analisar as formas de engajamento político utilizadas por grupos e indivíduos identificados com esse coletivo no Brasil.

No primeiro capítulo, realizamos um breve histórico do hacktivismo em escala global – tendo como ponto de partida o levante zapatista, em 1994 – para considerar que, no final dos anos 2000, os Anonymous representaram uma nova etapa na história do ativismo hacker. Com base principalmente nas obras de Levy (1984) e Himanen (2001), verificamos que o hacking sempre foi uma atividade intrinsecamente carregada de traços políticos. No entanto, o hacktivismo tal como o praticado pelos Anonymous emprestou a este fenômeno uma faceta ainda mais transgressiva e politizada. Argumentamos, ainda, que em tempos de crescente digitalização das mais diversas informações políticas, econômicas, culturais e mesmo de caráter intrinsecamente pessoal, os hackers passam a se tornar atores políticos de grande

relevância.

O segundo capítulo trouxe à discussão, em um primeiro momento, as fundações teóricas da chamada sociedade de controle e mostrou de que forma o hacktivismo resiste a tal controle. Além do texto seminal de Deleuze (1992), o autor que lançou as primeiras pressuposições de uma nova forma de exercício do poder, percorremos as principais expressões acadêmicas nesse sentido, passando por Hardt (2000), Pelbart (2011), Santos (2003), Silveira (2012) e, principalmente, Galloway (2004). Este, por sua vez, associou o controle deleuziano a um estilo de gerenciamento em particular – o protocolo, que está no cerne da mídia de massa mais controlada de todos os tempos: a Internet. Por serem atores protocológicos por excelência, os hackers têm a expertise – e, em alguns casos, o engajamento político – necessário para resistir ao controle por meio do protocolo, iludindo-o e hipertrofiando-o.

Ainda no segundo capítulo, em etapa posterior, debruçamo-nos sobre parte dos principais trabalhos que já lançaram interpretações sobre o ativismo hacker, dividindo-os em três perspectivas teóricas: (1) Desobediência civil digital; (2) Guerra da informação / ciberterrorismo; e (3) Hacktivismo por ele mesmo. Nesta pesquisa, filiamo-nos à primeira perspectiva por entender que ela é a mais apropriada para tratar dos aspectos sociais, culturais e políticos dessa forma de ativismo, uma vez que considera o fenômeno de uma maneira mais ampla – não se focando apenas em suas propriedades técnicas ou corporativistas.

No terceiro capítulo, apresentaram-se os principais resultados a respeito dos Anonymous Brasil. Após realizar um breve histórico do movimento internacional, posicionando seus traços culturais fundantes mais salientes, identificaram-se suas origens e principais faces no contexto brasileiro, dividindo a trajetória do coletivo em quatro fases: início, operacional, ápice e dispersão. Para tanto, valeu-se de depoimentos coletados junto a indivíduos identificados com os Anonymous e da observação direta de duas grandes operações deflagradas pelos hacktivistas: a Operação WeeksPayment e a Operação Globo, realizadas em 2012. Diante dos apontamentos revelados nesse capítulo, quando confrontados às premissas teóricas do capítulo anterior a ele, podemos inferir que:

▪ Os Anonymous Brasil praticam um ativismo on-line diferenciado por motivos táticos, culturais e de princípios, na formulação de Samuel (2004);

▪ Ainda tendo por base a obra de Samuel, os Anons desenvolvem o chamado hacktivismo de performance, deflagrando principalmente desfiguração de sites, ações

distribuídas de negação de serviço e vazamento de informações;

▪ Os Anonymous se configuram como representantes da "nova comunidade" hacker apontada por Jordan e Taylor (2004). Tal comunidade foi influenciada pela primeira geração, com o desejo de que toda informação deve ser livre, mas também pelas gerações seguintes, que deram o tom contrário ao *stablishment* e à autoridade, além de apresentarem um cunho político nas próprias linhas de código, como é o caso do movimento *open source*. No caso dos Anonymous, no entanto, esse ativismo extrapolou tais códigos, de modo que boa parte de suas ações tiveram como objetivo interferir mais diretamente no debate político;

▪ Entre os princípios básicos que conformam uma ação hacktivista eticamente motivada, tal como observaram Manion e Goodrum (2000), os Anonymous parecem cumpri-los. Não se voltaram para o lucro de qualquer pessoa ou grupo associado ao coletivo; tiveram motivação ética, mostrando a convicção de que a conduta contra a qual protestavam era injusta; e assumiram, em nome do coletivo, a responsabilidade pelas ações;

▪ A relação entre os indivíduos e grupos isolados, de um lado, e o coletivo Anonymous, como um todo, revelou um aspecto próprio da cultura hacker: o do individualismo colaborativo, tal como pontuado por Silveira (2012).

▪ A diversidade encontrada nos Anonymous Brasil corrobora a argumentação de Coleman e Golub (2008) no sentido de que não existe uma única e universal cultura hacker, mas sim uma heterogênea gama de indivíduos identificados com ela. Os vários graus de saturação tecnológica a que os hackers são submetidos modelam os públicos, as opiniões políticas e os compromissos éticos dos hackers, culminando com uma multiplicidade de atores e ideias;

▪ De alguma forma, as operações deflagradas pelos Anonymous Brasil tentaram forjar zonas autônomas temporárias, conforme teorizadas por Bey (2001). De súbito, ocuparam clandestinamente um espaço na rede, promovendo breves demonstrações de resistência, e se esvaíram com a mesma agilidade;

Já o capítulo anterior refletiu mais especificamente sobre a questão central deste trabalho, sugerindo quatro formas de engajamento político por parte dos Anonymous e refletindo sobre algumas das implicações quanto à adoção destas formas: a promoção do anonimato; a evangelização; a formação de redes distribuídas; e o fato de exibir e possibilitar várias formas de ações políticas.

E, por fim, após descrever todo o caminho aqui percorrido e apontar as principais

descobertas desta pesquisa, este trabalho conclui que o coletivo Anonymous, que reconfigurou e reformulou o ativismo hacker em escala global, apresenta-se um dos representantes dessa forma de resistência política que responde, em última análise, a um modo específico como o controle é implementado e exercido em alguns setores das sociedades contemporâneas – as sociedades do controle, na concepção e periodização histórica formuladas por Deleuze (1992). Por isso mesmo, suas formas de engajamento político, tais como descritas nos capítulos anteriores, não valorizam as ações políticas típicas às sociedades disciplinares ou de soberania, nas quais se verificavam outras formulações do exercício do poder.

Conforme se observou, são múltiplas as ferramentas e estratégias utilizadas como resistência ao controle de caráter protocológico, seguindo a interpretação de Galloway (2004). Em todas elas, usa-se o protocolo para se investir contra o próprio protocolo. No caso dos Anonymous, suas ações de negação de serviço hipertrofiam os protocolos de controle, valendo-se dos próprios protocolos para bloquear alguns fluxos fundamentais de comunicação; sua opção radical pelo anonimato esforça-se para iludir os sistemas de vigilância online implementados sistematicamente por governos e corporações em todo o mundo, empoderando os cibercidadãos ao possibilitar-lhes mais liberdade de ação; seus vazamentos de informações são uma forma de utilizar as mesmas redes, que são empregadas para controlá-los, com a finalidade de mostrar aos "controladores" que estes também estão sendo observados e, em alguns momentos, "hackeados".

*****

Antes de finalizar, cabe aqui uma última consideração. Certamente, não fez parte do escopo deste trabalho avaliar os resultados ou as ações práticas decorrentes do ativismo político adotado pelo hacktivismo, em geral, ou pelos Anonymous, em particular. Isso requereria outra abordagem e, principalmente, outro tipo de análise. Nesta dissertação, dedicamo-nos a apresentar e descrever uma outra forma de participação política que se pretende universal, mas não se aceitaria totalizante, e que, por definição, parece pouco preocupada em fornecer respostas definitivas e unívocas a perguntas como "em que isso vai dar?" ou mesmo "quais serão, ao final, os ganhos reais destas ações?".

Nesse sentido, os Anonymous representam algo diferente. “Anonymous é um pressuposto”, afirmou um Anon a este pesquisador. De fato: um pressuposto inacabado, que se (re)constrói e se (re)pensa à medida que acontece, e cuja potencialidade parece residir justamente na multiplicidade, de um lado, e na possibilidade de e convite à ação, de outro. Governos e corporações de todo o mundo certamente não investiriam tempo, esforço e dinheiro para prender, vigiar e reprimir esses atores se essa ideia se mostrasse tão inofensiva.

REFERÊNCIAS

ARQUILLA, John; RONFELDT, David. The advent of netwar. In: _____. (Org.). **In Athena's camp**: preparing for conflict in the information age. Washington: RAND, 1997. p. 275-293.

ANTOUN, Henrique. Expressões do novo ativismo: hackers e o individualismo colaborativo. Palestra ministrada no **seminário internacional Cidadania e Redes Digitais**, realizado na Universidade Metodista de São Paulo, em São Bernardo-SP, em 21 de outubro de 2011. Vídeo disponível em: <http://www.metodista.br/cidadaniaeredesdigitais/cidadaniaeredesdigitais/expressoes_do_novo_ativismo_hackers_e_o_individualismo_colaborativo>. Acesso em: 12/8/2012.

BEY, Hakim. **TAZ**: zona autônoma temporária. São Paulo: Conrad, 2001.

CASTELLS, Manuel. **O poder da identidade**. 3. ed. São Paulo: Paz e Terra, 2002.

_____. **A sociedade em rede**. 10. ed. São Paulo: Paz e terra, 2007.

_____. **Communication power**. Nova York: Oxford University Press, 2009.

_____. **Networks of outrage and hope**. Cambridge; Malden: Polity Press, 2012.

CLEAVER, Harry. Zapatistas e a teia eletrônica de luta. **Lugar Comum**, v. 4, p. 139-163, 1998.

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.

_____. Nossa esquisitice é livre. In: SILVEIRA, Sergio Amadeu da; JOSGRILBERG, Fábio Botelho. (Orgs.). **Tensões em rede**: os limites da cidadania na internet. São Bernardo do Campo: Universidade Metodista de São Paulo, 2012. p. 91-108.

COLEMAN, Gabriella; GOLUB, Alex. Hacker practice: Moral genres and the cultural articulation of liberalism. **Anthropological Theory**, v.8, n.3, p. 255-277, 2008.

COLEMAN, Gabriella; RALPH, Michael. Is it a crime? The transgressive politics of hacking in Anonymous. **Social Text Journal Blog**. 2011. Disponível em: <http://www.socialtextjournal.org/blog/2011/09/is-it-a-crime-the-transgressive-politics-of-hacking-in-anonymous.php >. Acesso em: 7 dez. 2011.

COSTA, Rogério da. Sociedade de controle. **São Paulo em Perspectiva**, v. 18, n. 1, p. 161-167, 2004.

CRITICAL ART ENSEMBLE (CAE). **Distúrbio eletrônico**. São Paulo: Conrad, 2001.

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

DELEUZE, Gilles. **Foucault**. São Paulo: Brasiliense, 2005.

DELEUZE, Gilles; GUATTARI, Feliz. **Mil platôs**: capitalismo e esquizofrenia. Vol. 5. São Paulo: Ed. 34, 1997.

DENNING, Dorothy. Hacktivism and Other Net Crimes: entrevista. [31 de agosto, 2000]. Nova York: Revista **Uniquity**.

DENNING, Dorothy. Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing foreign policy. In: ARQUILLA, John; RONFELDT, David. **Networks and netwars**: the future of terror, crime, and militancy. Washington: Rand Corporation, 2001. p. 238-288.

DOMINGUEZ, Ricardo. Digital zapatismo. 1998. Disponível em: <http://www.thing.net/~rdom/ecd/DigZap.html>. Acesso em: 7 mar. 2011.

DOMINGUEZ, Ricardo. Digital zapatismo. 1998. Disponível em: <http://www.thing.net/~rdom/ecd/DigZap.html>. Acesso em: 3/2/2012.

FOUCAULT, Michel. **História da sexualidade I**: a vontade de saber. Rio de Janeiro: Graal, 1988.

FOUCAULT, Michel. **Resumo dos cursos do Collège de France (1970-1982)**. Rio de Janeiro: Jorge Zahar, 1997.

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

GARRIDO, Maria; HALAVAIS, Alexander. Mapping networks of support for the zapatista movement: applying social-networks analysis to study contemporary social movements. In: MCCAUGHEY, Martha; AYERS, Michael D. (Orgs.). **Cyberactivism**: online activism in theory and practice. Nova York: Routledge, 2003. p. 165-184.

GOHN, Maria da Glória; BRINGEL, Breno M. (Orgs.). **Movimentos sociais na era global**. Petrópolis, RJ: Vozes, 2012.

GORZ, André. **O imaterial**: conhecimento, valor e capital. São Paulo: Annablume: 2005.

HAPLUKA, Max. **The evolution of Anonymous as a political actor**. 2011. 94 f. Monografia (Bacharelado em Estudos Sociais e Políticos) – Faculdade de Ciências Sociais e Comportamentais, Universidade Flinders, Austrália.

HALL, Stuart. **A identidade cultural na pós-modernidade**. 10. ed. Rio de Janeiro: DP&A, 2005.

HARDT, Michael. A sociedade mundial de controle. In: ALLIEZ, Éric. **Gilles Deleuze**: uma vida filosófica. São Paulo: Ed. 34, 2000. p. 357-372.

HARDT, Michael; NEGRI, Antonio. **Império**. Rio de Janeiro: Record, 2001.

HARDT, Michael; NEGRI, Antonio. **Multidão**: guerra e democracia na era do Império. Rio de Janeiro: Record, 2005.

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

JORDAN, Tim; TAYLOR, Paul A. **Hacktivism and cyberwars**: rebels with a cause? Londres e Nova York: Routledge, 2004.

Juris, Jeffrey S. Networked social movements: global movements for global justice. In: CASTELLS, Manuel (Org.). **The network society**: a cross-cultural perspective. Londres: Edward Elgar, 2004. p. 341-362.

JURIS, Jeffrey; PEREIRA, Inês; FEIXA, Carles. Global citizenship and the new, new social movements: Iberian connections. **Young: Nordic Journal of Youth Research**, v. 17, n. 4, p. 421-442, 2009.

LANDERS, Chris. Serious business: Anonymous takes on Scientology (and doesn't afraid of anything). **Baltimore City Paper**, p. 8, fev. 2008. Disponível em: <http://www2.citypaper.com/news/story.asp?id=15543>. Acesso em: 19 nov. 2011.

LEMOS, André. **Cibercultura**: tecnologia e vida social na cultura contemporânea. Porto Alegre: Sulina, 2002.

LESSIG, Lawrence. **Code and other laws of cyberspace**. 2. ed. Nova York: Basic Books, 2006.

LEVY, Steven. **Hackers**: heroes of the computer revolution. EUA: O'Reilly Media, 2010. Edição em e-book.

MALINI, Fabio. O valor no capitalismo cognitivo e a cultura hacker. **Liinc em Revista**, v. 5, n.2, p. 191-205, 2009.

MANION, Mark; GOODRUM, Abby. Terrorism or civil disobedience: toward a hacktivistic ethic. **Computers and society**, v. 30, n. 2, p. 14-19, jul. 2000.

MANOVICH, Lev. **Software takes command**. Nov. 2008. Disponível em: <http://lab.softwarestudies.com/2008/11/softbook.html>. Acesso em: 15 set. 2012.

MORAIS, Rodrigo de Oliveira. **Informacionalismo e ética hacker**: resistências digitais na sociedade em rede. 116 f. Dissertação (Mestrado em Comunicação e Cultura) – Escola de Comunicação, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2005.

NORTON, Quinn. Anonymous 101: introduction to the lulz. **Wired**, 2011. Disponível em: <http://www.wired.com/threatlevel/2011/11/anonymous-101/all/>. Acesso em: 11 nov. 2011.

ORTIZ, Pedro. México rebelde. In: COGGIOLA, Oswaldo. **América Latina**: encruzilhadas da história contemporânea. São Paulo: Xamã, 2003. p. 269-299.

PELBART, Peter Pál. **Vida capital**: ensaios de biopolítica. São Paulo: Iluminuras, 2011.

RAYMOND, Eric. **A catedral e o bazar**. 1998. Disponível em: <http://www.dominiopublico.gov.br/download/texto/tl000001.pdf>. Acesso em: 15 mar. 2012.

SAMUEL, Alexandra Whitney. **Hacktivism and the future of political particiption**. 2004. 273 f. Tese (Doutorado em Ciência Política) – Departamento de Governo, Universidade Harvard, Cambridge, Massachusetts.

SANTOS, Laymert Garcia dos. **Politizar as novas tecnologias**: o impacto sociotécnico da informação digital e genética. São Paulo: Ed. 34, 2003.

SILVEIRA, Sergio Amadeu da. Ciberativismo, cultura hacker e o individualismo colaborativo. **Revista USP**, São Paulo, n. 86, p. 29-40, ago./out. 2010.

SILVEIRA, Sergio Amadeu da. Poder e anonimato na sociedade de controle. In: _____; JOSGRILBERG, Fábio Botelho. (Orgs.). **Tensões em rede**: os limites da cidadania na internet. São Bernardo do Campo: Universidade Metodista de São Paulo, 2012. p. 109-123.

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.

STERLING, Bruce. **The Hacker Crackdown**: law and disorder on the electronic frontier. Nova York: Bantam, 1993.

THOMAS, Douglas. **Hacker culture**. Minneapolis: University of Minnesota Press, 2002.

UNDERWOOD, Patrick C. **New directions in networked activism and online social movement mobilization**: the case of anonymous and project chanology. 242 f. Dissertação (Mestrado em Sociologia) – Departamento de Sociologia e Antropologia, Universidade de Ohio, 2009.

VEGH, Sandor. **Hacking for democracy**: a study of the internet as a political force and its representation in the mainstream media. 2003. 349 f. Tese (Doutorado em Estudos Americanos) – Departamento de Estudos Americanos, Universidade de Maryland.

WRAY, Stephen. Electronic civil disobedience and the world wide web of hacktivism: a mapping of extraparliamentarian direct action net politics. **Switch**: New Media Journal, n.10. Disponível em: <http://switch.sjsu.edu/web/v4n2/stefan/index.html>. Acesso em: 03/02/2012.

YIN, Robert K. **Estudo de caso**: planejamento e métodos. 2. ed. Porto Alegre: Bookman, 2001.