UNIVERSIDADE FEDERAL DE GOIÁS
FACULDADE DE CIÊNCIAS SOCIAIS
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA POLÍTICA

RODRIGO DE OLIVEIRA SOBREIRA

ANONIMATO, REDES E POLÍTICA: UMA CARTOGRAFIA DO ATIVISMO CYPHERPUNK NO BRASIL

Goiânia
2015

sistema de bibliotecas ufg

PRPG
PRÓ-REITORIA DE PÓS-GRADUAÇÃO

UFG

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TESES E DISSERTAÇÕES NA BIBLIOTECA DIGITAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFG), regulamentada pela Resolução CEPEC nº 832/2007, sem ressarcimento dos direitos autorais, de acordo com a Lei nº 9610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou *download*, a título de divulgação da produção científica brasileira, a partir desta data.

1. Identificação do material bibliográfico: **[X] Dissertação** **[ ] Tese**

2. Identificação da Tese ou Dissertação:

Nome completo do autor: Rodrigo de Oliveira Sobreira

Título do trabalho: ANONIMATO, REDES E POLÍTICA: UMA CARTOGRAFIA DO ATIVISMO CYPHERPUNK NO BRASIL

3. Informações de acesso ao documento:

Concorda com a liberação total do documento [X] SIM [ ] NÃO[1]

Havendo concordância com a disponibilização eletrônica, torna-se imprescindível o envio do(s) arquivo(s) em formato digital PDF da tese ou dissertação.

Rodrigo de Oliveira Sobreira
Assinatura do(a) autor(a)[2]

Ciente e de acordo:

Assinatura do(a) orientador(a)[2]

Data: 18 / 11 / 2017

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. A extensão deste prazo suscita justificativa junto à coordenação do curso. Os dados do documento não serão disponibilizados durante o período de embargo.
Casos de embargo:

- Solicitação de registro de patente;
- Submissão de artigo em revista científica;
- Publicação como capítulo de livro;
- Publicação da dissertação/tese em livro.

[2] A assinatura deve ser escaneada.

RODRIGO DE OLIVEIRA SOBREIRA

ANONIMATO, REDES E POLÍTICA: UMA CARTOGRAFIA DO ATIVISMO CYPHERPUNK NO BRASIL

Dissertação apresentada ao Programa de Pós-Graduação em Ciência Política da Faculdade de Ciências Sociais da Universidade Federal de Goiás, para a obtenção do título de Mestre em Ciência Política.
Linha de pesquisa: Políticas Públicas e Sociedade Civil.
Orientador: Prof. Dr. Carlos Ugo Santander Joo

Goiânia
2015

Ficha de identificação da obra elaborada pelo autor, através do
Programa de Geração Automática do Sistema de Bibliotecas da UFG.

Sobreira, Rodrigo de Oliveira
ANONIMATO, REDES E POLÍTICA: UMA CARTOGRAFIA DO ATIVISMO CYPHERPUNK NO BRASIL [manuscrito] / Rodrigo de Oliveira Sobreira. - 2015.
170 f.: il.

Orientador: Prof. Dr. Carlos Ugo Santander Joo.
Dissertação (Mestrado) - Universidade Federal de Goiás, Faculdade de Ciências Sociais (FCS), Programa de Pós-Graduação em Ciência Política, Goiânia, 2015.
Bibliografia.
Inclui símbolos, gráfico, tabelas, lista de figuras, lista de tabelas.

1. Internet. 2. Ativismo. 3. Cartografia. 4. Privacidade. 5. Vigilância. I. Santander Joo, Carlos Ugo , orient. II. Título.

CDU 32

SERVIÇO PÚBLICO FEDERAL
UNIVERSIDADE FEDERAL DE GOIÁS
FACULDADE DE CIÊNCIAS SOCIAIS
PROGRAMA DE PÓS-GRADUAÇÃO EM CIENCIA POLÍTICA

ATA DA SESSÃO DE JULGAMENTO DA DISSERTAÇÃO DE MESTRADO DE

RODRIGO DE OLIVEIRA SOBREIRA

Aos dezoito dias do mês de maio de 2015, às 09:00 horas, na sala 29, de reunião da Faculdade de História, Campus II, da Universidade Federal de Goiás, realizou-se a sessão de julgamento da Dissertação de Mestrado do mestrando RODRIGO DE OLIVEIRA SOBREIRA, intitulada: *Anonimato, Redes e Política: uma cartografia do ativismo cypherpunks no Brasil.* A Banca Examinadora foi composta, conforme Portaria n.º 24/2015-FCS, de 07 de maio de 2015, pelos seguintes Professores Doutores: Carlos Ugo Santander Joo (Presidente/UFG), Sayonara de Amorim Gonçalves Leal (UnB) e Heloisa Dias Bezerra (UFG) – Suplente: e Francisco Mata Machado Tavares (UFG). O candidato apresentou o trabalho, em seguida os examinadores a arguiram. Às _____ horas, a Banca Examinadora passou a julgamento em sessão secreta, pela qual foram atribuídos ao mestrando os seguintes resultados:

(X) **Aprovado(a)** ( ) Reprovado(a)

Dr. Carlos Ugo Santander Joo

(X) **Aprovado(a)** ( ) Reprovado(a)

Drª. Sayonara de Amorim Gonçalves Leal

(X) **Aprovado(a)** ( ) Reprovado(a)

Drª. Heloisa Dias Bezerra

Resultado Final: Rever a Introdução. Reformular o uso da palavra "impacto"

Reaberta a sessão pública, a Presidente da Banca Examinadora proclamou os resultados e encerrou a sessão, da qual foi lavrada a presente ata que vai assinada por mim, Secretária do Programa de Pós-Graduação em Ciência Política, e pelos membros da Banca Examinadora.

Maria Auxiliadora Gonçalves de Souza _____

“A civilização se tornou complicada
Que ficou tão frágil como um computador
Que se uma criança descobrir
O calcanhar de Aquiles
Com um só palito pára o motor”

(Raul Seixas)

AGRADECIMENTOS

Podemos dizer que estamos sempre no meio do caminho, como na descida de um rio ou em uma estrada que se estende indefinidamente. Do meio do caminho, bem onde fica a pedra de Drummond, abre-se a nossa frente o desconhecido, o inesperado, as possibilidades, a expectativa e a esperança. Porém, mais do que olhar para frente, do meio do caminho podemos olhar para trás, para nós mesmos e para os que até ali caminharam juntos ou marcaram sua passagem na estrada. No fim das contas, somos o resultado de todas essas experiências. Prestar o devido agradecimento e respeito aos que participaram da caminhada é mais que necessário: é uma honra. Portanto, nesse momento registro meus sinceros agradecimentos:

Ao meu pai, Roberto Sobreira, exemplo de força, caráter e honestidade. Um homem genial que inspira a todos nós.

À minha mãe, Diná Miriam, pelo seu carinho, cuidado, paciência e amor. Sua dedicação e compromisso comigo e meu irmão é o que nos trouxe até aqui.

Ao meu irmão, Rogério Sobreira, parceiro de todas as horas e todos os palcos. Não poderia haver parceria melhor que essa. Juntos até o infinito.

Ao meu orientador, Professor Carlos Ugo Santander, pelas boas conversas e conselhos. O maestro que permitiu a execução dessa pesquisa com a dose de liberdade e ousadia que ela necessitava. Mais do que um professor, um amigo que levarei para a vida.

Ao Professor e amigo Francisco Tavares pelos instigantes debates em sala, pelas horas de conversa pelos corredores, os litros de bom café e, principalmente, pela inspiração e motivação em defesa de um mundo melhor. Extendo o agradecimento a todos os coleg@s do PROLUTA.

À Professora Heloísa Bezerra pelos indispensáveis conselhos para a realização dessa pesquisa. Boa parte do desenho desse trabalho se deve a observações preciosas sobre as possibilidades de abordagem do tema. Agradeço também a participação nas bancas de qualificação e defesa dessa dissertação.

Aos professores do Programa de Pós-Graduação em Ciência Política pela sua dedicação e motivação na nobre tarefa de mostrar os pedregosos caminhos da pesquisa em política e formar os futuros responsáveis pela compreensão de fenômenos tão complexos. Relembro uma frase que sintetiza a dificuldade e grandeza de tal esforço: “Deus deu a Física os problemas fáceis”.

Aos colegas do mestrado por compartilharem comigo todos esses momentos de intenso aprendizado e, em alguns momentos, desespero. O caminho foi mais agradável graças a vocês. Agradeço de maneira especial Andrey Pimentel e Hugo Henry, amigos para toda a vida com quem tive a honra de conviver e aprender durante esses dois anos.

Aos meus amigos que sempre me dão forças, ânimo e alegrias. O que eu aprendi e continuo aprendendo com todos vocês está além do que qualquer escola pode ensinar: amizade verdadeira em forma de amor fraternal.

Aos ativistas da Cryptorave por terem me recebido tão bem em seu evento, mostrando que além de bytes e fibra ótica, o que realmente nos une é o espírito humano.

À Marlene Marques e Vanessa Marques pela consideração, amizade e por sempre me receberem tão bem em sua casa. Obrigado pelo apoio e confiança.

E, por último, à Juliana, pelo amor, cuidado e carinho. Um amor que continua crescendo desde o primeiro dia. Um cuidado que se faz constante e insubstituível. Um carinho sem fim. A mão que me guiou nos momentos mais difíceis e não me deixou desistir. Para você dedico este trabalho e todo meu amor.

RESUMO

O avanço tecnológico proporcionado pela revolução da informática afetou diretamente diversos campos da vida humana. Novas formas de interação, diminuição da barreira tempo-espaço, reconfigurações nas formas produtivas. A internet representa uma das pontas mais conhecidas desse processo. A popularização da web, a partir de década de 1990, foi acompanhada por uma crescente preocupação por parte de governos e teóricos sobre suas consequências. O ativismo político encontra na tecnologia, desde os anos 1980, novas formas de expressão e ação. No início do século XXI, o processo de radicalização de alguns movimentos e o debate sobre sociedade de controle e vigilância se intensificou. A organização Wikileaks e os vazamentos de documentos da NSA (National Security Agency), por exemplo, demonstraram o poder e a relevância de tais grupos. Dessa forma, o presente trabalho pretende avaliar e mapear o impacto desse tipo de ativismo no Brasil. Por se tratar de uma pesquisa exploratória, a metodologia cartográfica será utilizada com o objetivo de fornecer um panorama do ativismo cypherpunk no Brasil. Optou-se pela metodologia cartográfica visando apresentar uma visão do impacto do discurso ativista cypherpunks no Brasil, tentando encontrar os principais disseminadores de discurso e ação e compreendendo tal processo como uma construção constante. Tal metodologia permite tanto o tratamento de dados robustos, obtidos por meio de mineração nas redes, quanto uma análise qualitativa de dados obtidos em fontes documentais. No Brasil, o Laboratório de Estudos sobre Imagem e Cibercultura (LABIC) da Universidade Federal do Espírito Santo tem se destacado como pólo de desenvolvimento de pesquisas e metodologias para cartografar as controvérsias na internet. Além da discussão teórica, o trabalho opera com data mining em redes sociais, especialmente Twitter. O objetivo é levantar dados primários sobre o debate sobre o tema no Brasil. Para isso, softwares de mineração de dados capturam tweets (yourTwapperKeeper) com palavras-chave determinadas pela discussão teórica. Em seguida, os dados são tratados e inseridos em um software de visualização (Gephi) que gera o "mapa" da rede e do debate.

Palavras-chave: Internet; Ativismo; Cartografia; Privacidade; Vigilância.

ABSTRACT

Technological advances from the information revolution have affected various fields of human life. New forms of interaction in productive ways. The internet is one of the cornerstones of this process. The popularization of the web, since the 1990s, was accompanied by a growing concern by governments and scholars about its consequences. The political activism has found on technology, since the 1980s, new forms of expression and action. In the early twenty-first century, the process of radicalization of some movements and the debate on society of control and surveillance has intensified. The Wikileaks organization and the NSA's (National Security Agency) documents leaked by Edward Snowden, for example, have shown the power and relevance of such groups. Thus, this study aims to assess and map the impact of this type of activism in Brazil. Since this is an exploratory research, the cartographic methodology will be used in order to provide an overview of cypherpunk activism in Brazil. We have chosen the cartographic methodology to present an overview of the impact of cypherpunks' discourse in Brazil. The research tries to find the main disseminators of speech and action and understanding this process as a constant construction. This methodology allows both the treatment of robust data, obtained through mining in networks, as a qualitative analysis of data from documentary sources. In addition to the theoretical discussion, this work operates with data mining in social networks, especially Twitter. The goal is to obtain primary data on the subject in Brazil. Thus, data mining software capture tweets (yourTwapperKeeper) with keywords determined by theoretical discussion. Then the data are processed and entered into a visualization software (Gephi) that generates the "map" of the network and debate.

Key words: Internet; Activism; Cartography; Privacy; Surveillance;

RESUMEN

Los avances tecnológicos de la revolución de la información han afectado a diversos campos de la vida humana. Las nuevas formas de interacción de manera productiva. El Internet es una de las piedras angulares de este proceso. La popularización de la web, desde la década de 1990, fue acompañado por una creciente preocupación por los gobiernos y académicos sobre sus consecuencias. El activismo político ha encontrado en la tecnología, desde la década de 1980, las nuevas formas de expresión y de acción. A principios del siglo XXI, el proceso de radicalización de algunos movimientos y el debate sobre la sociedad de control y vigilancia se ha intensificado. La organización Wikileaks y los documentos de la NSA (Agencia de Seguridad Nacional) filtrada por Edward Snowden, por ejemplo, han demostrado el poder y la relevancia de tales grupos. Así, este estudio tiene como objetivo evaluar y cartografiar el impacto de este tipo de activismo en Brasil. Como se trata de una investigación exploratoria, la metodología cartográfica se utilizará con el fin de proporcionar una visión general de activismo cypherpunk en Brasil. Hemos elegido la metodología cartográfica para presentar una visión general del impacto del discurso cypherpunks en Brasil. La investigación trata de encontrar los principales difusores de la palabra y la acción y la comprensión de este proceso como una construcción constante. Esta metodología permite que tanto el tratamiento de datos sólidos, obtenidos a través de la minería en las redes, como un análisis cualitativo de los datos de las fuentes documentales. Además de la discusión teórica, este trabajo opera con la minería de datos en las redes sociales, especialmente Twitter. El objetivo es la obtención de datos primarios sobre el tema en Brasil. Por lo tanto, la minería de datos de captura de los tweets de software (yourTwapperKeeper) con palabras clave determinadas por la discusión teórica. A continuación, los datos se procesan y se introdujeron en un software de visualización (Gephi) que genera el "mapa" de la red y el debate.

Palabras clave: Internet; Activismo; Cartografía; Privacidad; Vigilancia.

LISTA DE FIGURAS

LISTA DE QUADROS

Sumário

1 INTRODUÇÃO

O mundo contemporâneo instiga a curiosidade e desafia a capacidade de interpretação e análise. A realidade difusa e fragmentada e, ao mesmo tempo, unida por inúmeras redes constitui-se em um dos mais fascinantes objetos de análise. A busca por respostas em um mundo onde tudo parece estar ao alcance da mão, mas nada é suficientemente sólido para oferecer segurança, é um caminho denso e complicado de se percorrer. O mundo trabalhando em uma mesma unidade de tempo, mas em diferentes unidades de espaço têm sérias consequências para as relações políticas, humanas, econômicas e sociais.

As relações políticas são alteradas no contexto da mundialização. As forças de atração e repulsão, que antes eram visíveis e bem delimitadas, se diluem em meio à nova configuração de forças. O pensamento contestatório, que antes enxergava na rigidez do sistema econômico e social o inimigo a ser combatido, se depara com novas demandas, as quais requerem novos modelos de análises e ação.

A mundialização afetou, em diferentes escalas, todas as populações do mundo. A transferência dos centros decisórios e dos espaços públicos para a escala global interferiu na maneira de ver, agir e pensar sobre o mundo. As formas de dominação passaram a operar globalmente, potencializada pelo poder do financeiro, construindo uma nova configuração hegemônica.

Por outro lado, os movimentos de resistência ou movimentos anti-sistêmicos, na definição de Wallerstein (2004), também passam a se articular em escala global. Os diversos movimentos identitários, culturais, de luta por direitos humanos e políticos percebem a nova configuração global do poder hegemônico e, devido a isso, iniciam um novo processo de organização, em favor da organização em rede, como forma de resistência e de construção contra-hegemônica.

Desde o primeiro Fórum Social Mundial em 2001, até os violentos protestos contra a crise europeia em 2012, o que se observa são novas formas de organização e atuação dos movimentos anti-sistêmicos ou antirregime. Os novos embates contra-hegemônicos surgem de maneira inesperada, como o caso do *Wikileaks*, no qual o vazamento de informações

sigilosas, defendendo o acesso da população mundial à informação, constitui a principal forma de ação e resistência. Novos elementos são inseridos como o *hacker ativismo*, levandoa internet a assumir um papel central nas articulações desses movimentos. Os diversos movimentos de Ocupação (*Occupy*) ao redor do mundo, articulados através das redes, levantam novas demandas sociais e políticas, ainda que de forma difusa, que escapam dos domínios da política institucional.

Nesse contexto, o papel desempenhado pela ação política via internet merece ser destacado. Redes sociais e sites de compartilhamento desempenham um importante papel na mobilização e na construção do dissenso, constituindo uma Esfera Pública Interconectada. Por outro lado, outros tipos de ações são desenvolvidas nas redes, como: invasões, vazamento de informação, ataque a sites governamentais ou de corporações. Essas ações constituem uma força específica de atuação política via internet: ação direta, não-violenta, visando fins políticos. Diversos grupos com táticas distintas operam politicamente nas redes: ciberativistas, hackerativistas, cypherpunks, ativistas de software livre.

No que se refere ao primeiro tipo de ação, estudos têm se concentrado em mapear o efeito das redes nas mobilizações e na "caixa de ressonância", isto é, o impacto no mundo virtual das disputas do mundo real. Dessa forma, pretende-se propor, incialmente, a seguinte pergunta: quais os debates e controvérsias em torno da relação entre ativismo e internet no Brasil?

Considerando as diversas formas de atuação de grupos distintos, faz-se necessário um aprofundamento da questão. Sob o rótulo de ciberativismo encontram-se diferentes concepções de ação. Conforme Sérgio Amadeu da Silveira (2010),

> Por ciberativismo podemos denominar um conjunto de práticas em defesa de causas políticas, socioambientais, sociotecnológicas e culturais, realizadas nas redes cibernéticas, principalmente na Internet. O ciberativismo se confunde com a própria expansão da rede mundial de computadores. Ele influenciou decisivamente grande parte da dinâmica e das definições sobre os principais protocolos de comunicação utilizados na conformação da Internet. É possível posicionar os diversos grupos e atividades do ciberativismo situados mais à esquerda ou mais à direita. Todavia, esse enquadramento tradicional, que orientou a divisão política das ações e ideologias no mundo industrial, encontra crescente dificuldade operacional diante de muitas ações na sociedade informacional. (SILVEIRA, p. 31, 2010)

Nesse sentido, ações conduzidas na internet por ONGs, como o Greenpeace e a Anistia Internacional, com a intenção de atrair atenção para determinado assunto podem ser enquadradas no termo ciberativismo. Esse tipo de ação utiliza as redes como um canal de

vocalização, no qual exprimem suas causas e razões, de forma a forçarem a entrada de temas no debate público visando mudanças institucionais. Ainda que extremamente interessante e instigante esse tipo de ativismo não interessa a presente pesquisa.

Por outro lado, outros grupos utilizam a rede como meio essencial de ação, realizando ataques e vazamentos de informação. Dentre esses grupos, os Cypherpunks[1] têm estado em maior evidência na luta por seus objetivos graças, principalmente, ao Wikileaks. Desde o advento do site dedicado ao vazamento de informações sigilosas de governos e organizações, Julian Assange tem sido o porta-voz do movimento Cypherpunk, buscando demonstrar, por um lado, como governos e corporações violam direitos dos cidadãos e, por outro, como cidadãos, movimentos sociais e a sociedade civil como um todo pode se proteger e contra-atacar. Nas palavras de Assange (2013):

> O mundo não está deslizando, mas avançando a passos largos na direção de uma nova distopia transnacional. Esse fato não tem sido reconhecido de maneira adequada fora dos círculos de segurança nacional. Antes, tem sido encoberto pelo sigilo, pela complexidade e pela escala. A internet, nossa maior ferramenta de emancipação, está sendo transformada no mais perigoso facilitador do totalitarismo que já vimos. A internet é uma ameaça à civilização humana. (ASSANGE, 2013, p. 25)

Considerando isso, a pergunta pode ser reorganizada da seguinte forma: qual o impacto do discurso cypherpunks, em especial sobre privacidade e anonimato, no debate sobre políticas e internet no Brasil?

Em 2013, a discussão sobre internet e política obteve maior repercussão no Brasil devido ao vazamento de informações da NSA (National Security Agency), as quais comprovavam a espionagem de políticos e empresários brasileiros por parte do governo norte-americano. A partir desse fato, grupos de hackerativistas passaram a ter visibilidade com seu discurso de privacidade para os cidadãos e transparência para os governos.

Com o aumento do debate público a respeito do tema, ativistas brasileiros passaram a ter visibilidade e novos grupos se organizaram politicamente como forma de divulgar a luta criptográfica. Os dois principais exemplos são a CryptoParty[2], uma rede de ativistas e um

[1] O nome é um trocadilho com o termo Cyberpunk, criado por William Gibson. Cypher é uma referência a criptografia, principal instrumento de luta do movimento.
[2] https://cryptoparty.inf.br/

evento realizado com o objetivo de disseminar técnicas de criptografia, e a Actantes[3], organização que reúne ativistas e organiza ações diretas. Conforme o Manifesto Actante:

> Somos um coletivo que organiza ações diretas pela comunicação livre nas redes digitais. Diante da sociedade de controle lutamos pela privacidade e pelo direito a navegação anônima.
>
> (...)
>
> Somos actantes para hackear a sociedade de controle, para anular a biopolítica de modulação, para organizar a defesa da liberdade, da privacidade e da diversidade. (ACTANTES, 2013, online).

Esses grupos abrem novas perspectivas para o estudo da Ciência Política brasileira. Ao se voltar para um fenômeno tão complexo e instigante, a ciência política pode avançar em novas possibilidades de interpretação e ampliar seu arcabouço teorético-metodológico. Por isso, pode-se propor a seguinte pergunta: Quais os principais atores, redes e controvérsias impactadas pelo ativimo cypherpunk no Brasil?

O objetivo central da pesquisa é, a partir de uma metodologia cartográfica, mapear as principais controvérsias e os atores centrais no debate travado na internet brasileira. Para tanto, é necessário contemplar alguns objetivos específicos: a) discutir teoricamente o poder cibernético, o ciberativismo e os potencial de controle e resistência da rede; b) discutir o conceito de privacidade, suas garantias e violações; c) apresentar uma cartografia do debate sobre o tema na internet, apontando as principais autoridades e temas em questão.

O direito de resistência está implícito na concepção política ocidental, porém, toda vez em que é necessário resistir, sua forma de ação é sempre questionada. Isso indica, provavelmente, uma inadequação institucional para lidar com o dissenso. As democracias contemporâneas, apegadas a uma institucionalização instrumental, ainda não criaram os canais para a participação popular como forma de aprimoramento político e construção de direitos.Segundo a definição de Safatle (2012):

> A democracia admite o caráter "descontrutível" do Direito, e ela o admite pelo reconhecimento daquilo que poderíamos chamar de legalidade da "violação política". Pacifistas que sentam a frente de bases militares a fim de impedir que armamentos sejam deslocados (afrontando assim a liberdade de circulação), ecologistas que seguem navios cheios de lixo radiativo a fim de impedir que ele seja despejado no mar, trabalhadores que fazem piquetes em frente a fábricas para criar situações que lhes permitam negociar com mais força exigências de melhorias de condições de trabalho, cidadão que protegem imigrantes sem-papéis, ocupações de prédios públicos feitas em nome de novas formas de atuação estatal, trabalhadores sem-terra que invadem fazendas improdutivas, Antígona que enterra seu irmão: em

[3] http://actantes.org.br/

> todos esses casos, o Estado de Direito é quebrado em nome de um embate em torno da Justiça. (...) Uma sociedade que tem medo de tais momentos, que não é mais capaz de compreendê-los, é uma sociedade que procura reduzir a política a um mero acordo referente às leis que temos e aos meios que dispomos para mudá-las. (SAFATLE, 2012, p. 48)

Ao admitir a "violação política", Safatle toca em um ponto importante do debate: o direito do povo de resistir a regimes ou leis injustas. O princípio básico evocado na fundação da Era Contemporânea e do Estado de Direito, segundo o qual o poder emana do povo e este, enquanto soberano, pode revogar a ordem vigente. Atuando no limiar da legalidade, muitos hackerativistas se valem dessa premissa de "violação política" da lei. Pode-se afirmar que a a ação direta virtual é uma transposição do direito de resistência para o mundo cibernético, assim como o debate gerado em torno do tema constitui um esforço para a desobstrução dos canais tradicionais de comunicação e ampliação do alcance das demandas.

Um fenômeno tão atual e relevante ainda carece de pesquisas e estudos no Brasil. Conforme levantamento feito por Araújo (2011) sobre a produção acadêmica brasileira sobre o tema:

> Seguindo os critérios citados anteriormente, foram selecionados 22 trabalhos produzidos entre os anos de 2000 e 2010, sendo oito do Banco de Teses da Capes, nove do Portcom e cinco dos anais da COMPÓS. Estes trabalhos representam diferentes tipos de pesquisa, estando representados na amostra uma tese de doutorado, sete dissertações de mestrado e 14 artigos científicos de pesquisadores de todos os níveis. (ARAÚJO, 2011, p. 10)

Esse trabalho de levantamento do estado da arte da pesquisa sobre ciberativismo no Brasil demonstra a necessidade de se ampliar os estudos sobre o tema, aumentar o debate e diversificar as abordagens. Ainda nesse mesmo estudo, percebe-se que a Ciência Política brasileira praticamente ignorou o fenômeno: "Como era previsível, houve a predominância de trabalhos com área de origem no campo da comunicação (20), mas também foram encontrados trabalhos relacionados à Sociologia (1) e Artes (1)." (Araújo, 2011, p.10).

Por se tratar de uma pesquisa exploratória, a metodologia cartográfica será utilizada com o objetivo de fornecer um panorama do ativismo cypherpunk no Brasil. Optou-se pela metodologia cartográfica visando apresentar uma visão do impacto do discurso ativista cypherpunks no Brasil, tentando encontrar os principais disseminadores de discurso e ação e compreendendo tal processo como uma construção constante. Tal metodologia permite tanto o tratamento de dados robustos, obtidos por meio de mineração nas redes, quanto uma análise

qualitativa de dados obtidos em fontes documentais. Conforme Venturini (2010), a natureza dos dados na internet, sua rastreabilidade e agregabilidade, fornecm condições mais favoráveis para a realização de cartografias. Por rastreabilidade compreendem-se os dados e metadados gerados a cada interação e passíveis de captura e análise. Já agregrabilidade faz referência a capacidade de reunir uma enorme quantidade de dados de foma legível para a análise dos fatos. De forma a garantir a replicabilidade da pesquisa, os dados utilizados estão disponíveis em um link indicado nas Referências Bibliográficas.

No Brasil, o Laboratório de Estudos sobre Imagem e Cibercultura[4] (LABIC) da Universidade Federal do Espírito Santo tem se destacado como polo de desenvolvimento de pesquisas e metodologias para cartografar as controvérsias na internet. Destaca-se, ainda, o trabalho teórico desenvolvido no Brasil por PASSOS, KASTRUP & ESCÓSSIA (2009), ROLNIK (1989) e FONSECA & KIRST (2003). Em linhas gerais, tais trabalhos buscam desenvolver o método cartográfico a partir das indicações e construções de Deleuze e Guattari na obra Mil Platôs (1995) e em releituras do pensamento foucaultiano. Esses estudos, em especial aqueles relacionados a internet, também sofrem grande influência do pensamento do MACOSPOL (Mapping Controversies on Science for Politics), projeto de pesquisa multidisciplinar europeu sob a coordenação do pesquisador Bruno Latour.

Por fim, vale ressaltar que a presente pesquisa está vinculada ao Programa de Pesquisa sobre Ativismo em Perspectiva Comparada (PROLUTA) do Núcleo de Estudos e Pesquisas em América Latina e Política Comparada, projeto multidisciplinar dedicado a estudar o ativismo e as lutas antirregime contemporâneas em suas diversas formas de expressão e ação.

[4] http://www.labic.net/

2 PODER CIBERNÉTICO E ATIVISMO POLÍTICO

O poder é um conceito central na discussão política ao longo do tempo. A contemporaneidade imprime novas formas de relação e exercício de poder em diferentes esferas. Compreender tais mudanças é necessário para proceder com análises mais apuradas e próximas da realidade. Nesse sentido, o presente capítulo buscará discutir o impacto do poder cibernético no ativismo político. Para isso, dedica-se um primeiro tópico a uma discussão sobre o poder cibernético e suas principais formas de expressão. Em seguida, apresenta-se o debate sobre como protocolos técnicos, construídos de forma lógica e matemática, passam a desempenhar um papel político em uma sociedade de controle. O tópico seguinte trata da junção do poder cibernético estatal a um aparato de controle, isto é, como a doutrina de segurança nacional e estratégia de defesa aliadas ao poder político dos protocolos passa a desempenhar um papel central na modulação do biopoder nas sociedades contemporâneas. Devido à sua proeminência como potência militar e sua influência na própria estrutura da rede este tópico se concentra em analisar a doutrina norte-americana.

Após discutir o poder cibernético e suas possibilidades de controle, busca-se apresentar como os ativistas se apropriaram das tecnologias a favor de seus ideais. Ressalta-se o potencial ambivalente dos aparatos cibernéticos que, por um lado, servem como instrumentos de controle, por outro, abrem novas possibilidades de interação e resistência. Em seguida, apresenta-se uma breve discussão sobre Esfera Pública e Esfera Pública Interconectada com o objetivo de separar possibilidades de ativismo na internet. Enquanto grupos buscam colocar em pauta e influenciar a debate público sobre determinado assunto, outros entendem que a própria estrutura da rede, dominada por protocolos técnicos que afetam politicamente seu funcionamento e militarizada por meio de uma doutrina de segurança, deve ser o próprio alvo do ativismo. Por fim, apresenta-se a relação entre sociedade civil e poder cibernético, tratando de alguns exemplos recentes de atuação de ativistas.

2.1 O CONCEITO DE PODER CIBERNÉTICO

O conceito de poder cibernético (*cyberpower*) é uma construção recente e tem animado em novo debate teórico. Antes de tudo, ele se constitui em uma nova expressão do poder. Sendo necessário, assim, compreender esse conceito a luz de uma configuração de possibilidades de fontes e exercício do poder. O cyberpower é fruto de mudanças tecnológicas

que abriram novos campos de influência e conflitos nos quais diversos atores disputam espaço. Por isso, cyberpower é um tipo de poder que possui como fonte o ciberespaço e, por essa razão, é naturalmente difuso.

Dentro do debate sobre o cyberpower, o autor Joseph Nye é um dos principais teóricos a tratar do tema. Em sua obra "O Futuro do Poder" (2012), o poder cibernético surge como uma categoria essencial para se compreender as relações entre Estados e sociedade civil no século XXI. Outros autores, como, por exemplo, Andrew F. Krepinevich (2012), tem se dedicado ao estudo do poder cibernético com um viés securitário, isto é, como forma de combate e arma estratégica acessória ao poder bélico. Dessa forma, antes de debater o *cyberpower* em si, é necessário apresentar um conceito de poder e seus três aspectos relacionais.

Por definição básica, poder é a capacidade de realizar algo desejado ou de resistir a mudanças. No entanto, a categoria de poder é amplamente usada e seu significado não é fácil de ser definido. Nesse sentido, cientistas políticos buscaram elaborar definições que pudessem operacionalizar o conceito de forma que seu uso fosse mais amplamente aceito. A partir desses estudos, chegaram aos três aspectos relacionais do poder, isto é, as três faces nas quais o poder se manifesta e é exercido.

A primeira face do poder foi definida por Robert Dahl na década de 1950. Essa face do poder pode ser definida como a "capacidade de conseguir que os outros ajam de maneiras contrárias às suas preferências e estratégias iniciais" (NYE, 2012, p. 33). É uma das definições mais amplamente aceitas e conhecidas do poder, na qual a coerção e/ou a barganha alteram as preferências iniciais da outra parte envolvida.

Após essa definição de Dahl, outros cientistas políticos ampliaram esse conceito e desenvolveram a chamada segunda face do poder. Essa face baseia-se no controle da agenda. Isto é, "se as ideias e as instituições podem ser usadas para ajustar a agenda para a ação de uma maneira que faça as preferências dos outros parecerem irrelevantes ou fora dos limites, talvez jamais seja necessário pressioná-los" (NYE, 2012, p. 34). Esse aspecto do poder concentra-se em manter fora da discussão alguns aspectos e fazer com o que a outra parte nem mesmo os elabore enquanto preferências ou estratégias.

Por fim, a terceira face do poder, aperfeiçoada teoricamente na década de 1970, constitui-se em moldar as preferências básicas dos atores antes mesmo delas serem

elaboradas: “se conseguir que os outros queiram o mesmo que você, não será necessário anular seus desejos iniciais” (NYE, 2012, p. 35). Dessa forma, o sujeito que exerce o poder influencia as estruturas da formação de preferência dos outros sujeitos, submetendo-os a desejos pré-concebidos.

O que é inerente a um conceito de poder é que ele está submetido a um contexto no qual sua fonte se localiza. Por isso, por exemplo, o poder naval deriva da capacidade de domínio dos mares; o poder aéreo depende do controle das tecnologias aeronáuticas; e o poder econômico tem que ser sustentado pela capacidade produtiva. Nesse sentido, o poder cibernético é derivado de seu contexto específico: o ciberespaço. O conjunto de ferramentas tecnológicas, redes de comunicações, fluxos de informação formam um espaço no qual o controle ou a forma de utilização desses mecanismos confere poder ao ator que o domina.

A grande questão que envolve o poder cibernético é a sua difusão. O domínio das tecnologias necessárias para se operar no ciberespaço é uma preocupação presente na agenda de quase todos os Estados no mundo, porém o monopólio dessas ferramentas é algo distante e quase impossível de ser alcançado. Devido à própria arquitetura da rede, descentralizada e aberta, é possível que diversos atores entrem em cena com um custo de operação muito baixo e um alto potencial de ação.

> Such cyber transformations are still fanciful, but a new information revolution is changing the nature of power and increasing its diffusion. States will remain the dominant actor on the world stage, but they will find the stage far more crowded and difficult to control. A much larger part of the population both within and among countries has access to the power that comes from information. Governments have always worried about the flow and control of information, and the current period is not the first to be strongly affected by dramatic changes in information technology. (NYE, 2010, p. 1).

Dessa forma, o poder cibernético se apresenta de forma difusa, com vários atores potenciais interagindo entre si de forma cooperativa ou não. Os Estados são parte integrante desse processo e desempenham papel preponderante. A infraestrutura física necessária para a existência do ciberespaço encontra-se sobre a jurisdição de diversos Estados, podendo, assim, ser afetada pela coerção estatal e regulada pela força da lei. Por outro lado, vários grupos podem se valer de poder cibernético com objetivos diversos (ativismo político, terrorismo, atividades criminosas). Por isso, Nye destaca a crescente dificuldade dos Estados em controlar totalmente essa fonte de poder.

Após apresentar as três faces do poder e o argumento de que o poder se sustenta em um determinado contexto – nesse caso, o ciberespaço – é necessário um conceito de poder cibernético. Em primeiro lugar, o poder cibernético depende de uma série recursos relacionados à criação, controle e distribuição de informações por meio de computadores e outros meios eletrônicos: a infraestrutura, as redes, os softwares e o capital humano envolvido. Dessa forma, pode-se definir poder cibernético (cyberpower) como "a habilidade de obter o resultado preferido através do uso de recursos informacionais eletronicamente interconectados no domínio do ciberespaço" [5] (NYE, 2010, p. 3). Em uma definição um pouco mais abrangente, poder cibernético é "a habilidade de usar o ciberespaço para criar vantagens e influenciar eventos em outros ambientes operacionais e através dos instrumentos de poder" [6] (NYE, 2010, p.4).

O poder cibernético, enquanto forma de exercício de poder baseado no ciberespaço, também apresenta as três faces discutidas acima. O poder cibernético pode atuar alterando as preferências dos envolvidos (primeira face); pode alterar a agenda dos afetados (segunda face); e, por fim, pode moldar as preferências de forma que estas estejam condicionadas a uma preferência exterior. Da mesma forma, cada face do poder cibernético ocorre como *soft power* ou *hard power*. No ciberespaço, as ações podem visar o convencimento e a influência através do discurso, formando uma zona de atração (*soft power*); ou podem se valer de ataques à própria estrutura da rede e dos dispositivos envolvidos (*hard power*).

A primeira face do poder cibernético se manifesta como *hard power* por meio de ataques a servidores, vírus e coerção a ativistas; já enquanto *soft power*, se manifesta como campanhas públicas pela internet, propaganda governamental ou antirregime e aliciamento de militantes. A segunda face do poder cibernético atua como *hard power* ao criar filtros, firewall e pressões para que algumas ideias sejam excluídas; por outro lado, atua como *soft power* monitoramento dos mecanismos de busca, regras para nomes de domínios e para a criação de softwares. Por último, a terceira face do poder cibernético é *hard power* ao ameaçar usuários que distribuem conteúdo ofensivo; e é *soft power* ao desenvolver preferências, como, por exemplo, aversão total a ideias nazifascistas (NYE, 2010, p. 7)

[5] Tradução livre de: "the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain".
[6] Tradução livre de: "the ability to use cyberspace to create advantages and influence events in other operational environments and across the .instruments of power."

Dessa forma, para alterar preferências os envolvidos podem atacar computadores e redes ou disseminarem discursos. Para controlar a agenda os concernidos podem cercear o acesso a determinadas informações ou monitorar as buscas. Por fim, para evitar que algumas preferências sejam sequer cogitadas, o poder cibernético pode ameaçar determinados conteúdos e bloquear o acesso a certos discursos.

A partir disso, a fonte do poder no ciberespaço é um ponto importante de ser compreendido. Estados, organizações e indivíduos podem atuar no ciberespaço e exercer poder de maneiras distintas. É inegável o poder do Estado dentro do ciberespaço, suas principais fontes são: desenvolvimento e o suporte da infraestrutura; coerção legal; controle do mercado; recursos militares para ciberataques; reputação de legitimidade. As organizações baseiam seu poder em: grandes orçamentos e capital humano; transnacionalidade; desenvolvimento de produtos; reputação. Por fim, os indivíduos têm como principais recursos: o baixo custo para entrar no ciberespaço; facilidade de sair e anonimato.

Por outro lado, Estados são vulneráveis em relação à alta dependência de em sistemas complexos e a instabilidade política. Organizações sofrem com problemas legais, questões de propriedade intelectual e quedas de sistemas. Por fim, indivíduos são ameaçados pelas coerções legais e ilegais conduzidas por governos e organizações.

Assim, é possível estabelecer um panorama do poder cibernético, expondo em linhas gerais seu conceito, contexto, fontes de recursos e de fragilidade. A grande novidade dessa forma de poder, ainda muito recente em comparação a outras, é possibilidade da ação individual ou de pequenas organizações com um potencial próximo ao de grandes potências. Guardadas as devidas proporções, um ataque de ciberterroristas pode afetar comunicações, sistemas de informação ou até mesmo o controle da energia elétrica de um país, causando danos reais à economia e a população. Por outro lado, os chamados hackerativistas podem influenciar decisões políticas e abrir um amplo debate internacional. Por esse motivo, entender como o ativismo político se utilizou da evolução tecnológica para seus objetivos é essencial para se compreender como os indivíduos podem se valer do poder cibernético em sua ação política.

2.2 PROTOCOLOS TÉCNICOS COMO INSTRUMENTO POLÍTICO E SOCIEDADE DE CONTROLE

A arquitetura da internet, isto é, o diagrama das relações entre os computadores em rede, determina uma série de possibilidades de interação. Nesse universo de condicionantes tecnológicos, a gramática básica dessas interações é o conceito de protocolo. Conforme, Sérgio Amadeu da Silveira (2009a) define:

> É possível afirmar de modo mais sintético que a 'arquitetura de rede' é a descrição dos formatos de dados e dos procedimentos usados para a comunicação entre seus nós ou pontos. Ela pode ser decomposta em dois elementos importantes: os protocolos, que trazem padrões, regras e procedimentos de comunicação, e a topologia da rede. Protocolos são essenciais na comunicação em rede, são um conjunto de regras e convenções para a comunicação entre os dispositivos dessa rede. Um protocolo inclui formatação de regras que especificam como os dados são transformados em mensagens. Também pode incluir convenções de como definir mensagens de aviso ou realizar a compressão de dados de modo confiável para apoiar uma rede de comunicação de alto desempenho. (SILVEIRA, 2009a, p.2)

Por protocolo entende-se a série de procedimentos, recomendações e regras que determinam uma operação técnica: "computer protocols govern how specific technologies are agreed to, adopted, implemented, and ultimately used by people around the world". (GALLOWAY, 2004, p. 7). Visto dessa forma, um protocolo é uma linguagem lógica e formal que opera permitindo a comunicação entre computadores. Dessa maneira, o protocolo comprime a mensagem e a transmite sem distinção sobre seu conteúdo, garantindo assim a neutralidade da rede.

Por outro lado, conforme defende Alexander Galloway (2004), os principais protocolos da internet operam gerando uma tensão. Por um lado, um altamente hierárquico e controlado, o protocolo DNS[7]. Por outro lado, o protocolo TCP/IP[8] que permite conexões horizontais entre quaisquer computadores. A tensão entre os protocolos e, consequentemente,

---

[7] "The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates information from domain names with each of the assigned entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet. This article presents a functional description of the Domain Name System. Broader usage and industry aspects are captured on the Domain name page". Disponível em: http://en.wikipedia.org/wiki/DNS (acesso em 08/06/2014)

[8] "The Internet protocol suite is the networking model and a group of communications protocols used for the Internet and similar networks. It is commonly known as TCP/IP, because its most important protocols, the Transmission Control Protocol (TCP) and the Internet Protocol (IP), were the first networking protocols defined in this standard. It is occasionally known as the DoD model, because the development of the networking model was funded by DARPA, an agency of the United States Department of Defense." Disponível em: http://en.wikipedia.org/wiki/TCP/IP (acesso em 08/06/2014)

as formas de conexão com a rede, é a razão da ambivalência da tecnologia. Enquanto estrutura rígida vertical (DNS) a rede é um instrumento de controle; enquanto forma de conexão horizontal, anárquica e sem regulação, a internet é um instrumento de organização política. Nesse sentindo, um protocolo técnico passa a desempenhar um papel político.

Entender como os protocolos funcionam e sua gramática específica enquanto linguagem é fundamental para se entender como o ativismo e a ação política se apropriam de tais tecnologias e, devido à ambivalência inerente a esses processos, se tornam alvos de instrumentos de controle. Mais ainda, como a consciência desse fato condiciona novas formas de ação política como a criptografia.

Galloway (2004) defende que o protocolo é criado a partir da contradição entre duas máquinas: uma hierárquica e outra anárquica. Dessa contradição, nasce a possibilidade de controle e, ao mesmo tempo, de organização e resistência.

> What contributes to this misconception (that the Internet is chaotic rather than highly controlled), I suggest, is that protocol is based on a contradiction between two opposing machines: One machine radically distributes control into autonomous locales, the other machine focuses control into rigidly defined hierarchies. The tension between these two machines—a dialectical tension—creates a hospitable climate for protocological control. (GALLOWAY, 2004, p. 8)

A máquina que distribui o controle entre os vários nós da rede opera sob o protocolo TCP/IP. Seu design permite que um computador se comunique diretamente com outro estabelecendo uma relação *peer-to-peer*[9]. O potencial desse protocolo é o de estabelecer redes distribuídas, nas quais as informações e inteligências não estão centralizadas em um único local. O protocolo TCP/IP permita a horizontalidade radical da rede e a livre distribuição de conteúdos.

A segunda máquina apontada por Galloway opera com o protocolo DNS. O chamado *Domain Name Service* funciona de maneira análoga a uma "lista telefônica" da internet. Isto é, o protocolo transforma o nome dos *websites* em um número de IP (*internet protocol*) necessário para encontrar o conteúdo ao redor do mundo. A estrutura do protocolo DNS

[9] Segundo definição da P2P Foundation: "So: what is peer to peer? Here's a first tentative definition: It is a specific form of relational dynamic, is based on the assumed equipotency of its participants, organized through the free cooperation of equals in view of the performance of a common task, for the creation of a common good, with forms of decision-making and autonomy that are widely distributed throughout the network" Disponível em: http://p2pfoundation.net/Defining_P2P_as_the_relational_dynamic_of_distributed_networks (acesso em 08/06/2014)

demonstra como conteúdos podem ser controlados ou banidos da rede. Conforme aponta Galloway,

> All DNS information is controlled in a hierarchical, inverted-tree structure. Ironically, then, nearly all Web traffic must submit to a hierarchical structure (DNS) to gain access to the anarchic and radically horizontal structure of the Internet. As I demonstrate later, this contradictory logic is rampant throughout the apparatus of protocol. (...)There are over a dozen root servers located around the world in places like Japan and Europe, as well as in several U.S. locations. (GALLOWAY, 2004, p. 9)

Chama a atenção o fato de haver poucos servidores DNS ao redor do mundo e a maioria deles localizados nos Estados Unidos, Europa e Japão. Seguindo a lógica rígida adotada pelo protocolo, conteúdos inadequados, posicionamentos políticos divergentes, novas possíveis tecnologias e serviços ou, até mesmo, países inteiros podem ser desligados da internet por meio do controle do protocolo DNS. Isto é, tais conteúdos podem ser retirados da "lista telefônica" da internet impedindo o acesso. Este condicionamento demonstra o caráter político que um protocolo técnico pode assumir, funcionando, assim, como um instrumento de controle. As análises de Foucault, Deluze e Guattari apontam nessa direção: a transição de uma sociedade disciplinar para uma sociedade de controle.

Conforme destacam Hardt e Negri (2013), em uma análise sobre a transição do biopoder de uma sociedade disciplinar para uma sociedade de controle:

> A sociedade disciplinar é a sociedade na qual a dominação social é construída através de uma rede ramificada de dispositivos ou de aparelhos que produzem e regem costumes, hábitos e práticas produtivas. Colocar esta sociedade para trabalhar e garantir obediência a seu poder e a seus mecanismos de integração e/ou de exclusão faz-se por intermédio de instituições disciplinares – a prisão, a fábrica, o asilo, o hospital, a universidade, a escola, etc. – que estruturam o terreno social e oferecem uma lógica própria à "razão" da disciplina. (HARDT & NEGRI, 2013, p. 161)
>
> .

O advento das novas tecnologias da informação e o constante aumento das interações sociais mediadas por computadores e redes abriram novas perspectivas para poderes disciplinares e de controle. O panóptico analisado por Foucault (1977), a partir da concepção de Bentham, introjeta nos indivíduos a constante autovigilância. "O panóptico funciona como uma espécie de laboratório de poder. Graças a seus mecanismos de observação, ganha em eficácia e em capacidade de penetração no comportamento dos homens" (FOUCALT, 1977, p. 169). Ou ainda, "ele programa, ao nível de um mecanismo elementar e facilmente transferível, o funcionamento de uma sociedade toda atravessada e penetrada por mecanismos

disciplinares" (FOUCAULT, 1977, p. 173). A visão foucaultiana de uma autodisciplina introjetada nos indivíduos por meio de um sistema disciplinar complexo que perpassa todas as instituições sociais assume um novo caráter com os sistemas de controle cibernético desenvolvidos a partir das interações em redes, principalmente na internet.

Nesse sentido, Deleuze (1992), ao revisitar os conceitos de Foucault sobre a sociedade disciplinar, começa a desenvolver o conceito de transição de uma sociedade disciplinar para uma sociedade de controle. Segundo ele, Foucault demonstrou que as sociedades disciplinares estavam situadas nos séculos XVIII e XIX, atingindo seu apogeu no século XX. A sociedade disciplinar substituiu as sociedades de soberania e, da mesma forma, seria superada por outro modelo. "São as sociedades disciplinares que estão substituindo as sociedades de controle. 'Controle' é o nome que Burroughs propõe para designar o novo monstro, e que Foucault reconhece como nosso futuro próximo" (DELEUZE, 1992, p. 220).

A sociedade de controle se difere da sociedade disciplinar em relação à sua lógica de dominação. Enquanto esta se baseia em moldes disciplinares rígidos e definidos, executados nas instituições, aquela é baseada em modulações, que se transformam constantemente. A sociedade disciplinar era marcada por um constante recomeço em cada nova instituição (da família para a escola, da escola para a fábrica, etc.), já a sociedade de controle é marcada por uma permanente volatilidade na qual nunca se termina nada[10].

Deleuze (1992) destaca um ponto essencial para a compreensão da função dos protocolos cibernéticos na sociedade de controle e uma possível resistência:

> As sociedades disciplinares têm dois pólos: a assinatura que indica o indivíduo, e o número de matrícula que indica sua posição numa massa. É que as disciplinas nunca viram incompatibilidade entre os dois, e é ao mesmo tempo em que o poder é massificante e individuante (...). Nas sociedades de controle, ao contrário, o essencial não é mais uma assinatura nem um número, mas uma cifra: a cifra é uma senha, ao passo que as sociedades disciplinares são reguladas por palavras de ordem (tanto do ponto de vista da integração quanto da resistência). A linguagem numérica do controle é feita de cifras, que marcam o acesso à informação, ou à rejeição. Não estamos mais diante do par massa-indivíduo. Os indivíduos tornaram-se "dividuais", divisíveis, e as massas tornaram-se amostras, dados, mercados ou "bancos". (DELEUZE, 1992, p. 222)

[10] A analogia com a obra do escritor tcheco Franz Kafka feita por Deleuze exemplifica bem a tensão entre as duas formas de dominação social: "a quitação aparente das sociedades disciplinares e a moratória ilimitada das sociedades de controle (em variação contínua)". Segundo Deleuze, são dois modos jurídicos distintos e se o próprio direito hesita entre ambos é porque o processo se encontra em transição (DELEUZE, 1992, p. 222).

A linguagem numérica apontada por Deleuze é encontrada por Galloway (2004) ao analisar os protocolos de comunicação em redes. Os mecanismos cibernéticos potencializam a fluidez das redes e o aparato de controle e modulação do biopoder. Da mesma forma, Deleuze prevê a cifra numérica substituindo palavras de ordem, tanto do ponto de vista do controle quanto da resistência. O ativismo criptográfico, objeto dessa pesquisa, se insere nesse contexto de controle ciberneticamente mediado amparado em uma complexa linguagem numérica de protocolos. Conforme destacam Hardt e Negri (2013) ao falar da sociedade de controle, o poder passa a se exercer por "máquinas que organizam diretamente os cérebros (por sistemas de comunicação, redes de informação) e os corpos (por sistemas de vantagens sociais, atividades desenvolvidas)." (HARDT & NEGRI, 2013, p. 162). Portanto, o aspecto fundamental a ser observado é a transformação constante de aparatos técnicos, regidos pela lógica das ciências da natureza, em instrumentos de dominação e/ou resistência política. Ainda que não seja novidade, as perspectivas que se abrem a partir de tal constatação colocam as ciências sociais em uma área de fronteira, na qual suas interfaces se tornam mais ricas e prolíficas para a produção do conhecimento, interpretação e intervenção na realidade.

O potencial de controle cibernético e, consequentemente, de biopoder desenvolvido a partir das interações com novas tecnologias, juntamente com a história do desenvolvimento da internet e das redes, demonstram que esse campo é um território de conflito constante no qual conceitos militares de segurança e estratégia são aplicados visando garantir o controle do ciberespaço. A mais recente onda de militarização e aumento do controle no ciberespaço reanimou os hackerativistas e ativistas criptográficos. Entender brevemente os conceitos que guiam esse processo de militarização é o objetivo do tópico seguinte.

2.3 MILITARIZAÇÃO DO CIBERESPAÇO

A estrutura e arquitetura da internet é o resultado inusitado do trabalho de militares, acadêmicos e hippies (CASTELLS, 2003). Projetada inicialmente como aparato militar, foi desenvolvida conjuntamente com centros de pesquisa civis e contagiada por entusiastas da contracultura. Nesse contexto, o trabalho da RAND Corporation[11] foi essencial para o

[11] A RAND Corporation é uma das principais agências independentes de fomento à pesquisa sobre temas de interesse do Departamento de Defesa dos Estados Unidos da América. A marca "RAND" foi formada pela contração das palavras research and development (pesquisa e desenvolvimente) e a Agência foi criada em 1946 pela aeronáutica dos Estados Unidos como uma empresa independente e sem fins lucrativos com a finalidade de promover através da pesquisa e da análise o desenvolvimento de material que auxiliasse a elaboração de políticas

desenvolvimento do que hoje conhecemos como internet. No interior da RAND, corporação diretamente ligada ao Departamento de defesa norte-americano, dois autores começaram a problematizar a questão do conflito cibernético e suas possíveis consequências. Nas obras: *Cyberwar is coming* (1993), *The Advent of Netwar* (1996) e *In Athena's Camp* (1997), John Arquilla e David Ronfeldt apontam para o futuro do conflito em uma sociedade altamente informatizada e mediada ciberneticamente.

Em seus estudos, Arquilla e Ronfeldt desenvolvem conceitos fundamentais para se compreender a orientação das políticas de defesa norte-americana para o ciberespaço. O primeiro é o conceito de *netwar* (guerra em rede). Segundo Antoun (2013):

> Arquilla e Ronfeldt designavam um modo emergente de luta e conflito surgido na sociedade contemporânea a partir da revolução tecnológica com a construção da infraestrutura do ciberespaço. A guerra em rede era o oposto correlato do conceito de guerra de controle (cyberwar), também por eles gerado na mesma ocasião, ambos constituindo grande parte do campo da guerra da informação (infowar) no mundo atual. (ANTOUN, 2013, p. 210).

Nesse sentido, a guerra de controle (*cyberwar*) é o conflito em maior escala entre dois Estados, enquanto a guerra em rede (*netwar*) é o conflito em menor intensidade entre um Estado e outros atores dispersos por meio de táticas que se utilizam das novas tecnologias informáticas e do poder cibernético. Ambas contidas no campo da chamada infowar. “Netwar refers to information-related conflict at a grand level between nations or societies. It means trying to disrupt, damage, or modify what a target population “knows” or thinks it knows about itself and the world around it.” (ARQUILLA & RONFELDT, 1997, p. 100). Já a *cyberwar* na definição dos autores:

> Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting if not destroying the information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to “know” itself: who it is, where it is, what it can do when, why it is fighting, which threats to counter first, etc. It means trying to know all about an adversary while keeping it from knowing much about oneself. It means turning the “balance of information and knowledge” in one’s favor, especially if the balance of forces is not. It means using knowledge so that less capital and labor may have to be expended. (ARQUILLA & RONFELDT, 1997, p. 105).

---

e tomada de decisões no âmbito da defesa e da segurança nacional e internacional dos Estados Unidos (ANTOUN, 2013, p. 233)

Partindo dessas definições, as preocupações estratégicas norte-americanas se apresentam em duas frentes. A primeira prepara o conflito cibernético entre dois Estados, em moldes mais próximos de guerras tradicionais (cyberwar). Enquanto a segunda (netwar), se preocupa com conflitos de baixa intensidade entre Estado e grupos organizados (movimentos insurgentes, ativistas antirregime, grupos terroristas, etc.). Os ataques cibernéticos do governo russo a Estônia em 2007[12] (RICHARDS, 2009) ou o caso do vírus *Stuxnet*[13] usada contra o programa nuclear iraniano são exemplos de *cyberwar*. Por outro lado, os conflitos entre simpatizantes zapatistas na rede e a organização de protestos e ações diretas na rede por ativistas são exemplos de *netwar*.

Segundo os autores, o conflito ocorre, atualmente, em cinco fronteiras: a) Fronteira terrestre; b) Fronteira Naval; c) Fronteira Aérea; d) Fronteira Aeroespacial; e) Fronteira Interna; f) Fronteira cyberespacial.

Devido à posição privilegiada e da doutrina geopolítica americana da Ilha-continente, o conflito terrestre foi resolvido ainda no século XIX. Duas fronteiras pacificadas, ao norte Canadá e ao sul México, sem possibilidades imediatas de conflitos ou ameaças. Da mesma forma, a doutrina militar de conquistas dos mares, influenciada diretamente pelo pensamento de Alfred Mahan e sua obra "*The Influence of Sea Power upon History*" (1890), lançou o pensamento estratégico norte-americano aos mares, construindo a maior força naval do planeta e, consequentemente, pacificando a fronteira naval.

Em paralelo a isso, o desenvolvimento do poderio aéreo, com tecnologia de caças supersônicos, bombardeiros e, mais recentemente drones, aliado à possibilidade de alcance global devido ao posicionamento de porta-aviões, colocam novamente os EUA em posição confortável como grande potência aérea. No âmbito da corrida aeroespacial, a derrocada da União Soviética e a ascensão de programas de cooperação internacional na área espacial, colocaram os EUA em relativa segurança (somente mais recentemente o avanço de pesquisas

[12] "On April 26, 2007, the small Baltic state of Estonia experienced the first wave of denial-of-service (DoS) attacks. Accompanied by riots in the streets, these cyberattacks were launched as a protest against the Estonian government's removal of the Bronze Soldier monument in Tallinn, a Soviet war monument erected in 1947. These attacks targeted prominent government websites along with the websites of banks, universities, and Estonian newspapers. After three weeks, the attacks ceased as suddenly as they had begun, but not before the Estonian government undertook measures to block all international web traffic, effectively shutting off the "most wired country in Europe" from the rest of the world." (RICHARDS, 2009, p. 1)

[13] O vírus Stuxnet foi encontrado nos sistemas de controle industrial da Siemens no Irã. O vírus se destaca por conseguir atacar o CLP (Comando Lógico Programável) de grandes plantas industriais, afetando diretamente o funcionamento de máquinas e equipamentos. (McMILLAN, 2010, online) Disponível em: http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems?taxonomyName=Network+Security&taxonomyId=142 Acesso: 10/06/2014.

e tecnologia chinesa surge como um possível contraponto a este poderio). Por fim, as duas grandes fronteiras não pacificadas, segundo a doutrina estratégica norte-americana, destacadas pelos dois pesquisadores: a fronteira interna e a fronteira ciberespacial.

Os atentados terroristas de 11 de setembro de 2001 abriram novas perspectivas e desafios para o pensamento estratégico norte-americano. Um ataque executado dentro das fronteiras nacionais, de maneira surpreendente, alertou para o perigo de uma fronteira interna não pacificada. As medidas que se seguiram aos atendados demonstram a clara preocupação do governo com tentativa de contenção e controle das atividades na Fronteira Interna. Dentre tais medidas, destaca-se o PATRIOTIC ACT[14] que municiou as autoridades de defesa a investigarem possíveis suspeitos de terrorismo e outros atos ilícitos. Com isso, a Fronteira Interna é tratada como o inimigo sem rosto, isto é, em nome da segurança nacional todos os indivíduos são potencialmente suspeitos. Os documentos[15] da *National Security Agency* (NSA) vazados por Edward Snowden demonstram a abrangência e poder de interceptação desenvolvido como parte da estratégia de segurança nacional do governo norte-americano sob o amparo de tais leis (HARDING, 2014).

O controle da Fronteira Interna passa, necessariamente, pela vigilância e monitoramento das atividades das populações. Com isso, a Fronteira Ciberespacial se torna, essencialmente, o grande campo de batalha aberto no século XXI. Controlar as formas de comunicação, os fluxos de informação, a política de protocolos e, através disso, moldar desejos e opiniões é um passo fundamental na luta por corações e mentes. O título do livro de Arquilla & Ronfeldt (1997) aponta justamente para isso, uma mudança no paradigma do conflito no século XXI. Sai o deus da guerra Ares, do poder militar e da força, e entra a deusa Athena, da inteligência e comunicação. O conflito no século XXI, segundo os autores, é necessariamente uma luta pelos fluxos de informação e instrumentos cibernéticos. A partir disso, conceitos como *cyberwar*, ciberterrorismo e ciberativismo assumem novo sentido. São diferentes atores lutando no mesmo campo de batalha.

A particularidade da batalha pela fronteira ciberespacial é que seu instrumento fundamental, o poder cibernético, se apresenta de forma difusa entre os atores. Além disso, os custos para a entrada em uma disputa de poder nesse meio podem ser relativamente baixos

[14] Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act. Disponível em: http://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf Acesso 11/06/2014.
[15] A organização não-governamental Eletronic Frontier Foundation reuniu e disponibilizou em seu site os arquivos liberados por Edward Snowden: https://www.eff.org/nsa-spying/nsadocs Acesso em: 11/06/2014.

para determinados atores, facilitando o ingresso e a saída destes em situações de conflitos. Ao contrário do poder militar necessário para se dominar as fronteiras terrestre, naval e aérea, o poder cibernético pode depender de aparatos e instrumentos complexos, porém acessíveis, residindo em sua apropriação e ressignificação o potencial de uso como fonte de poder.

> Indeed, many of the problems of dealing with Information Warfare are linked to the nature of information technology itself. The most important feature may simply be the falling cost of information processing; since the 1950s costs have declined at a rate of about 90 percent every five years, and most experts expect this trend to continue for the foreseeable future. One result is that information technology—and, with it, the ability to play in the Information Warfare game—is constantly becoming more available, and quite rapidly. Unlike nuclear weapons technology or aerospace weapons technology, which have been spreading steadily but slowly, the diffusion of Information Warfare technology is likely to accelerate. If a party cannot afford some form of information technology and Information Warfare capability today, it probably will be able to afford the technology tomorrow. This is evidenced in the spread of dedicated military electronic systems, but even more in the availability of commercial information technology such as computer networks, satellite and fiberoptic communications, cellular telephone systems, and so on. All of these can be used for hostile purposes, and can be attacked by a hostile power (ARQUILLA & RONFELDT, 1997, p. 456).

Com uma doutrina militar de segurança nacional aplicada ao ciberespaço e sua posição privilegiada em relação à topologia da rede, isto é, a grande presença de servidores e empresas de tecnologia em seu território, os Estados Unidos contribuem largamente para uma crescente militarização da internet. Nesse sentido, a atividade política na internet, principalmente o ativismo dissidente ou antirregime, se torna uma fonte constante de preocupação e monitoramento – o trecho destacado acima demonstra claramente como a doutrina militar norte-americana considera potencialmente perigoso o chamado *Information Warfare*. Por esse motivo, é necessário entender como os ativistas se apropriaram da tecnologia e passaram a usar a rede em suas formas de protesto e organização.

2.4 ATIVISMO E TECNOLOGIA

Para entender o ciberativismo, seus conceitos e derivações, é necessária uma breve reconstrução das principais correntes explicativas do fenômeno da cibercultura. Diversos teóricos se voltaram para o assunto, produzindo um amplo leque de explicações para as consequências da crescente interação entre a humanidade e o meio cibernético. Em linhas gerais, essas interpretações se dividem em tecnófilos e tecnofóbos, ou ainda, prometeicos e fáusticos, conforme Francisco Rüdiger (2013). Segundo ele, os tecnófilos remontam a Francis

Bacon e “são estes que procedem ao elogio da técnica moderna, com base na capacidade emancipatório e beneficente” (RÜDIGER, 2013, p. 51). Essa visão coloca a evolução da técnica em um sentido benevolente que ao final conduzirá todos ao bem comum. Por outro lado, a corrente tecnófoba, que remete a Georg Simmel, “cresceu em meio à reversão de expectativas históricas que começa a cercar espiritualmente o desenvolvimento tecnológico na virada para o século XX” (RÜDIGER, 2013, p.15). Para os fáusticos, a mecanização da vida e as máquinas representam um perigo à própria existência humana.

Essa primeira divisão entre tecnófilos e tecnófobos é útil para posicionar os autores dentro de um espectro que vai desde uma tecnoutopia de Pierre Lévy (1999) até o tecnoapocalipse de Kroker e Weinstein (1994). Enquanto o primeiro defende que a “inteligência coletiva” proporcionada pelo ciberespaço irá necessariamente conduzir a um futuro melhor com base no amor (LÉVY, 1995), os outros autores decretam que o fim da história e sua substituição pela história virtual, assim como a consequente transformação dos seres humano em lixo tecnológico.

> Technotopia is about disappearances: the vanishing of the body (into a relational data base), the nervous system into “distributive processing,” and the skin into wetware. As technology comes alive as a distinctive species, we finally encounter the end of (human) history and the beginning of virtual history. A waiting time of growing bodies for endless circulation through all the synapses and gateways of the data: networks. A euphoric space where subjectivity drains away into televisual memories, and desire is recombined into a, vertiginous matrix of doubled possibilities. Virtual reality skin-grafts the logic of the, ambiialent sign onto the “standing reserve” of the social. (KROKER & WEINSTEIN, 1994)

Por outro lado, alguns autores tentam superar essas abordagens unidimensionais buscando criar uma teoria crítica da cibercultura. Para eles, a humanidade e técnica não são opostas e o foco da análise deve se concentrar nas relações estabelecidas e nas opções geradas. Tecnófilos e tecnófobos caem em um fetichismo tecnológico ao desconsiderarem que a tecnologia necessita de fins não tecnológicos, isto é, sua aplicação no mundo real sob o imperativo das condições materiais. Em uma análise que remete a Marcuse, homens e máquinas devem ser entendidos em suas relações e determinações históricas. Autores como Kellner (1999) apontam nesse sentido, ao buscar criticar as teorias da tecnologia e, ao mesmo tempo, apontar para possibilidades emancipatórias.

> Critical theory of technology attempts to develop a dialectical optic that avoids one-sided approaches in theorizing and evaluating the genesis of the new technologies and their often contradictory and ambiguous effects. I also want to develop democratic and activist perspectives on the new technologies, suggesting some ways that they might be used for such things as self-valorization and empowerment,

> democratization and progressive social transformation, in contrast to strengthening the forces of corporate and state domination. (KELLNER, 1999, p.189-90)

A visão das ferramentas tecnológicas como instrumentos de possível emancipação e de interferência no mundo real é de vital importância para compreender o fenômeno do ciberativismo. Uma vez que uma ação politicamente motivada é elaborada e executada por meio das redes e do ciberespaço, os indivíduos envolvidos no processo têm a mínima consciência ou crença de que sua capacidade de manipular o meio técnico pode interferir nas relações de poder. Isto é, ainda que submetida a uma lógica de mercado hegemônica e as condições materiais vigentes, ciberativistas recusam tanto o otimismo inocente quanto o pessimismo catastrófico. Pois, tais tecnologias "não são função de um propósito social pré-determinada: são parte de um contexto histórico em meio ao qual a vida é articulada. As pessoas possuem o poder de reinventar o sentido simbólico e o caráter funcional dos aparatos tecnológicos". (RÜDIGER, 2013, p. 66)

A partir disso, a ideia de utilizar os meios tecnológicos como forma de ação política pode tomar corpo. Segundo o pesquisador e ativista Stefan Wray (1998), é possível identificar cinco estágios na relação entre computadores e ativismo político: ativismo computadorizado, guerra informacional de base, desobediência civil eletrônica, *hacking* politizado e resistência a guerras futuras[16]. Para ele, o ano de 1998 é um marco nessa junção entre tecnologia e ação política cunhando os termos: desobediência civil eletrônica e hackerativismo.

O processo de aproximação e apropriação mútua entre tecnologia e política, segundo Wray, remonta a meados dos anos 1980, sendo o ativismo computadorizado sua primeira expressão: "*as an example, the first version of PeaceNet appeared in early 1986. PeaceNet enabled - really for the first time - political activists to communicate with one another across international borders with relative ease and speed*" (WRAY, 1998, p.2). Essa primeira forma de ativismo computadorizado privilegiava o discurso, o diálogo, a troca de argumentos, através de listas de e-mails e de Bulletin Board Systems[17] e, posteriormente, websites e fóruns. O ativismo computadorizado se aproxima, assim, do que Wray denomina como

[16] "computerized activism, grassroots infowar, electronic civil disobedience, politicized hacking, and resistance to future war" (WRAY, p. 1) Tradução livre.

[17] Bulletin Board System (BBS) é um software que permite conexão via telefone a um sistema através de um computador, tal como se faz hoje na internet. (Disponível em: http://pt.wikipedia.org/wiki/Bulletin_board_system. Acesso em 15/01/2014.) O BBS foi posteriormente substituído pela WWW (World Wide Web) devido aos custos e facilidade de operação.

"*Habermasian Web*" (WRAY,1998, p. 3). Isto é, um espaço de debate nos moldes de uma esfera pública habermasiana que privilegia a livre troca de argumentos racionais.

O segundo momento é o que Wray (1998) chama de guerra informacional de base (grassroot infowar), uma intensificação do ativismo computadorizado que gerou uma guerra de palavras e propaganda. A grande mudança notada é a intenção de fazer com a guerra textual levasse a ações reais. Wray identifica nesse momento o começo da mudança da internet de um espaço de comunicação para, também, um espaço de ação. Ou seja, mais do que reportar fatos e apresentar diálogos, a guerra informacional busca denunciar a realidade e engajar mais indivíduos na ação. Nesse sentido, o autor aponta o movimento internacional de solidariedade pro-Zapatista como o melhor exemplo dessa mudança de paradigma na internet.

> At the end of 1997, news of the Acteal massacre in Chiapas, in which 45 indigenous people were killed, quickly spread through global pro-Zapatista Internet networks. Within a matter of days there were protests and actions at Mexican consulates and embassies all over the world. This incident, too, is now seen as a turning point in the stance by some toward the Internet infrastructure. (...) following there has been a shift, the beginning of the move toward accepting the Internet infrastructure as both a channel for communication and a site for action. (WRAY, 1998, p. 4)

A terceira forma de ação é a desobediência civil eletrônica. Nesse tipo de ação, táticas tradicionais de desobediência civil dos movimentos sociais são transportadas para a internet, como bloqueios e *sit-ins* virtuais. Tais táticas consistem em, basicamente, sobrecarregar o acesso a determinadas páginas causando quedas e impedindo o acesso de outras pessoas. Na análise de Wray, esse tipo de ação completa a distinção iniciada na guerra informacional. A guerra de propaganda convocando para a ação deixava a posição da internet em uma situação ambígua: tanto canal para comunicação quanto para ação. A partir da desobediência civil virtual, fica mais evidente uma transformação no uso da infraestrutura da internet, se afastando gradualmente de um conceito de esfera pública e se tornando cada vez mais um espaço de conflitos.

O passo seguinte é o chamado hacking politizado. Nessa modalidade de ação, os ativistas invadem sites e trocam seus conteúdos por mensagens políticas ou sátiras. A principal diferença da desobediência civil eletrônica é que, enquanto esta é executada em grupos, nos quais as identidades são, geralmente, conhecidas; aquele é executado por indivíduos que preferem permanecer anônimos. A opção pelo anonimato ocorre devido ao terreno legalmente ambíguo no qual essas ações são executadas.

Por escrever no final dos anos 1990, Wray apostava que a quinta forma de ação seria a resistência a guerras. De fato, atividades recentes do coletivo Anonymous tem se voltado contra alvos envolvidos em guerras e atos contra a paz (COLLEMAN, 2013). Porém, essas ações se constituem em atos coordenados de *hacking* político e desobediência civil eletrônica, podendo ser considerada mais uma ação conjunta de outros tipos do que uma nova forma de ativismo. Por outro lado, ações recentes do chamado Exército Eletrônico Sírio têm demonstrado o potencial do uso das mesmas ferramentas por parte de governos. Em suporte ao governo do Bashar Al-Assad, o Exército Eletrônico Sírio atacou diversos sites da oposição ao governo, de organizações de direitos humanos, meios de comunicações e governos que apoiam rebeldes. (NORMAN, 2011).

Apresentado o caminho desenvolvido por Wray (1998) para explicar o encontro e a apropriação mútua entre tecnologia e ativismo político e, principalmente, como esse caminho conduziu a uma mudança no uso da própria infraestrutura da internet, tornando-a um espaço potencialmente conflituoso, passa-se a uma análise do próprio conceito de ciberativismo e hackerativismo.

Na definição de Sérgio Amadeu da Silveira (2010): "Por ciberativismo podemos denominar um conjunto de práticas em defesa de causas políticas, socioambientais, sociotecnológicas e culturais, realizadas nas redes cibernéticas, principalmente na Internet". Esse conceito abre possibilidade tanto para ações que visam participar e influenciar o debate público, quanto aquelas cujo objetivo é usar a infraestrutura das próprias redes como forma de atingir objetivos políticos. Nesse sentido, o ciberativismo pode utilizar a internet como uma Esfera Pública, em sentido habermasiano. Ações como petições virtuais, fóruns de discussão, *mass mailing* e campanhas em redes sociais constituem alguns exemplos desse tipo. Por outro lado, Samuel (2004) define "*hacktivism is the nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends*." Ao situar o hackerativismo em um terreno ilegal ou legalmente ambíguo a autora clarifica melhor a diferença nesses tipos de ações. Isto é, as ações podem ter como alvo a própria infraestrutura das redes, invasão de sistemas, vazamento de informações, derrubada de sites. Devido à velocidade do desenvolvimento de novas e inusitadas formas de hackerativismo a repressão legal pode se deparar com situações ambíguas nas quais a lei estabelecida não consegue atingir a realidade dos fatos.

Um dos primeiros coletivos hackers, Cult of Dead Cow define hackerativismo como: *"a special operations group sponsored by the CULT OF THE DEAD COW (cDc). We view*

access to information as a basic human right. We are also interested in keeping the Internet free of state-sponsored censorship and corporate chicanery so all opinions can be heard." (CDC, 2001). Em outra declaração o coletivo reafirma suas diretrizes de luta pela liberdade de informação: "(...) RECONHECENDO a importância para lutar contra os abusos dos direitos humanos com respeito ao acesso razoável à informação na Internet; CONSEQÜENTEMENTE NÓS SOMOS CONVENCIDOS que a comunidade hacker internacional tem um imperativo moral a agir" (CDC, 2001, grifo no original). A moral hacker surge como o motor da ação. Uma moral nascida da própria constituição dos sujeitos em interação com a técnica e as redes.

Ao analisar a ética e a moral hacker, Pekka Himanen (2001) busca identificar como a ética hacker se afasta da ética protestante de trabalho - a partir da análise clássica de Max Weber. Para isso, identifica os sete principais valores que diferenciam a ética hacker: paixão, liberdade, valor social, abertura, atividade, consideração e criatividade[18] (HIMANEN, 2001, p. 139-141). Os dois primeiros valores (paixão e liberdade) constituem a ética de trabalho, hackers buscam misturar trabalho realmente motivado com liberdade de execução, especialmente em relação ao tempo. Os valores seguintes (valor social e abertura) correspondem à ética do dinheiro. Hackers se dedicam a projetos que tenham valor para a comunidade e que gere reconhecimento em seu meio. Da mesma forma, seus projetos devem ser abertos para que outros possam colaborar e gerar novas possibilidades.

Dos valores *atividade* e *consideração*, surge o que Himanen chama de *Nethic* (Himanen, 2001, p.140), a ética aplicada às redes como forma de estabelecer relações que garantam sua própria existência. Por *atividade* os hackers entendem uma postura ativa, liberdade de expressão, privacidade para criações individuais e rejeição a uma atitude passiva na rede. Já *consideração* está relacionada com a preocupação com os outros e, consequentemente, consigo mesmo e com o desejo de livrar a sociedade das redes da mentalidade de sobrevivência competitiva. Isso conduz a um desejo de incluir o maior número possível de pessoas nas redes de forma benéfica e, principalmente, lutar contra a estrutura hierarquizada e de vigilância que pode surgir devido à arquitetura da internet.

A *Nethic* de Himanen (2001) confirma o compromisso hacker com a luta pela liberdade, neutralidade e abertura das redes. Pode-se afirmar que o hackerativismo deriva diretamente da *Nethic*, utilizando os outros valores como complemento a atividade

[18] Tradução livre de: "passion, freedom, social worth, openness, activity, caring and creativity".

politicamente motivada. As lutas conduzidas pelos hackers são, em última instância, o embate entre duas concepções de mundo. A primeira derivada do que Himanen identifica com a ética protestante, isto é, uma concepção liberal centrada no trabalho e na acumulação individual. A segunda visão de mundo é fruto da ética hacker, baseada em outra lógica de trabalho, passionalmente motivada, descentralizada, mais preocupada com o compartilhamento e a colaboração e, da mesma forma, com a expansão e garantia da existência do meio virtual.

Portanto, o desenvolvimento de uma ética própria nascida das redes, unida ao ativismo político e de protestos de rua, abriram novas possibilidades de manifestações na internet. Tais manifestações, ora atuam como *proxy* do mundo real, buscando potencializar e reverberar temas e outras formas de protestos; ora tem como principal foco de ação a própria rede, isto é, temas pertinentes a estrutura, liberdade e própria existência das redes. Essa diferenciação é essencial para se compreender os tipos de ciberativismo e seu escopo de ação. Por esse motivo, é necessária uma breve discussão sobre os conceitos de Esfera Pública e Esfera Pública Interconectada, com o objetivo de situar o debate e posicionar o ativismo cibernético entre dois pontos principais: de um lado, o ativismo discursivo que busca nas redes ampliar ou colocar temas em debate; por outro, o ativismo de ação direta que compreende que a própria estrutura da rede deve ser alvo da ação, uma vez que esta é submetida a uma arquitetura de controle e vigilância.

2.5 ESFERA PÚBLICA INTERCONECTADA

A partir dos estudos de Jürgen Habermas o conceito de Esfera Pública entrou em discussão na teoria política, principalmente no campo conhecido como Democracia Deliberativa ou discursiva. A obra “Mudança Estrutural na Esfera Pública” (1984) é o marco inicial nesse sentido. Ainda que, posteriormente, o próprio autor tenha modificado algumas de suas elaborações e sofridos diversas críticas e contribuições ao conceito, a obra permanece como essencial para se compreender a elaboração teórica em torno do conceito.

Em sua obra *Mudança Estrutural da Esfera Pública* (1984), Habermas traça um histórico do termo esfera pública e sua evolução na sociedade moderna. Primeiramente, até o século XVIII, esfera pública referia-se a um lugar no qual o poder dos reis ou da aristocracia era exercido e de onde evocavam a sua soberania. Ela surge como espaço exclusivo das elites sociais do século XVIII. Porém, após as revoluções políticas dos séculos XVIII e XIX, a

expressão esfera pública passou a traduzir uma noção de espaço participativo e de cultura urbana, nos finais do século XX. Deste modo, esfera pública passa a constituir o que Habermas (1984) denomina “esfera pública da burguesia” (HABERMAS, 1984, p.42).

> A esfera pública de burguesia pode ser entendida inicialmente como a esfera das pessoas privadas reunidas em um público; elas reivindicam este esfera pública regulamentada pela autoridade, mas diretamente contra a própria autoridade, a fim de discutir com ela as leis gerais da troca na esfera fundamentalmente privada, mas publicamente relevante, as leis do intercâmbio de mercadorias e do trabalho social. (HABERMAS, 1984, p. 42)

Para Habermas, um indivíduo é capaz de participar da esfera pública quando é capaz de emitir uma opinião pública. Esta opinião é gerada por meio de uma racionalização, isto é, todo ser humano é capaz de racionalizar acerca de determinado assunto ou questão e emitir uma opinião baseada no seu melhor juízo. Dessa forma, a esfera pública é capaz de discutir temas e também de levantar críticas e juízos sobre as diversas questões. Isto é, para Habermas, vital para o controle do poder político. Pois, ampliando a extensão dos temas discutidos e criticados, a avaliação pública se constituiria uma esfera de legitimação do poder.

Por construir sua análise a partir de uma categoria específica, a esfera pública burguesa, Habermas teve que lidar com questões relativas à igualdade dos participantes do debate público. Na esfera pública burguesa, aqueles que emitiam opiniões públicas eram homens e proprietários. Da mesma forma, Habermas defendia a existência de uma esfera pública única, excluindo outras que pudessem surgir, por exemplo, uma esfera pública operária. A esfera pública burguesa encontrava sua origem na vida urbana e na esfera pública literária. “A “cidade” não é apenas economicamente o centro vital da sociedade burguesa; em antítese política e cultural à “corte”, ela caracteriza uma primeira esfera pública literária que encontra as suas instituições nos *coffee-houses*, nos *salons* e nas comunidades de comensais” (HABERMAS, 1984, p. 44-45).

Posteriormente, Habermas amplia sua definição de esfera pública, focando sua atenção no fato de que a esfera pública não é uma estrutura normativa, não existindo enquanto instituição ou organização. Nesse sentido, a esfera pública seria mais adequadamente descrita como “uma rede adequada para a comunicação de conteúdos, tomadas de posição e opiniões; nela os fluxos comunicacionais são filtrados e sintetizados, a ponto de se condensarem em opiniões públicas enfeixadas em temas” (HABERMAS, 2003, p. 92).

A função da esfera pública em sociedades complexas é captar as demandas, problemas e desejos na realidade social e pressionar os Sistemas (Estado e economia). Isto é, as demandas do Mundo da Vida são debatidas por meio de uma esfera publica, por sujeitos livres e racionais, e, assim, pressionam o Estado, legitimando e/ou limitando o poder público. Habermas também passa a enxergar a possibilidade da existência de várias esferas públicas.

> Em sociedades complexas, a esfera pública forma uma estrutura intermediária entre o sistema político, de um lado, e os setores privados do mundo da vida e sistemas de ação especializados em termos de funções, de outro lado. Ela representa uma rede super-complexa que se ramifica especialmente num sem número de arenas internacionais, nacionais, regionais, comunais e subculturais, que se sobrepõem umas às outras; essa rede se articula objetivamente de acordo com os pontos de vista funcionais, temas, círculos políticos, assumindo a forma de esferas públicas mais ou menos especializadas. (HABERMAS, 2003, p. 107)

Dessa forma, qualquer tema pode ser objeto de apreciação na esfera pública. Os diversos interesses e pressões do Mundo da Vida podem ser canalizados para o debate público. Isto depende diretamente da capacidade dos concernidos de elaborarem argumentos racionais e convincentes capazes de tornar o tema público.

Outra ampliação importante no conceito de esfera pública feita por Habermas foi à concepção de que esta se manifesta em diversos níveis. Cada nível se diferencia de acordo com a complexidade da comunicação e da organização empregada e o alcance. Assim, Habermas (2003) identifica três tipos de esfera pública: “esfera pública episódica (bares, cafés, encontros na rua); esfera pública da presença organizada (encontro de pais, concertos de rock, encontros de partidos) e a esfera pública abstrata, produzida pela mídia (leitores e expectadores singulares e espalhados globalmente)” (HABERMAS, 2003, p. 107).

O conceito de esfera pública abstrata é fundamental para compreender o impacto do desenvolvimento das novas tecnologias de comunicação e informação no debate público e no discurso democrático. Nesse sentido, o aumento das possibilidades comunicacionais, isto é, das oportunidades de fala e da ampliação das vozes na esfera pública, pode contribuir substancialmente para a pressão exercida sobre o Estado. A mídia de massa aponta, primeiramente, para isso. No entanto, novos desafios a essa concepção são colocados com o advento da internet. Foco de interesse do presente artigo. Portanto, qual a consequência do surgimento da internet para a esfera pública? Para debater essa questão, Yochai Benkler (2006) desenvolveu o conceito de esfera pública interconectada.

Segundo Benkler (2006), o advento da internet interferiu diretamente nos custos das oportunidades de fala. Enquanto nos meios de comunicação em massa (TV, rádio, jornais de grande circulação) o custo para emitir opiniões e juízos era muito alto, a internet, a partir de sua arquitetura, proporciona maiores condições de expressão por um custo muito menor. Duas características são essenciais nesse processo: a arquitetura em rede que permite múltiplas interações, ao contrário da estrutura tradicional dos meios de comunicação emissor (mídia) e receptor (audiência); e a eliminação dos custos de fala para além de sua comunidade (BENKLER, 2006, p. 212).

> It therefore portends significant, though not inevitable, changes in the structure of the public sphere from the commercial mass-media environment. (...) the cost of being a speaker in a regional, national, or even international political conversation is several orders of magnitude lower than the cost of speaking in the mass-mediated environment. This, in turn, leads to several orders of magnitude more speakers and participants in conversation and, ultimately, in the public sphere (BENKLER, 2006, p. 213).

A diminuição dos custos tem impacto quantitativo e qualitativo. De um lado, o aumento do número de falantes e opiniões. De outro, a mudança na qualidade dessa relação com a mídia de massa, mais do que audiência passiva, expectadores e leitores podem interagir e fornecer argumentos na esfera pública. No modelo habermasiano, os juízos construídos na esfera privada eram aos poucos levados para a esfera pública. O que Benkler (2006) aponta é que esse processo pode ser amplificado pela internet atingindo o poder relativo da mídia. Partindo dessa ideia, diversos pontos na relação mídia e esfera pública são afetados: a estrutura da entrada de temas e proposições; a apresentação de assuntos para o discurso; a maneira como os assuntos são filtrados e pro quem; a maneira como as posições são cristalizadas e sintetizadas, servindo até como fonte para os grandes meios de comunicação (BENKLER, 2006, p. 213).

O poder de uma esfera pública interconectada reside na forma com que os sujeitos se apossam e se empoderam na rede. O conjunto de ferramentas tecnológicas disponibilizadas na rede só possui valor político quando utilizados como forma de expressão e ampliação das vozes na esfera pública. Dessa forma, a esfera pública interconectada não exclui a esfera pública tradicional, ela serve como uma nova de inserção e construção do discurso, impactando, cada vez mais, na esfera pública.

> The networked public sphere is not made of tools, but of social production practices that these tools enable. The primary effect of the Internet on the public sphere in liberal societies relies on the information and cultural production activity of

> emerging nonmarket actors: individuals working alone and cooperatively with others, more formal associations like NGOs, and their feedback effect on the mainstream media itself. These enable the networked public sphere to moderate the two major concerns with commercial mass media as a platform for the public sphere: (1) the excessive power it gives its owners, and (2) its tendency, when owners do not dedicate their media to exert power, to foster an inert polity (BENKLER, 2006, p. 219-220).

Dessa concepção democratizante da internet surgem também diversas críticas. Em geral, estas seguem duas linhas. Por um lado, afirmam que o excesso de informação e opiniões irá conduzir a uma fragmentação do discurso, polarização e perda da comunidade política. Por outro lado, o segundo tipo de crítica aponta que a internet pode causar mais centralização. O argumento central é que a própria infraestrutura da rede e o mercado de atenção são menos divididos do que parecem. Em suma, maior oportunidade de fala e menor chance de ser ouvido.

Essas duas críticas acompanharam a internet desde sua popularização nos anos 1990. Justamente por isso, o hackerativismo parece apontar para novas formas de utilizar a rede e interferir na esfera pública interconectada. As ações dos hackerativistas buscam superar as críticas apontadas acima (fragmentação e mercado da atenção) e, ainda, colocam em pauta uma nova questão: o anonimato. Os indivíduos dotados de razão pública são responsáveis pelas consequências de uma opinião ou proposta proferida na esfera pública. O anonimato defendido por alguns hackerativistas questiona essa ideia e tenta demonstrar que o garantia de preservação da identidade pode fazer com que novos temas possam ser mais bem problematizados na esfera pública.

Conforme apresentado anteriormente, uma diferenciação entre ciberativismo e hackerativismo é necessária para se compreender a relação com a esfera pública interconectada e o um processo de deliberação público. Enquanto o ciberativismo pode utilizar a rede como caixa de ressonância e, nesse sentido, se aproximar formar e influenciar uma esfera pública interconectada; o hackerativismo se aproxima mais de ações diretas no mundo real, transportadas para o ambiente virtual, nas quais alvos estratégicos são alvos com objetivo de chamar a atenção para determinadas causas.

A diferença nas duas formas de ação pode ser entendida, em último grau, como uma divergência de racionalidades empregadas. A esfera pública interconectada é, acima de tudo, um ambiente discursivo no qual sujeitos empregam argumentos com objetivo de convencer seus pares. O hackerativismo, por sua vez, utiliza de argumentos discursivos aliados a formas

de ação teleológicas. Isto é, o discurso é levado até os interessados por meio de ações performáticas e, algumas vezes, legalmente ambíguas, que visam um fim específico e estratégico.

O trajeto histórico traçado pro Wray mostra como o ambiente da internet foi se tornando, cada vez mais, um espaço de conflitos. Nesse sentido, as táticas de hackerativistas foram se afastando das táticas dos ativistas online. Samuel (2004) indica as principais táticas de hackerativistas: derrubada de sites; redirecionamento de sites; ataque de negação de serviço; roubo de informação; roubo e distribuição de informação; sites paródia; sabotagem virtual; desenvolvimento de softwares[19].

A esfera pública interconectada, conforme analisada por Benkler (2006), é constituída pelo discurso formado através das relações mediadas pelas inúmeras ferramentas das redes. As principais, nesse sentido, são: e-mail, *mass mailing*, blogs, web sites e redes sociais. Isto é, um conjunto de ferramentas discursivas que permitem réplicas por parte dos concernidos e uma ampliação do debate. A partir desse mesmo conceito surgem as questões que hackerativistas buscam superar: o mercado da atenção e as regras da discussão. Com a ampliação das oportunidades de fala, a atenção dos concernidos é algo a ser disputado. Da mesma forma, as regras da discussão devem ser levadas em conta: liberdade de expressão e responsabilidade pública.

As ações diretas virtuais, assim como as realizadas no mundo real, colocam em pauta ou ampliam o debate sobre determinado assunto. As táticas hackerativistas visam justamente isso, um passo além do simples recurso discursivo. No entanto, algumas dessas táticas afetam a liberdade de expressão e a responsabilidade pública. Enquanto a primeira pode atrapalhar o debate democrático, a segunda pode fazer surgir novos temas e opiniões, ainda que isso se insira na zona legalmente ambígua ou ilegal.

O processo deliberativo é apontado por Cohen através de postulados, criticamente apresentados por Habermas (2003). Segundo ele, as deliberações:

a) acontecem de forma argumentativa;
b) são inclusivas e públicas;
c) são livres de coerções externas;
d) são livres de coerções internas;

[19] Tradução livre de: "site defacements, site redirects, denial-of-service attacks, information theft, information theft and distribution, site parodies, virtual sabotage and software development" (SAMUEL, 2004, p.7).

> e) visam a um acordo motivado racionalmente e podem, em princípio, ser desenvolvidas sem restrições ou retomadas a qualquer momento.
> f) políticas abrangem todas as matérias passíveis de regulação;
> g) políticas incluem também interpretações de necessidade e transformação de preferências e enfoques pré-políticos (HABERMAS, 2003, p. 29-30).

A liberdade de expressão é condição essencial para o desenvolvimento do processo deliberativo. Os sujeitos devem poder se expressar sem coerções e/ou constrangimentos. Nesse sentido, o hackerativismo age de maneira ambígua. Por um lado, amplia as vozes dos que não possuem capacidade para se expressar e chamam a atenção para causas e opiniões. Por outro, ao atacarem sites e alterarem o discurso alheio, afetam a liberdade de expressão e a livre formulação de argumentos. No entanto, apenas algumas táticas causam danos à liberdade de expressão, uma vez que, devido ao compromisso moral hacker com a liberdade de informação, tais atos são contraproducentes.

Os sujeitos racionais que entram no debate público são capazes de emitir razões públicas e avaliar razões de outros sujeitos. A responsabilidade por cada razão é inerente à condição de participante de um processo deliberativo, isto é, razões privadas, ilegais ou antidemocráticas limitam as possibilidades de uma boa deliberação. Em um ambiente de esfera pública interconectada está condição se torna mais dispendiosa. Devido à velocidade da troca de informações e de discursos e à natureza horizontal e quase desregulada da rede diversas razões são proferidas sobre determinado tema e várias não contribuem para uma deliberação racional. São mensagens de razões privadas, motivadas por preconceitos e, em alguns casos, ilegais. Por isso, a questão da responsabilidade pública é tão cara ao debate na esfera pública interconectada.

Hackerativistas, em geral, defendem o direito ao anonimato na rede. Da mesma maneira, preferem permanecerem anônimos devido ao ambiente legalmente ambíguo, até mesmo ilegal, no qual suas ações se desenvolvem. Por isso, em um primeiro momento, o hackerativismo atinge a *accountability* necessária para o processo deliberativo de maneira negativa. No entanto, as mesmas ferramentas utilizadas por hackerativistas para garantir o anonimato podem incentivar pessoas a colocarem temas mais complicados em debate. Ainda que os princípios da deliberação apontados acima apontem que todos os temas passíveis de regulação podem ser discutidos, temas relacionados à segurança nacional e segredos de Estados oferecem riscos aos sujeitos que decidem tornar público tais informações e, assim, iniciar um debate.

A organização *Wikileaks*[20] é o principal exemplo nesse sentido. A arquitetura desenvolvida pelos hackerativistas da organização permitia o vazamento de informações sigilosas de governos e corporações, garantindo o anonimato dos informantes. Com isso, diversos casos se tornaram públicos e entraram em debate: os grupos de extermínio no Quênia; os ataques a civis nas guerras do Afeganistão e Iraque; vazamento de cabos diplomáticos dos Estados Unidos (ASSANGE, 2013). Tais vazamentos causaram amplo debate na Esfera Pública e forçaram governos a prestarem contas publicamente. Nesse caso, o anonimato permitiu a livre circulação de temas e problematizações.

A repressão a crimes é o principal argumento contra o total anonimato na rede. Os chamados "Quatro Cavaleiros do Infoapocalipse: lavagem de dinheiro, drogas, terrorismo e pornografia infantil" (APPLEBAUM, 2013, p.87) são a base do discurso de repressão ao anonimato. Além desses citados, podem-se incluir os discursos criminosos de ódio (racismo, xenofobia, homofobia, etc.) como argumento contra o anonimato na rede e na esfera pública interconectada.

Dessa forma, o desafio colocado pelo hackerativismo aponta para um aprofundamento da discussão sobre a qualidade do discurso e das possíveis formas de deliberação online. Retomando os princípios da *Nethic* (HIMANEN, 2001) de *atividade* e *consideração*, fundamento moral da comunidade hacker, a defesa de uma internet livre, democrática e inclusiva, com garantias a direitos individuais básicos como privacidade, surge como o principal norte dos hackerativistas. Os desdobramentos de suas táticas são efeitos colaterais em nome desses princípios, para os quais os outros valores da ética hacker surgem como possível antídoto: valor social e abertura. Suas táticas e ferramentas devem estar a serviço da comunidade e do livre desenvolvimento do conceito individual de boa vida; da mesma forma, elas devem ser abertas para atualizações, sugestões e melhorias por parte dos outros concernidos. Portanto, os desafios criados pelos hackerativistas para a esfera pública interconectada e a deliberação online forçam o aprimoramento e desenvolvimento de novas técnicas e formas discursivas, constituindo-se, assim, mais um impulso nas possibilidades de aprimoramento democrático em conjunto com novas tecnologias.

O presente tópico buscou apresentar em linhas gerais o conceito de esfera pública, a partir da definição habermasiana, e sua evolução para um conceito de esfera pública interconectada, na elaboração de Benkler (2006). Essa reconstrução histórica do termo foi

[20] http://wikileaks.org

necessária para se compreender como arcabouço teórico iniciado em Habermas pode fornecer subsídios para a compreensão de fenômenos contemporâneos como a interação política nas redes. A contribuição de Benkler (2006) é essencial nesse sentido, pois, aponta para novas possibilidades de interconexões na esfera pública, tornando-se mais aberta, porosa e formando canais com vias múltiplas nos quais cidadãos, organizações da sociedade civil e meios de comunicação podem interagir de forma criativa e contínua.

Em seguida, a elaboração da relação entre a popularização da internet e o ativismo política tinha como objetivo demonstrar como a ação política se apropriou dessas ferramentas e desse espaço. O que se observou foi uma relação de apropriação mútua, isto é, o discurso e a ética hacker e o ativismo político do mundo real se uniram para construir o que pode ser chamado de ciberativismo. Posteriormente, com o aprofundamento das táticas hackers de ativismo, o chamado hackerativismo assume uma postura diferente constituindo-se como uma atitude de enfrentamento e conflituosa, afastando-se de uma imagem de esfera pública baseada apenas em lógicas discursivas.

O conceito de esfera pública interconectada traz em si dois desdobramentos que o hackerativismo parece enfrentar: a diminuição da atenção do público e as possíveis ameaçar as regras da deliberação. Ambas as questões são desafios enfrentados por hackerativistas, ora trabalhando para superá-las, ora sendo a causa de tais desequilíbrios. No caso da atenção, as táticas de hackerativistas conseguem atrair a atenção para temas e debates que ainda não atingiram a amplitude necessária na esfera pública. No caso das regras do discurso a questão é mais delicada. Hackers podem tanto facilitar a liberdade de expressão (criando novos espaços e ferramentas), quanto bloquear o discurso de opositores (atacando sites e alterando discursos). A questão do anonimato surge como outro desafio latente. Por um lado, o anonimato pode fomentar atitudes que prejudicariam seriamente a deliberação pública (discursos de ódio e crimes); por outro, a garantia da preservação da identidade serve como estímulo para que questões delicadas sejam colocadas em debate e amplificadas por toda esfera pública.

Portanto, o hackerativismo age colocando novos desafios para o aprimoramento da deliberação pública, principalmente a deliberação online. Suas táticas, embasadas na ética hacker, empurram os limites do discurso e do debate público para novas fronteiras. Da mesma maneira, o comprometimento dos hackers com a liberdade de informação e privacidade aponta, provavelmente, para uma constante evolução. Ainda que questões delicadas e, em

alguns casos, até mesmo ilegais, o hackerativismo parece mais contribuir do que prejudicar a deliberação online.

2.6 SOCIEDADE CIVIL E PODER CIBERNÉTICO

Hackerativismo deriva da ideia central hacker: a informação quer ser livre (LEVY, 2001). Ação cibernética com fins políticos que visa desbloquear o acesso a informações, ou ainda, trazer a tona fatos desconhecidos, porém relevantes, visa atrair luzes para o reconhecimento de questões morais, éticas e sociais, ainda latentes na organização social contemporânea. Isto é, em última instância o ativismo hacker se vale de uma premissa recognitiva: a ideia de que o outro precisa ser levado em consideração em um processo de reconhecimento mútuo - fato que é potencializado e/ou bloqueado pelas possibilidades abertas pelas redes cibernéticas.

Dentro desse contexto, alguns grupos se distinguem de acordo com sua filosofia e ação. Nos últimos anos, com o acirramento acerca do debate sobre o controle e vigilância da internet e seu uso como instrumento de dominação, os hackerativistas autodenominados cypherpunks ganharam notoriedade. O grupo se define da seguinte forma:

> Os cypherpunks defendem a utilização da criptografia e de métodos similares como meio para provocar mudanças sociais e políticas. Criado no início dos anos 1990, o movimento atingiu seu auge durante as "criptoguerras" e após a censura da internet em 2011, na Primavera Árabe. O termo *cypherpunks*[21] – derivação (criptográfica) de *cipher* e *punk* – foi incluído no *Oxford English Dictionary* em 2006. (ASSANGE, 2013, p.5)

Ao levarem às últimas consequências a luta pela privacidade, os cypherpunks chamam a atenção para a desconsideração da esfera privada na constituição de políticas públicas - principalmente de segurança nacional. Ao negar o acesso a dados privados, os cypherpunks e cidadãos estão se colocando em posição de igualdade com as instituições (Estado e corporações) tentando reverter uma situação assimétrica.

[21] Além da etimologia da palavra, há uma referência explícita ao termo cyberpunk, criado por William Gibson (1984). O termo cyberpunk surgiu para designar um subgênero de ficção científica, mas logo passou a rotular toda uma subcultura, influenciando moda, cinema, literatura e música. Seu foque principal é na ideia "*high tech, low life*" (Alta tecnologia e baixo nível de vida) e nas relações entre humanos e máquinas. Para mais referências, consultar a obra "Visões Perigosas: uma arque-genealogia do cyberpunk" de Adriana Amaral (2006).

A primeira esfera na qual a luta dos hackerativistas se desenvolve é a jurídica. Governos e corporações buscam restringir e controlar o acesso a informações e defender o direito de cópia. Projetos de lei nos Estados Unidos são principais exemplos – cabe ressaltar que devido a sua centralidade na arquitetura da rede e seu poder econômico e político, leis norte-americanas acabam influenciando todo o mundo. As principais são: DMCA (*Digital Millennium Copyright Act*[22]) de 1998; SOPA (*Stop Online Piracy Act*[23]) e PROTECT IP Act (*Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011*[24]) de 2011. Em linhas gerais, todas tentam aumentar a repressão ao compartilhamento de arquivos sob a alegação de violação de direitos autorais. Tais medidas constituem a primeira face *hard power* do poder cibernético dos Estados. No entanto, apenas o DMCA entrou em vigor, os outros dois foram duramente combatidos por ativistas em todo o mundo, causando a retirada dos projetos da pauta de votação.

A associação entre hackers e crimes é praticamente instantânea no discurso construído e no arcabouço jurídico. Assim, os hackers e, consequentemente, os hackerativistas são excluídos do reconhecimento jurídico, sendo publicamente considerados ameaças à propriedade intelectual e financeira. Esse fato motiva a ação moralmente motivada dos hackers, isto é, ativismo política baseado na Nethic. Esse esforço visa se afastar do conceito de *cracker*[25] e buscar o reconhecimento jurídico de suas demandas nas redes.

Da mesma forma, os cypherpunks, que também são hackerativistas motivados por sua própria ética e moral, criam ferramentas para reverter à situação assimétrica garantida pela pelo poder de coerção estatal no ciberespaço vigente. Em nome da segurança nacional, governos têm estabelecidos leis e mecanismos de vigilância em massa das comunicações[26]. Assim, esses ativistas fornecem ferramentas para que cidadãos e grupos garantam sua

---

[22] Disponível em: http://www.copyright.gov/legislation/dmca.pdf (Acesso em 25/01/2014).
[23] Disponível em: https://www.govtrack.us/congress/bills/112/hr3261 (Acesso em 25/01/2014).
[24] Disponível em: https://www.govtrack.us/congress/bills/112/s968 (Acesso em 25/01/2014).
[25] "This original benevolent meaning stands in stark contrast to the later and more commonly used meaning of a "hacker", typically as a person who breaks into computer networks in order to steal or vandalize. Here at TMRC, where the words "hack" and "hacker" originated and have been used proudly since the late 1950s, we resent the misapplication of the word to mean the committing of illegal acts. People who do those things are better described by expressions such as "thieves", "password crackers". or "computer vandals". They are certainly not true hackers, as they do not understand the hacker ethic." Definição do primeiro grupo de hackers, o Tech Model Railroad Club of MIT. Disponível em: http://tmrc.mit.edu/hackers-ref.html (acesso 25/01/2014). Ver também "Hacker: heroes of the computer revolution" de Steven Levy (1984).
[26] O principal exemplo é o "Patriot Act" de 2001. Criado logo após os atentados ao World Trade Center, durante a gestão Bush, a lei amplia os poderes do Estado para investigar, espionar e prender qualquer pessoa suspeita de terrorismo ou envolvimento com organizações terroristas.

privacidade e impeçam que os governos tenham acesso aos dados, desafiando o estatuto legal e forçando uma luta por reconhecimento e ampliação desses direitos.

> Acho que nós hackers somos responsáveis pelas ferramentas que construímos e disponibilizamos para o resto do mundo, e pode ser que estejamos testemunhando o início da prática eficiente dessa responsabilidade, quando tais ferramentas são usadas coletivamente. (...) nós, como cidadãos, temos o poder de matar de matar esse monstro (ACTA[27]) – com facilidade, com as ferramentas da internet, com as listas de discussão, os wikis e os fóruns de bate-papo, entre outros –, e acho que podemos estar testemunhando o despertar da maturidade da internet, sua entrada na adolescência e a evolução das maneiras pelas quais ela pode ser utilizada pela sociedade em geral para tentar promover mudanças (ZIMMERMANN, 2013, p. 86).

No atual contexto, a principal fonte de poder dos hackerativistas é o vazamento de informações sigilosas de Estados e corporações. A organização Wikileaks, liderada pelo hacker Julian Assange, é o principal exemplo. Ao desenvolver uma arquitetura que permitia o anonimato dos chamados *whistleblowers*[28], a organização conseguiu divulgas milhares de documentos sigilosos, como por exemplo: denúncias de esquadrões da morte no Quênia; documentos das guerras do Afeganistão e Iraque; e cabos diplomáticos das embaixadas norte-americanas (LEIGH & LUKE, 2011).

O vazamento de documentos sigilosos como instrumento de pressão nos Estados e/ou organizações não é fenômeno exclusivo do hackerativismo. Na década de 1970, Daniel Ellsberg foi o responsável pelo vazamento de um documento chamado “Pentagon Papers”, no qual expunha a situação norte-americana no conflito no Vietnã. Para empreender tal tarefa, Ellsberg empregou uma imensa quantidade de tempo e dinheiro, uma vez que todo o trabalho de copiar os documentos era feito de forma manual.

> It took the Harvard – and Cambridge- educated analyst more than a year of on-and-off grunt work to create a full set of the papers and duplicate them at commercial copy centers, eventually creating an eight-foot-tall stack of breached classified documents. At ten cents a page in those shops, the process also required Ellsberg to spend several thousand dollars. (The equivalent of more than twenty thousand dollars today, accounting for inflation) (GREENBERG, 2012, p. 20).

Com a junção do ativismo político com as novas tecnologias, o vazamento de informações se tornou mais fácil e mais abrangente. Os documentos do exército norte-americano vazados por Bradley Manning, um analista de inteligência, ultrapassam em

---

[27] Anti-Counterfeiting Trade Agreement (Acordo Comercial Antifalsificação), um acordo multinacional nos moldes da SOPA e PIPA (ZIMMERMAN, 2013, p. 86).

[28] Em tradução livre, whistleblower é o indivíduo responsável pelo vazamento de informações sigilosas de governos e/ou corporações.

quantidade os “Pentagon Papers”. No entanto, foram obtidos e disseminados de maneira mais rápida e efetiva. Aqui reside o potencial do poder cibernético dos indivíduos e organizações. A comparação com o vazamento de Ellsberg demonstra como o poder cibernético pode atuar e fazer com que vozes dissidentes sejam ouvidas no debate global.

> In the midst of his work as a low-level intelligence analyst in Iraq, Manning slipped a rewritable CD marked with “Lady Gaga” into the tray of his work machine, a PC connected only to the military’s high-security Secret Internet Protocol Router Network, or SIPRNet. The SIPRNet was “air-gapped”: It wasn’t connected to the Internet through any plug or wireless signal. But Manning could simply copy the CD’s music to the computer, delete it from the rewritable disc, burn whatever top secret data he wanted to the piece of plastic, and walk away with it minutes later. (...) The data caches that Manning replicated, allegedly, included 91,000 files from the war in Afghanistan, 392,000 from the Iraq War, 779 files of inmates in the Pentagon’s Guantánamo prison, and a quarter of a million memoranda from the U.S. State Department, which also shared its data with troops via SIPRNet. (GREENBERG, 2012, p.21)

As fortes sanções sofridas por Manning (condenado a trinta anos de prisão) demostram a face *hard power* do poder estatal, com o objetivo não só de punir o soldado pelo vazamento mas, principalmente, desencorajar atos futuros da mesma natureza. No entanto, atos mais recentes como o de Edward Snowden demonstram que a motivação moral, baseada em um compromisso com a liberdade de informação, ainda serve como impulso para enfrentar possíveis sanções e colocar na agenda temas pertinente para toda a comunidade internacional.

Edward Snowden, ex-funcionário da NSA (*National Securty Agency*), foi responsável por uma série de vazamentos de documentos que demonstravam a forma de operar da agência norte-americana, capturando dados telefônicos e na internet e espionando líderes mundiais. Suas revelações foram divulgadas pelo jornal britânico *The Guardian* e tiveram enorme repercussão internacional. Países como Brasil e Alemanha eram apontados como alvos da espionagem norte-americana. Como principal resultado, a presidenta Dilma Roussef cancelou uma visita oficial aos Estados Unidos[29] e, juntamente, com a Alemanha iniciaram uma proposta de regime internacional de regulação da internet junto a Organização das Nações Unidas[30].

O caso Snowden é um exemplo de como o poder cibernético funciona de maneira dinâmica. Estados usam as redes para espionar cidadãos, corporações e outros Estados.

[29] http://www.estadao.com.br/noticias/nacional,dilma-cancela-viagem-aos-eua,1075730,0.htm

[30] http://www.itamaraty.gov.br/sala-de-imprensa/notas-a-imprensa/resolucao-sobre-o-direito-a-privacidade-na-era-digital

Corporações usam o poder cibernético para espionagem industrial e coleta de dados de consumidores. Já os indivíduos podem se valer do poder cibernético para se proteger de ingerências, atacar Estados e corporações ou para reverter assimetrias. Por exemplo, ao usar o poder cibernético Edward Snowden conseguiu interferir diretamente na política internacional, estremecendo relações entre países e fomentando uma resolução conjunta nas Nações Unidas. Vale ressaltar que os motivos das reações às denúncias foram as próprias ações dos envolvidos, o ato de Snowden consistiu em tornar público o que antes era sigiloso, trazendo o tema para a agenda global.

Dessa forma, considerando que o poder é exercido por A sobre B, o poder cibernético pode ser organizado da seguinte forma:

Quadro 1 – Relações de poder cibernético

A/B	Estados	Corporações	Sociedade Civil
Estados	Espionagem, coerção e controle de infraestrutura, ciberataques.	Coleta de dados e controle do mercado e da infraestrutura	Coleta de dados e monitoramento de comunicações; coerção legal.
Corporações	Desenvolvimento de softwares e hardwares	Espionagem industrial	Coleta e venda de dados pessoais
Sociedade Civil	Criptografia, vazamento de informações sigilosas e ciberataques.	Criptografia, software livre e ciberataques.	Organizações civis, campanhas públicas e mobilizações, criação de ferramentas colaborativas.

O custo da ação individual, ou em pequenos grupos, também é drasticamente afetado pelo poder cibernético. Impactar no espaço público global e na agenda internacional demanda poder de coerção e barganha, tradicionalmente garantidas para os Estados pelo poder econômico e o poder militar. O ativismo operava em pequeno raio de ação e, na maioria das vezes, conseguia afetar apenas o ambiente doméstico. Com a assimilação das ferramentas tecnológicas e a apropriação de um tipo de poder cibernético por parte de ativistas, tais ações

e campanhas passaram a se articular em escala global. O Movimento Zapatista (1994) e a organização da Batalha de Seattle (1999) foram os primeiros exemplos desse tipo de ativismo globalmente articulado.

Após a crise de 2008 diversos movimentos de contestação surgiram no cenário internacional – Primavera Árabe, *Occupy Wall Street*, Indignados, 15M, apenas para citar alguns. Apesar de divergentes em seus próprios contextos e demandas, a utilização do poder cibernético é uma constante em todos eles. As ferramentas proporcionadas pelas redes fomentaram o debate público, as mobilizações e interferiram diretamente na agenda global. Contudo, não se descarta aqui a potência política das multidões, apenas ressalta-se o poder cibernético como fator que atua diminuindo as assimetrias de poder entre os atores envolvidos. Tais formas de empoderamento, a partir do poder cibernético, estão fomentando inciativas criativas ao redor do mundo para superar o déficit democrático. Como exemplo, os estudos sobre a tecnopolítica de Javier Toret (2013), fruto do 15M na Espanha, são os mais avançados nesse sentido, visando reunir a energia do ativismo com as ferramentas do ciberespaço, abrindo novos canais de participação e formas de exercício do poder cibernético.

3 PRIVACIDADE, EXCEÇÃO E RESISTÊNCIA

O presente capítulo enfrenta o desafio de demarcar o debate e o ativismo cypherpunks. Para isso, parte de três pontos considerados centrais: privacidade, Estado de Exceção e resistência. Dessa forma, busca-se discutir o sentido de privacidade, por meio de uma breve reconstrução histórica do conceito, e debater seu estatuto de proteção normativa frente a um aparato de controle. O que resulta de tal análise está em consonância com um dos grandes desafios políticos e da agenda de Direitos Humanos do século XXI: a efetivação de direitos. A tensão entre o que está normatizado e as garantias reais dão a tônica dessa questão.

A partir disso, a dificuldade de efetivação dos direitos será tratada em uma chave explicativa a partir da obra de Giorgio Agamben (2004). Obviamente, tal abordagem não esgota a ampla discussão sobre a efetivação e garantia de direitos fundamentais e outros fatores deveriam ser levados em consideração para abarcar o problema. Porém, a teoria de Agamben sobre a crescente utilização do Estado de exceção como técnica de governo parece fornecer elementos que sustentam a crítica à violação de direitos. Ao discutir a técnica da exceção aliada à militarização do ciberespaço busca-se apresentar como o ativismo se insere nessa zona de suspensão de direitos, articulando sua luta para uma esfera além da normativa.

Por fim, a resistência será tratada a partir do debate estabelecido no capítulo anterior. O objetivo é: identificar exemplos no Brasil; apontar pontos em comum entre as diferentes formas de organização dos ativistas. Dessa forma, pretende-se situar o debate e, principalmente, a ação no Brasil. Com isso, comparando discursos e formas de ação, busca-se definir conceitos-chaves que permitam a análise empírica das redes e o mapeamento no capítulo seguinte.

3.1 PRIVACIDADE

A privacidade de dados e comunicações está hoje no centro do debate sobre a relação Estado e indivíduo. Considerado um direito essencial e garantido em diversas Constituições, o direito à privacidade se depara com a disseminação de dados nas redes cibernéticas, em especial a internet, e ao mesmo tempo uma doutrina de segurança que trata o ciberespaço como uma fronteira de guerra a ser dominada. Porém, a discussão sobre o tema remonta ao embate entre utilitaristas e liberais (SILVEIRA, 2009b).

O utilitarismo de Jeremy Bentham e Stuart Mill argumenta que a busca pela felicidade é o maior ideal da existência humana e, por isso, deve ser perseguida a todo custo. Essa corrente filosófica acreditava poder calcular objetivamente o sofrimento e o prazer de uma determinada população, cabendo ao bom governo fornecer subsídios, por meio da educação e da legislatura, de superação do sofrimento e busca da felicidade. Assim, as ações são medidas de acordo com sua utilidade em busca do propósito maior: a felicidade. “Por felicidade se entende prazer e ausência de dor; por infelicidade, dor e a privação do prazer. (MILL, 2000, p. 187)”.

Nessa busca por arranjos sociais visando à felicidade comum, Bentham rejeitava qualquer incerteza acerca da identidade dos indivíduos, pois a falta de conhecimento claro sobre cada um dificultava ou inviabilizava os cálculos de bem-estar geral. Uma de suas obras mais famosas, o Panopticon, é retomada por Foucault em seus estudos sobre as prisões e a construção de uma sociedade disciplinar. O que Foucault observa é o desejo de Bentham em construir um tipo de controle social no qual o indivíduo estaria sob uma constante vigilância, de tal forma que esta seria introjetada no seu modo de ser gerando um senso de autovigilância. Foucault estabelece ainda uma relação entre o objetivo utilitarista de Bentham e o lirismo revolucionário, de inspiração rousseuniana, presente na Revolução Francesa.

> Eu diria que Bentham é o complemento de Rousseau. Na verdade, qual é o sonho rousseauniano presente em tantos revolucionários? O de uma sociedade transparente, ao mesmo tempo, visível e legível em cada uma de suas partes; que não haja mais nela zonas obscuras, zonas reguladas por privilégios do poder real, pelas prerrogativas de tal ou tal corpo ou pela desordem; que cada um, do lugar que ocupa, possa ver o conjunto da sociedade; que os corações se comuniquem uns com os outros, que os olhares não encontrem mais obstáculos, que a opinião reine, a de cada um sobre cada um. (FOUCAULT, 2014, p.326).

Partindo dessa ideia, Foucault identifica em Bentham a ideia de uma constante vigilância por meio da opinião. Isto é, todos estariam visíveis e abertos a uma vigilância coletiva, por esse motivo, não seriam punidos por cometer o mal, mas sim, estariam tão inseridos em contexto de vigilância que não cogitariam fazer o mal. Em contrapartida, o pensamento liberal considera que a defesa da esfera da vida privada é essencial para arranjo da sociedade. O pioneiro nesse pensamento é o filósofo liberal francês Benjamin Constant. Para ele, a defesa do anonimato e da privacidade era essencial para o que chamava de “liberdade dos modernos”: “A ideia de liberdade para os modernos, segundo Constant, incorpora a esfera privada e os direitos dos indivíduos diante das maiorias. Para ele, não cabe

ao Estado legislar sobre tudo, sobre comportamentos, crenças, inclinações e fantasias dos indivíduos." (SILVEIRA, 2009b, p.125).

A discussão levantada por Constant sobre "liberdade dos antigos" e "liberdade dos modernos" também pode ser colocada nos termos de um debate entre liberais e republicanos. Isto é, republicanos colocariam a esfera privada e as liberdades individuais como subordinadas aos interesses do bem coletivo; enquanto liberais defenderiam as liberdade individuais e o direito a uma vida privada, longe de intervenção ou regulação estatal.

Com o paradigma do Estado Constitucional, de inspiração liberal, o direito à privacidade aparece em diversas constituições como um direito fundamental. A Constituição Americana (1787), em sua Quarta Emenda, de 1791, deixa claro o direito à inviolabilidade das casas, pessoas e correspondências.

> Amendment IV: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. (USA, 1791).

O objetivo dessa emenda é proteger os cidadãos contra buscas em seus domicílios, violação das correspondências e um estado de vigilância constante. Fato com o qual os colonos lidavam desde o domínio britânico.

Na verdade, a oposição à invasão de privacidade pelo governo foi um fator decisivo para a fundação dos próprios Estados Unidos, quando colonos norte-americanos protestaram contra leis que permitiam aos agentes do governo britânico saquear qualquer casa que quisessem. Os colonos concordavam que fosse legítimo o Estado obter mandados específicos para revistar pessoas quando os indícios estabelecessem uma causa provável para suas infrações. Mas os mandados genéricos – a prática de submeter a população inteira a revistas indiscriminadas – eram fundamentalmente ilegítimos (GREENWALD, 2014, p.12)

Da mesma forma, a Constituição brasileira garante a intimidade e a vida privada, a inviolabilidade da casa e o sigilo das correspondências e comunicações telefônicas (BRASIL, Artigo 5°, inciso XII, 1988). Uma análise comparativa de diversas constituições, o que não é o objetivo do presente trabalho, demonstraria que o direito à privacidade e ao sigilo das comunicações está presente em diversos países.

De maneira análoga, a legislação internacional também atua no sentido de manutenção de tais direitos. A Declaração Universal dos Direitos do Homem, de 1948, traz em seu Artigo 12°: "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei" (ONU, 1948).

O Pacto Internacional sobre Direitos Civis e Políticos, adotado pela XXI Assembleia Geral da ONU, de 1966, assinado e ratificado pela maioria dos países-membros[31], também é explícito em seu Artigo 17°:

> 1. Ninguém poderá ser objetivo de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais às suas honra e reputação. 2. Toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas (ONU, 1966).

As denúncias do ex-técnico da NSA (National Security Agency) Edward Snowden, em 2013, demonstravam a abrangência e o poder de interceptação de comunicações do governo norte-americano (GREENWALD, 2014; HARDING, 2014). O impacto de tais revelações levaram os governos de Brasil e a Alemanha a apresentar uma resolução condenando tais práticas e reforçando o direito à privacidade. O documento ressalta que o direito à privacidade é um direito humano e, além disso, amplia a compreensão de que as pessoas possuem os mesmos direitos tanto online quanto off-line.

> 1. Reafirma os direitos previstos no Pacto Internacional sobre Direitos Civis e Políticos, em particular o direito à privacidade e a não ser submetido a ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, bem como o direito à proteção da lei contra essas ingerências ou ofensas, de acordo com o artigo 12 da Declaração Universal dos Direitos Humanos e artigo 17 do Pacto Internacional sobre Direitos Civis e Políticos; 2. Reconhece que o rápido avanço das tecnologias da informação e da comunicação, inclusive a natureza global e aberta da Internet, constitui força motriz da aceleração do progresso para o desenvolvimento em suas várias formas; 3. Afirma que os mesmos direitos que as pessoas possuem fora da rede ("offline") devem ser protegidos em rede ("online"), em particular o direito à privacidade; (ASSEMBLEIA GERAL DA ONU, 2013).

A extensão da compreensão de direitos online de maneiro análoga aos direitos off-line abre um novo campo de discussão para a privacidade e a segurança de dados. O que fica

[31] O Brasil ratificou a assinatura em 1991, depositando a adesão em janeiro de 1992. De acordo com o Artigo 49° do Pacto Internacional sobre Direitos Civis e Políticos: "2. Para cada Estado que ratifique o presente Pacto, ou a ele adira, depois de ter sido depositado o trigésimo quinto instrumento de ratificação ou de adesão, o Pacto entrará em vigor decorridos três meses após a data em que esse Estado tenha depositado o seu instrumento de ratificação ou de adesão". Sendo assim, o Pacto entra em vigor no Brasil em abril de 1992. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/D0592.htm (Acesso em 20/09/2014).

evidente é existência de um arcabouço jurídico que visa proteger tais direitos. A ampliação do direito ao sigilo em correspondências, incluindo as comunicações eletrônicas, é um avanço nesse sentido. O que ocorre, porém, é que a natureza do ciberespaço dificulta de maneira única a garantia de tais direitos. Isto é, a forma como a arquitetura e a infraestrutura da rede estão organizadas, os protocolos de comunicação e, principalmente, a doutrina de militarização do ciberespaço constituem obstáculos para o funcionamento de tais mecanismos jurídicos. O que se objetivou nesse tópico foi demonstrar, brevemente, como o direito à privacidade surge do debate entre utilitaristas e liberais, sendo, posteriormente, acolhido em diversas cartas constitucionais e em tratados internacionais. O que se objetiva no tópico seguinte é discutir como uma doutrina de militarização do ciberespaço e o conceito de Estado de Exceção inviabilizam a garantia de tais direitos.

3.2 ESTADO DE EXCEÇÃO EM GIORGIO AGAMBEN

A doutrina de segurança norte-americana inaugurada pelo governo George W. Bush e as consequentes violações massivas de direitos humanos, principalmente direito à privacidade, podem ser compreendidas a partir dos estudos do filósofo italiano contemporâneo Giorgio Agamben.

Nas obras "Homo Sacer – poder soberano e vida nua" (2002) e "Estado de Exceção" (2004), Giorgio Agamben trata de temas cruciais para o debate político e dos direito humanos na contemporaneidade. A ideia de um poder soberano capaz de despir de direitos políticos determinados indivíduos ou grupos os deixando "nus" (homo sacer), isto é, contando apenas com seu aspecto biológico como forma de sobrevivência, é o ponto de partida para sua investigação. Nesse caminho, Agamben parte de uma visão hobbesiana e, em especial em seu estudo sobre Estado de exceção, estabelece diálogo com a obra de Carl Schmmitt.

O Estado de Exceção em Agamben encontra-se um espaço ambíguo e indefinido, uma zona de junção entre o jurídico e o político, assim como a guerra civil, a insurreição e a resistência. "O estado de exceção apresenta-se como forma legal daquilo que não pode ter forma legal" (AGAMBEN, 2004, p. 12). Em seu estudo, o filósofo aponta como diversos juristas tentaram conter o estado de exceção dentro do aspecto jurídico[32], tentar dar amparo legal a algo que é, em si, a suspensão do estatuto jurídico. Percebendo tal paradoxo, Agamben

[32] Diversos países apresentam em suas constituições as atribuições de um "Estado de Sítio" ou "Matial Law".

busca apontar como o estado de exceção se torna, cada vez mais a partir do século XX, uma técnica de governo. Sendo assim, sua inscrição na ordem jurídica não é necessária devido à existência de outras formas de exercício da exceção.

Agamben retoma a famosa definição de soberano de Carl Schmitt, que afirma que soberano é "aquele que decide sobre o estado de exceção", para debater sobre quem determina a necessidade. O princípio necessitas legem non habet (a necessidade não tem lei) pode ser usado para determinar uma situação na qual a manutenção da ordem e preservação do estatuto jurídico vigente dependem da suspensão dos mesmos. Nesse sentido, uma teoria sobre o estado de exceção se divide em dois grupos: aqueles que tentam inserir a exceção no ordenamento jurídico e os que a consideram exterior a esse ordenamento. Para Agamben, o estado de exceção não está nem dentro nem fora do ordenamento jurídico, pois a "suspensão da norma não significa sua abolição e a zona de anomia por ela instaurada não é (...) destituída de relação com a ordem jurídica" (AGAMBEN, 2004, p. 39). Portanto, mais uma vez, para Agamben o estado de necessidade é o fundamento do estado de exceção.

> O princípio de que a necessidade defina uma situação particular em que a lei perde sua vis obligandi (esse é o sentido do adágio necessitas legem non habet) transforma-se naquele em que a necessidade constitui, por assim dizer, o fundamento último e a própria fonte da lei. Isso é verdadeiro não só para os autores que se propunham a justificar desse modo os interesses nacionais de um Estado contra um outro (...), mas também para os juristas, de Jellinek a Duguit, que veem na necessidade o fundamento da validade dos decretos com força de lei emanados do executivo no estado de exceção (AGAMBEN, 2004, p. 43)

Porém, a crítica que é construída diz respeito ao próprio conceito de necessidade. Diversos autores continuam a tratar de maneira ingênua, segundo Agamben, a necessidade como uma situação objetiva. Dessa forma, a necessidade pode ser um juízo subjetivo e, com isso, as medidas tomadas em seu nome, de caráter excepcional, podem estar submetidas a objetivos específicos. Por isso, "a necessidade se reduz, em última instância, a uma decisão, como também aquilo que ela decide é, na verdade, algo indecidível de fato e de direito" (AGAMBEN, 2004, p. 47).

Ao analisar a doutrina de segurança do governo Bush, Agamben aponta para como o estado de exceção instaurado após os atentados de 11 de setembro de 2001 cria uma ordem na qual é possível "anular radicalmente todo estatuto jurídico do indivíduo, produzindo dessa forma, um ser juridicamente inominável e inclassificável" (AGAMBEN, 2004, p. 14). A necessidade de combate ao terrorismo é o fundamento de um estado de exceção permanente,

no qual indivíduos são despidos de seus direitos civis e colocados em uma zona de anomia onde o ordenamento jurídico é suspenso.

Considerando o que foi discutido acima, a doutrina de segurança para a fronteira ciberespacial e o estado de exceção instaurado simultaneamente são uma ameaça real aos direitos humanos e, em especial, o direito à privacidade. Pois, ainda que garantidos pelo ordenamento jurídico interno e resguardados pelo direito internacional, tais direitos são suspensos em nome de uma necessidade. Nesse sentido, a defesa de tais direitos, a militância e resistência política no ciberespaço passam a depender mais das leis da física do que das leis dos homens.

A crítica de Agamben abre uma possibilidade interpretativa para os grupos de resistência. Uma vez que, a ideia de uma Esfera Pública Interconectada, descrita anteriormente, está condicionada a uma arquitetura e uma topologia da rede, que podem ser usadas como instrumentos de controle e influência no próprio debate. Por tal razão, grupos ciberativistas precisam enfrentar um desafio duplo: em primeiro lugar, denunciar discursivamente tais mecanismos de controle e de militarização que estão em andamento; em segundo lugar, criar e divulgar técnicas de superação da dominação e do controle no ambiente virtual. Os ciberativistas e hackerativistas denunciam e, ao mesmo tempo, tentam desconstruir o aparato de controle. Nesse sentido, a ideia de um Estado de exceção aliado a um aparato cibernético de controle só pode ser enfrentado para além de uma esfera normativa e discursiva.

Esse debate tem repercutido em todo mundo principalmente após dois eventos-chave: o Cablegate do Wikileaks, em 2010; e o vazamento de documentos da NSA por Edward Snowden. Enquanto o Wikileaks denunciou abusos cometidos pelos Estados Unidos na ocupação do Iraque e outros segredos da diplomacia norte-americana, os documentos vazados por Edward Snowden demonstraram a amplitude e a capacidade de monitoramento da NSA, empresas e outras agências. Tais denúncias reverberaram de maneira especial no Brasil, levando ao cancelamento de uma visita oficial da presidenta Dilma Rousseff os Estados Unidos e ao documento apresentado nas Nações Unidas em conjunto com a Alemanha.

Além disso, ativistas, coletivos e outras organizações da sociedade civil já travavam um amplo debate em torno da regulação, legislação e controle da internet no país. A discussão que levou ao Marco Civil da internet no Brasil, apesar de não ser o objeto de interesse do

presente estudo, demonstrou o poder de mobilização desses diversos atores da sociedade civil, ainda que com algumas derrotas no campo legislativo.

Por essa razão, enumerar e descrever, brevemente, os principais grupos ativistas do Brasil é uma tarefa fundamental para a criação de conceitos e indicadores para a etapa seguinte do presente trabalho. Isto é, analisando as formas de organização e os principais tópicos debatidos será possível criar palavras-chaves e/ou conceitos para uma busca de dados nas redes.

3.3 GRUPOS ATIVISTAS NO BRASIL

A relação entre ativismo, participação política e novas tecnologias tem sido tema de amplo debate no Brasil[33]. Tais discussões, em geral, giram em torno da apropriação da tecnologia por parte de movimentos, da internet como instrumento da ampliação da participação política e etnografias de comunidades virtuais. Essas contribuições ampliam o conhecimento sobre os atores envolvidos nos processos e apontam para novas agendas de pesquisas.

O que se pretende aqui é apresentar os principais agentes envolvidos, atualmente, no debate sobre privacidade e internet no Brasil. Para isso, em primeiro lugar, foram coletados documentos e publicações de diversas organizações. Nesse sentido, estabelece-se aqui a hipótese a ser testada de que as organizações aqui listadas são Autoridades e/ou Hubs no debate sobre privacidade, política e internet no Brasil. Segundo Sérgio Amadeu da Silveira (2013): “enquanto um bom HUB representa um nó que aponta para muitos ‘nós’ da rede, uma boa Autoridade é apontada por diversos outros HUBs.” (2013). Isto é, quando um nó na rede tem vários post replicados ele pode ser considerado uma autoridade; por outro lado, quando um nó replica muito conteúdo de outros nós ele pode ser considerado um Hub.

As organizações aqui apresentadas foram escolhidas como possíveis Autoridades e/ou Hubs devido a sua presença constante nos debates online e off-line. Dessa forma, comprovando-se tais hipóteses, será possível mapear o impacto do ativismo anti-vigilância na internet brasileira. Determinar as Autoridades e os principais Hubs é o primeiro passo para se identificar o potencial e a forma de organização dessa rede. As fontes usadas para a descrição

[33] A ANPOCS (Associação Nacional de Pós-Graduação e Pesquisa em Ciências Sociais) tem dedicado Grupos de Trabalho exclusivamente para debater o tema, demonstrando a importância do tema para a pesquisa social no Brasil. Além disso, a ABCIBER (Associação Brasileira de Cibercultura) se dedica exclusivamente a promover a pesquisa e a troca de conhecimento na área.

e análise dos principais atores são os documentos e publicações elaborados pelas organizações, todas disponíveis em seus respectivos websites e/ou redes sociais (Facebook e Twitter).

3.3.1 Partido Pirata

O Partido Pirata brasileiro (sigla PIRATAS) faz parte da rede de partidos piratas espalhados pelo mundo. Após surgir na Suécia (PiratPartiet) em 2006, os ideais de livre compartilhamento de informações, luta contra as leis de propriedade intelectual, e contra as violações contra a privacidade logo se espalharam pelo mundo. Segundo os dados do próprio partido[34], existem hoje movimentos, partidos regularizados e/ou em vias de regularização em 43 países.

O primeiro fato que chama a atenção em relação aos partidos piratas, que o difere dos demais movimentos, é a opção pela disputa dentro do sistema político. Isto é, tentar ampliar as ações e os ideais do ativismo, virtual ou não, disputando eleições. Na Suécia, seu local de origem, o partido elegeu um eurodeputado em 2009. Na Alemanha foram eleitos 43 deputados nas eleições estudais de 2012.

No Brasil, o Partido Pirata surgiu como um coletivo de ativistas em 2007. Entre 2009 e 2011, o Movimento do Partido Pirata do Brasil (MPPBr) criou coletivos em diversos estados visando a legalização da legenda. Esse crescimento levou a fundação oficial do partido em convenção realizada em julho de 2012. Seguindo o que prevê a lei, o partido publicou seu estatuto e programa no Diário Oficial da União em setembro de 2013. Desde então, vem atuando na criação de coletivos regionais, fortalecimento das pautas e coleta de assinaturas para disputar as eleições de 2016.

Em relação a sua forma, o Partido Pirata se declara diferente dos partidos convencionais: “Atuamos de forma distribuída e não-hierárquica” (PIRATAS, online). Seus documentos e declarações apontam para uma tentativa de desenvolver um modelo de participação ciberneticamente mediado. Internamente, o partido experimenta técnicas de deliberação online de ampla participação por meio de uma rede social própria (http://social.partidopirata.org/) e da plataforma deliberativa *Loomio* (https://www.loomio.org/?locale=pt-BR). Embora não seja o tema do presente trabalho, vale ressaltar que as experiências de integração entre tecnologia e deliberação tentam suprir as

[34] http://www.pp-international.net/ (acesso em 20/11/2014).

lacunas e limitações apontadas no campo da Democracia Deliberativa – debate fundamental para a ciência política, em especial no Brasil.

Em seu Estatuto, no artigo 3°, o Partido Pirata declara suas cláusulas pétreas que devem guiar sua atuação política:

> I – a defesa dos direitos humanos e das liberdades civis; II – a defesa do direito à privacidade; III – a defesa ao acesso livre à informação; IV – a defesa do acesso e compartilhamento livres de cultura e conhecimento; V – a transparência pública; VI – a democracia plena; VII – o Estado Laico; VIII – a liberdade de expressão; IX – a colaboratividade; X – a igualdade de gênero, em todas as suas expressões; XI – o combate a todas as formas de discriminação; XII – o combate a todas as formas de autoritarismo; XIII – a defesa do direito inalienável de resistir à opressão; XIV – o internacionalismo; XV – a defesa do ativismo hacker; XVI – o gozo pleno dos direitos inerentes à cidadania, inclusive políticos, ativos e passivos, independente da nacionalidade; XVII – a plena autodeterminação individual; XVIII – a neutralidade da rede. (PIRATAS, 2013, online).

O ativismo hacker, a cibercultura e os conceitos de livre informação e livre compartilhamento estão fortemente contemplados em suas cláusulas pétreas. A defesa aos direitos humanos é depurada em temas específicos como defesa da privacidade, do acesso ao conhecimento, da liberdade de expressão, das formas de discriminação. Para além desses tópicos, o comprometimento com a internet como matriz de sua atuação política fica evidente no inciso XVIII, que defende a neutralidade da rede.

Por outro lado, em suas Diretrizes e em seu Programa o Partido Pirata defende de maneira relativamente vaga em relação a temas centrais do debate político como: saúde, educação e segurança pública. Por exemplo, em sua diretriz para educação: “O Partido Pirata propõe a reformulação dos princípios que regem a educação no Brasil, assumindo o compromisso de envolver de forma colaborativa e transparente os agentes que interagem no processo educacional” (PIRATAS, 2013, online). Ou ainda, diretriz para saúde: “O Partido Pirata reafirma a necessidade da universalização do acesso à saúde – em todas as esferas – e o aprimoramento da gestão de atendimento através de ferramentas eletrônicas” (PIRATAS, 2013, online). Ao confrontar temas da agenda tradicional dos partidos fica mais claro que o leitmotiv dos Piratas é a relação entre tecnologia e política.

O Programa do Partido Pirata reserva um amplo espaço para demarcar suas posições em relação a temas da internet. Os seguintes tópicos demonstram isso de maneira mais enfática: 2. Transparência e Eficiência da Gestão Pública; 3. Privacidade; 4. Internet como bem universal acessível a todas as pessoas; 5. Direitos Autorais e Reprodução Não-comercial;

6. Patentes; 7. Padrões Abertos e Software Livre; 8. Políticas de Cultura; 9. Liberdade nas Comunicações. (PIRATAS, 2013, online). As propostas de técnicas de governo passam, necessariamente, pela ampliação do uso de novas tecnologias e abertura dos processos. Da mesma forma, a ampliação de direitos caminha lado a lado com o aumento das possibilidades de participação e, principalmente, da qualidade da deliberação.

Nesse sentido, pode-se elencar como os pontos principais do discurso e do programa do Partido Pirata: liberdade e acesso a internet, neutralidade da rede, privacidade para pessoas, transparências para os governos, códigos aberto e livre circulação de informação. Esses pontos são comuns aos partidos piratas ao redor do mundo, mesclados com cores regionais como no caso brasileiro em sua atuação no debate sobre o Marco Civil.

3.3.2 Actantes

Em seu site (http://actantes.org.br/), a organização Actantes se define como "um coletivo que organiza ações diretas pela comunicação livre nas redes digitais". A organização se posiciona contra a Sociedade de Controle e a Biopolítica da Modulação atuando no debate fornecendo subsídios técnicos e teóricos para a conscientização dos usuários da rede. Teoricamente, o enfrentamento de tais temas remete a autores como Foucault, Deleuze, Negri e Hardt.

Em seu Manifesto, a Actantes afirma: "lutamos pela privacidade e pela navegação anônima; combatemos a informática de dominação; defendemos o direito das pessoas de compartilharem livremente o conhecimento e os bens culturais" (ACTANTES, online). Esses são os principais pontos de defesa e atuação do grupo. Para atingir tais objetivos, o grupo se baseia na ideia de ambivalência tecnológica, discutida por Galloway (2004): "Tecnologias são criadas e utilizadas para divertir e para oprimir, mas também para salvar e para libertar. Por isso, exploramos sua ambivalência e toda a dimensão ideológica dos plugins, dos protocolos e dos softwares" (ACTANTES, online).

A partir da ambivalência das tecnologias cibernéticas, isto é, da possibilidade de apropriação, reconfiguração e recombinação de tais tecnologias em prol de outros objetivos, as atividades da Actantes podem ser divididas em duas frentes: ação direta e educativa. Em relação às ações diretas, o site da organização não é claro quanto ao seu modo e repertório de ação, por razões óbvias devida a ambiguidade legal que essas ações podem incorrer. A

Actantes apenas afirma: “Somos um coletivo que organiza ações diretas pela comunicação livre nas redes digitais. (...) Somos actantes e organizamos ações diretas (ACTANTES, online)”. No entanto, em relação a sua atuação educacional, agindo como um polo disseminador de conhecimentos técnico-políticos e de debates, a organização apresenta claramente seus cursos e palestras para a sociedade em geral. Dentre os cursos oferecidos pela organização estão: Lógica de programação com Python; Administração Sistema Operacional Linux; proteção de dados – básico 1. Todos voltados para o desenvolvimento de habilidades e ferramentas em software livre e proteção de dados e privacidade. Além dos cursos presenciais na sede da organização, em São Paulo, há uma série de tutoriais para os interessados nos temas: Cultura de Segurança no sistema Debian; TextSecure 2.0.3; IMAP e POP3 – Características; Criptografia Simétrica e Assimétrica; ChatSecure - Instalação e Configuração. Os tutorais são diretamente relacionados ao uso correto de ferramentas para a privacidade online.

A Actantes também está engajada em campanhas online pelo direito ao livre conhecimento e à privacidade. Em seu site, a organização lista as principais campanhas que participa: Um Lar para Snowden; “Necessária e Proporcional”: Pelo fim da vigilância em massa; campanha pelo Marco Civil da Internet. Além disso, diversas palestras são organizadas com a ideia de chamar a atenção para os temas e fomentar o debate, entre elas: “CRIPTOPOLÍTICA: Discutindo a Sociedade de Controle em tempos de vigilância em massa”; “Cryptowars: Backdoors obrigatórios e retenção de dados” (em parceria com a Saravá). Por fim, a Actantes lista suas principais hashtags: #AaronSwartz #EFF #InternetsOwnBoy #BandaLargaEUmDireito #DialogosConectados #Presidenciaveis #ConflitoIsraelPalestina #Wikileaks #DialogosConectados #CampanhaBandaLarga #MarinaSilva #EFF #Hackers #OpenWirelessMovement.

3.3.3 Saravá

O Grupo Saravá é um dos coletivos de ativistas mais bem organizado e mais atuante no Brasil. Em seu site, o grupo afirma que se insere em um contexto “no qual o conhecimento técnico se faz fundamental para o avanço da sociedade na sua busca por justiça social (SARAVÁ, online)”. Partido desse princípio, a ação coletiva e a perspectiva de mudança social passam necessariamente pelo domínio e apropriação da linguagem e do funcionamento

de aparatos tecnológicos. Seguindo essa premissa, o Grupo Saravá desenvolve atividades educativas e de apoio a diversos movimentos sociais. Por isso, segundo o grupo, sua missão é:

> Prover instrumentos tecnológicos para movimentos sociais e para a sociedade em geral, além de pesquisar e desenvolver ferramentas, instrumentos, protocolos, documentações, softwares, serviços e oficinas que possibilitem a replicação da iniciativa do Grupo por outros grupos e pessoas, tendo cuidado para evitar a apropriação capitalista dessas inovações. (SARAVÁ, online)

Dessa forma, o grupo se dedica a fornecer a infraestrutura necessária para a atuação de movimentos sociais progressistas, tanto para comunicação quanto para a hospedagem e distribuição de conteúdos. Nesse sentido, o Saravá divide sua atuação em três eixos: 1) Estudo, pesquisa, desenvolvimento, experimentação e sistematização de atividades; 2) Operação e manutenção das atividades; 3) Replicação da atividade, de modo a compartilhar os desenvolvimentos com a sociedade.

A atuação do Grupo Saravá segue um "Conjunto de Princípios Ético", documento elaborado coletivamente em um fórum sobre "Cultura livre e Capitalismo". Os princípios éticos são debatidos em um total de vinte e três tópicos. Os tópicos falam sobre: 0) a mobilidade dos princípios; 1) a autonomia; 2) a apropriação pública; 3) o licenciamento; 4) o acesso público; 5) a diversidade; 6) a gestão; 7) as invenções; 8) as pesquisas e as metodologias; 9) a expansão e a organização em redes; 10) as doações; 11) a auto-sustentabilidade; 12) a gestão financeira; 13) a privacidade; 14) a espetacularização; 15) a sociedade livre; 16) a garantia de expressão; 17) a distinção entre produtor/a e consumidor/a; 18) a transformação da sociedade; 19) a união; 20) a intolerância; 21) a remuneração pelo trabalho; 22) a capitalização sobre trabalho. Ressalta-se que essa não é uma carta fechada, mas sim uma série de sugestões de posicionamentos que tem guiados os signatários. Por essa razão, salienta-se o princípio 0, isto é, a possibilidade de mudança ou mesmo abandono de alguns princípios caso eles não mais sejam expressões da ação coletiva. Dentre os principais pontos, destaca-se a autonomia dos movimentos de mídia livre, sua cultura de apropriação e compartilhamento; diversidade e a inclusão de pontos de vistas diversos; a recusa do financiamento público ou privado; transparência dos processos internos e defesa da privacidade individual.

Quanto ao seu modus operandi, o Grupo Saravá deixa claro que a participação no grupo atende a critérios políticos como confiança, engajamento, responsabilidade e comprometimento. Da mesma forma, o tamanho do grupo deve ser suficiente, mas limitado a

certo número como forma de garantir agilidade e eficiência. Sua relação externa é guiada para colaborar com outros grupos, ativistas e coletivos, porém afirmam: “O Grupo desenvolve atividades públicas, porém é um grupo fechado uma vez serve como fiel depositário de informações e dados pessoais sensíveis de terceiros, além da segurança de sua infraestrutura (SARAVÁ, online)”. Ainda ressaltam sua posição no que eles denominam “ecossistema de grupos”:

> O Grupo não deve se tornar um elemento central na articulação entre movimentos sociais, uma vez que a centralização cria um ponto de falha evidente. Ao contrário, ele deve ter um tamanho razoável e encorajar que outros grupos surjam para que haja distribuição de esforços, redundância e resiliência. Deve também encorajar a troca de recursos entre tais grupos (SARAVÁ, online).

Assim, o Grupo Saravá se concentra em fornecer subsídios técnicos para a ação de outros grupos. Para isso, oferece um serviço de hospedagem de projetos. Em sua “Carta de Hospedagem do Saravá” algumas de suas posições políticas ficam mais evidentes. Segundo o documento, o grupo é “parte de uma intersecção de vários grupos que discutem política e tecnologia de diferentes formas” (SARAVÁ, online). Nesse sentido, a hospedagem de projetos funciona como uma tentativa de construir uma vizinhança ou um rizoma. Por esse motivo, reafirma: “Sendo a tecnologia também uma construção social, seus propósitos, sua configuração e os processos nos quais ela interfere não podem prescindir dos desígnios dos grupos sociais onde ela é manipulada (SARAVÁ, online)”.

A ideia de construção social também se aplica a internet, por isso o grupo declara:

> A internet é um ambiente de cooperação, mas também de apropriação e exploração de bens públicos. Nós entendemos que ela só se torna essencialmente um espaço público na medida em que as pessoas possam controlar seus meios de produção e de acesso, o que não ocorre em espaços corporativos ou governamentais. Por isso buscamos a criação de espaços públicos, não corporativos e não estatais, e esperamos que os grupos por nós hospedados colaborem com a construção desses espaços. Durante a construção de tais espaços, realizamos discussões nas quais tentamos desvendar temas como cultura, sociedade, tecnologia, ativismo, mudanças sociais entre outros. Tais estudos, quando possível, são disponibilizados publicamente. Estudamos as implicações políticas da técnica, desenvolvemos sistemas e instrumentos a partir de outros valores políticos, além de dialogarmos politicamente dentro da lógica cíclica da teoria/prática. (SARAVÁ, online).

Com sua postura de se manter como colaborador no ecossistema ativista, o Saravá se envolve na realização de alguns cursos, palestras e eventos. Os principais são a CryptoRave e a CryptoParty, ou ainda, palestras em conjunto com a Actantes e a Eletronic Frontier

Foundation como: “Cryptowars: Backdoors obrigatórios e retenção de dados”. Além disso, o grupo enfrentou problemas com o Ministério Público, chegando a ter seus servidores apreendidos devido a um processo contra a Rádio Muda – a mais antiga rádio livre em operação no país.

3.3.4 Escola de Ativismo

A Escola de Ativismo, devido a sua cooperação com as outras organizações citadas, surge, também, como um coletivo que se destaca na resistência cibernética. Como o próprio nome sugere, o grupo busca se pautar em processos pedagógicos e de construção coletiva de ferramentas e tecnologias sociais que possam fomentar, viabilizar e fortalecer lutas sociais diversas. Nesse sentido, a Escola de Ativismo, em seu website, declara que sua missão é “fortalecer o ativismo no Brasil por meio de processos de aprendizagem voltados para potencializar os grupos e as ações que trabalham pela democracia, combate a todas as formas de injustiças, defesa dos direitos humanos e da sustentabilidade ambiental (ATIVISMO, online)”.

O coletivo atua organizando encontros, palestras e cursos para movimentos sociais e de resistência. Em sua página oficial é possível encontrar as últimas atividades da Escola de Ativismo: “Semeando Ativismo: seminário de comunicação para o Ativismo”; “Oficina de Memes”; “Primaveras: diálogos sobre ativismo, democracia e sustentabilidade”; “Oficina de Comunicação Digital para o Ativismo”; “The Yes Lab: Oficina de ação criativa”. Tais atividades mantém o caráter educativo. Por outro lado, o grupo realiza uma pesquisa intitulada “Ativismo no Contexto Urbano”, na qual busca compreender o campo de atuação de organizações, coletivos e movimentos que trabalham nos temas de mobilidade/transporte, resíduos sólidos e infraestrutura em 12 cidades brasileiras: São Paulo, Rio de Janeiro, Salvador, Brasília, Belo Horizonte, Belém, Curitiba, Fortaleza, Manaus, Porto Alegre, Recife e São Luís. No entanto, ainda não estão disponíveis os dados e os resultados da pesquisa. Além disso, a Escola de Ativismo é uma das idealizadoras e organizadoras dos dois principais eventos sobre privacidade e internet no Brasil: a Cryptoparty e a Cryptorave.

3.3.5 Anonymous Brasil

Ao adotar como símbolo a máscara inspirada em Guy Fawkes, da graphic novel de Alan Moore “V de Vingança”, o grupo autointitulado Anonymous deu um rosto ao

hackerativismo nos últimos anos, em especial na cobertura de suas ações por parte das mídias tradicionais. O grupo surgido em fóruns de discussão tem sido objeto de diversos trabalhos que buscam entender sua origem, metodologia e impacto político. Dentre tais pesquisas, destaca-se o da antropóloga Gabriella Coleman, pesquisadora da cultura hacker, com os trabalhos "Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous" (COLEMAN, 2014) e "Anonymous in Context: The Politics and Power behind the Mask" (COLEMAN, 2013). A obra "Nós Somos Anonymous", de Parmy Olson (2013), também tenta compreender o universo particular do grupo. No Brasil, destaca-se a dissertação de mestrado apresentada por Murilo Bansi Machado, na Universidade Federal do ABC, "Por dentro do Anonymous Brasil: poder e resistência na Sociedade de Controle".

De todos os grupos, coletivos e organizações aqui enumerados, o Anonymous é o mais disperso e difícil de apreender. Isto é, sua organização baseada em uma "legião" de hackerativistas dispostos a colaborar em suas "operações" é um desafio metodológico para as ciências sócias, uma vez que o anonimato e, ao mesmo tempo, um senso de humor sarcástico dificultam o contato com fontes confiáveis e informações sobre o grupo.

Autores como Olson (2013) apontam para a origem do grupo no fórum 4chan[35], um site de compartilhamento de imagens conhecido por postagens com conteúdo explícito e, muitas vezes, grotesco e agressivo. A possibilidade de participar do fórum sem a necessidade de criação de um perfil, isto é, de forma anônima, favoreceu o desenvolvimento de um ambiente anárquico e com linguagem e moral própria. A estética e o humor dos participantes dos tópicos do fórum, em especial o chamado "/b/ board" dedicado a temas aleatórios, foi fundamental na formação do que posteriormente ficou conhecido como Anonymous.

A autora Gabriella Coleman (2013), uma das principais pesquisadoras do grupo, divide a evolução do grupo em duas partes. A primeira, entre 2005 e 2010, representa a formação do grupo e suas primeiras ações de trolling[36] até o chamado ativismo irreverente, com ações mais displicentes e baseadas no senso de humor próprio do grupo. A segunda, entre 2010 e 2012, cobre a explosão da ação direta digital, com diversas operações e ataques coordenados a organizações e Estados. Coleman aponta para as principais características do

[35] http://www.4chan.org/. Em sua descrição o site declara: 4chan is a simple image-based bulletin board where anyone can post comments and share images. There are boards dedicated to a variety of topics, from Japanese animation and culture to videogames, music, and photography. Users do not need to register an account before participating in the community.

[36] Na gíria do grupo, trolling se refere a uma série de ações visando irritar ou desestabilizar o alvo. Estas podem ser postagens, piadas, gozações, cyberbulling, montagens, comentários.

grupo que garantem sua eficiência: “its ability to land media attention, its bold and recognizable aesthetics, its participatory openness, the misinformation that surrounds it and, in particular, its unpredictability”. (COLEMAN, 2013, p. 2). Porém, por outro lado, o grupo constituído basicamente por jovens ao redor do mundo não dispõe de material humano e recursos financeiros necessários para causar danos maiores, como no caso de um conflito cibernético entre dois Estados.

Devido ao caráter anárquico e aberto a participação do grupo, logo surgiram perfis se autodenominando Anonymous Brasil. Os chamados Anonymous Brasil não possuem website ou perfis em redes sociais oficiais. Justamente por isso, é possível encontrar diversos sites e páginas que se declaram Anonymous e funcionam como uma rede para agregar simpatizantes e divulgar notícias e operações. Suas diretrizes básicas e conteúdos são diretamente ligados às declarações, notícias e operações do Anonymous internacional. O grupo declara:

> Nós não somos uma organização e não temos líderes. Oficialmente nós não existimos e não queremos existir oficialmente. Nós não seguimos partidos políticos, orientações religiosas, interesses econômicos e nem ideologias de quaisquer espécies. Mais uma vez: Anonymous não tem líderes. Se alguém lhe disser que representa ou lidera Anonymous, este alguém não conhece a ideia Anonymous, porque nós não podemos ser representados ou liderados, porque isto é o que somos: uma ideia. (...) No Brasil, estamos agora nos expandindo e queremos convidá-lo a juntar-se a nós, anonimamente. Preservando o anonimato, poderemos agir contra a corrupção com mais eficácia, sem perseguição. Não esperamos que você acredite neste texto. Pedimos apenas que você se informe e procure as informações por você mesmo sem interferências midiáticas. Veja com seus próprios olhos os fatos que estão acontecendo no mundo e na sua própria cidade. Vamos todos juntos à favor do Brasil, contra a corrupção! (ANONYMOUS BRASIL, online).

Percebe-se uma influência direta dos textos do Anonymous internacional e uma rápida adaptação ao cenário brasileiro. Machado (2013) afirma que o grupo passou a agir mais intensamente no Brasil a partir da #OpPayBack, deflagrada contra as instituições financeiras que bloqueavam as doações ao Wikileaks (Mastercard, PayPal e Amazon). Durante essa operação foram criados canais de comunicação para os Anonymous brasileiros se organizarem. Desde então, o coletivo nacional apoiou e recebeu apoio do Anonymous internacional e ainda deflagrou operações em nível local.

As duas principais operações do Anonymous Brasil, segundo Machado (2013), foram a #OpWeeksPayment e a #OpGlobo. A primeira visava “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” (MACHADO, 2013, p.

7). Já a segunda operação, atacou diversos sites das Organizações Globo (TV Globo, Editora Globo, Fundação Roberto Marinho, etc.), vinculando mensagens contra a organização, como por exemplo: “Você está sendo manipulado”; “O povo não é bobo”.

Por esse motivo, o ramo brasileiro do Anonymous demonstra capacidade de organização e operação nos mesmos moldes do Anonymous internacional. Da mesma forma, está conectado a essa rede global de hackerativistas e participa de debates e operações em todo o mundo. Por esse motivo, o grupo pode ser considerado, também, um dos grupos de resistência cibernética no Brasil.

3.3.6 Cryptoparty e Cryptorave

A Cryptoparty e a Cryptorave são, diferentemente dos grupos citados até agora, eventos organizados por ativistas. Isto é, acontecem com dia, hora e local marcado e reúne diversos ativistas e grupos. Tais eventos buscam apresentar o debate ao grande público e divulgar ferramentas e tecnologias de resistência ao controle cibernético. Em 2013 e 2014, foram realizadas diversas Cryptoparties pelo Brasil e uma Cryptorave em São Paulo.

A Cryptoparty é uma iniciativa global de divulgação de métodos de criptografia e comunicação segura na internet. Em seu site internacional, o evento se define como: “a decentralized, global initiative to introduce the most basic cryptography software and the fundamental concepts of their operation to the general public, such as the Tor anonymity network, public key encryption (PGP/GPG), and OTR (Off The Record messaging)” (CRYPTOPARTY, online). Uma Cryptoparty segue alguns princípios fundamentais: livre participação; aberta ao público; não alinhada politica ou comercialmente; totalmente contra assédio e/ou discriminação de gênero, orientação sexual, aparência, raça, religião e habilidade técnica. Além disso, os participantes são encorajados a desenvolverem suas próprias atividades e colaborarem no aprendizado coletivo.

A Cryptorave teve sua primeira edição em abril de 2014, em São Paulo. O evento manteve o conteúdo e os princípios de uma Cryptoparty, porém com uma extensão muito maior. A Cryptorave durou 24h e reuniu diversas palestras, oficinas, debates, treinamentos e atividades artísticas. Segundo declarações da organização[37], a Cryptorave brasileira o maior evento sobre criptografia, privacidade e política com maior público. A programação ofereceu, dentre outras atividades, as seguintes palestras: “Cyberguerra e a militarização da internet”;

[37] https://cryptorave.org/

“Snowden, NSA e o fim da privacidade”; “As baixas da luta pela liberdade na rede”; “Criptomoedas”; “Saiba como da maior prejuízo à NSA”; “A quem interessa a guarda de logs”; “Princípios para a governança global da internet”; “Segurança, vigilantismo e soberania: o caso da Ucrânia”. De maneira geral, o leitmotiv dos debates foi a extensão de um programa global de violação da privacidade e liberdade na internet e, como consequência, as formas individuais e coletivas de resistência cibernética.

Diversas organizações, coletivos e ativistas (Actantes, Escola de Ativismo, Saravá) colaboraram para a realização das diversas cryptoparties e da Cryptorave. Esse fato reforça a importância de tais eventos como ponto de divulgação, troca de experiências e aprendizado coletivo, funcionando como uma espécie de Hub para os ativistas da privacidade e liberdade da internet. Além disso, seu princípio de abertura ao pública para a divulgação do debate político e do aprendizado de técnicas básicas de criptografia constituem uma interface fundamental na relação entre os ativistas e o grande público.

3.3.7 Oficina Antigilância

A Oficina Antivigilância constitui outro ponto importante no ecossistema de ativistas da privacidade e liberdade na internet. A inciativa foi criada visando: “ser um espaço de discussão sobre as garantias ao direito à privacidade na rede. Em pauta, as ferramentas e tecnologias que visam proteger os usuários, debates sobre legislação e o contexto político internacional, envolvendo governos, setor privado e sociedade civil” (ANTIVIGILÂNCIA, online). Dessa forma, os interessados podem acompanhar seus “Boletins Antivigilância”, participar das listas de discussões e ter acesso a conteúdos, referências e materiais para a organização de oficinas presenciais.

O “Boletim Antigilância” é publicado desde novembro de 2013, passando a ser trimestral em 2014. Com dez edições postadas na rede, o Boletim Antigilância traz uma coletânea de artigos, notícias e comentários sobre os principais acontecimentos políticos e tecnológicos relacionados à privacidade e liberdade na internet. Sendo assim, pode ser considerado um dos principais canais de discussão e divulgação do debate sobre privacidade e internet.

3.4 ANALISANDO A RESISTÊNCIA CIBERNÉTICA NO BRASIL: PONTOS EM COMUM

O ativismo na internet assume diversas formas e absorve um repertório abrangente e heterogêneo. Devido à natureza global da internet, isso não é exclusividade do caso brasileiro. De maneira geral, os ativistas trocam experiências, compartilham resultados e imitam técnicas e ações ao redor do mundo. Cabe ressaltar que, embora não seja o foco desse presente trabalho, fatores culturais e regionais podem afetar essas ações, como os hackers ligados ao fundamentalismo islâmico ou ao governo norte-coreano. Nesse sentido, por que discutir o ativismo cibernético no Brasil?

Nos últimos anos, o acesso à internet a e popularização das novas tecnologias da informação deram um salto quantitativo no Brasil. Dados Banco Mundial[38] e da União Internacional de Telecomunicações[39] demonstram esse avanço por meio de uma série histórica da porcentagem de usuários.

Tabela 1 – Porcentagem da população brasileira com acesso a internet.

Ano	Porcentagem da população com acesso a internet (%)
2000	2,87
2001	4,53
2002	9,15
2003	13,21
2004	19,07
2005	21,02
2006	28,18
2007	30,88
2008	33,83
2009	39,22
2010	40,65
2011	45,69
2012	48,56
2013	51,60

Fonte: International Telecommunication Union (adaptado).

Nesse contexto, os debates sobre crimes virtuais privacidade e segurança na internet vêm acompanhando esse processo. Por um lado, os crimes cibernéticos se inserem uma

[38] http://data.worldbank.org/indicator/IT.NET.USER.P2?order=wbapi_data_value_2013+wbapi_data_value+wbapi_data_value-last&sort=desc (acesso em 13/10/2015)

[39] http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx (acesso em 13/10/2014).

categoria jurídica e a ampliação do debate aponta para uma atualização dos mecanismos legais para a proteção dos indivíduos frente delitos cometidos no meio virtual. Por outro lado, ainda que possa ser vinculado a questões criminais, o debate sobre privacidade na rede tem se politizado cada vez mais. A hipótese para isso é o fato de que, enquanto questões criminais indivíduos ou grupos causam danos a terceiros, a relação entre Estado, grandes corporações da internet e indivíduos é assimétrica.

A assimetria da relação fica evidente nos principais vazamentos de informações dos últimos anos: Wikileaks e Edward Snowden. A capacidade dos governos de interceptarem comunicações privadas e dados pessoais e, por outro lado, o lucrativo mercado de dados de compras e preferências por parte de empresas, demonstram a fragilidade e, muitas vezes, o desconhecimento dos indivíduos da sua real condição enquanto usuário. Tal questão conduz a uma intensificação do debate em duas frentes, segundo Silveira (2009a) política da internet e política na internet. A política da internet gira em torno dos temas da gestão da rede, das políticas de privacidade e segurança, da legislação que afeta empresas prestadoras de serviços e indivíduos, políticas públicas de popularização de acesso, etc. Já a política na internet reflete os debates e a ações de grupos diversos que usam a internet como plataforma política, tanto como uma interface real-virtual quanto como atividade exclusiva na rede.

O impacto das denuncias de espionagem em 2013 ficaram evidentes na agenda oficial do governo brasileiro: cancelamento da visita oficial da presidenta Dilma Rousseff aos Estados Unidos; inciativa brasileira e alemã nas Nações Unidas para garantir os direitos online; esforço do governo para a aprovação do Marco Civil da internet como forma de demonstrar sua preocupação com tema. Tais temas merecem serem estudados e abrem uma nova agenda de pesquisa sobre o uso da internet como instrumento estratégico de política externa. No entanto, o foco dessa pesquisa é a outra ponta do processo: os grupos de resistência. Da mesma forma, as denúncias de espionagem e violações de privacidade deram mais fôlego e impulsionaram o debate de tais grupos, conseguindo até superar ser círculos tradicionais mais fechados.

Se, por um lado, é possível avaliar governos e políticas públicas a partir de documentos oficiais, discursos e indicadores quantitativos; por outro, a criação de dados sobre a ação dos grupos de resistência encontra diversas dificuldades. Devido às escolhas de abordagem da presente pesquisa, isto é, para cartografar o ativismo sobre privacidade na internet, é necessário identificar os principais atores e descrever seus métodos e discurso. Isso

não se constitui uma etnografia ou uma análise de discurso, metodologias com técnica e rigor científico próprio. Ao descrever os grupos e os principais pontos de seu discurso e ação o que se intenta é encontrar os pontos em comum que possam orientar a construção de uma cartografia das redes. Mapear as discussões e seu impacto em um público mais amplo a partir de conceitos-chave que norteiam a ação.

Partido desse pressuposto, os grupos aqui elencados foram identificados como os principais atores no ciberativismo brasileiro. Devido à própria natureza de tais grupos comprometidos com o anonimato e privacidade, alguns atores relevantes podem ter sido deixados de fora. Para identificar tais grupos, realizou-se uma busca pelas principais publicações sobre o tema. Graças à estrutura em rede e a cooperação entre os principais atores foi possível identificar outros atores a partir de publicações compartilhadas e eventos em comum.

Dessa forma, fica evidente o leitmotiv comum a todos os atores: privacidade, anonimato e criptografia. Os grupos diferem em sua forma de ação, desde o debate na esfera pública interconectada, objetivando a conscientização e divulgação da causa; passando por ações pedagógicas, visando municiar indivíduos interessados em no assunto a ir além do debate; até, por fim, algumas ações diretas contra alvos estratégicos com a intenção de chamar a atenção para a causa e demonstrar capacidade e poder por parte de grupos de resistência. Portanto, uma cartografia do ativismo cypherpunks no Brasil deve partir dessa tríade de conceitos.

O que se buscou nesse capítulo foi apresentar uma pequena construção do conceito de privacidade e seus mecanismos de proteção legal. Em seguida, uma breve discussão sobre o conceito de “exceção” em Agamben, para demonstrar como a suspensão de direitos é uma técnica de governo contemporânea e, por esse motivo, a resistência, muitas vezes, deve se articular para além de uma busca pela criação e defesa de direitos no plano institucional. A partir disso, buscou-se apresentar os principais grupos brasileiros que atuam nesse sentido. Para isso, optou-se pela descrição das ações e declarações dos atores a partir de suas publicações originais. Tal procedimento visava identificar os pontos em comum entre os grupos elencados. Com essa identificação é possível avançar para o debate metodológico e a análise de dados. Isto, a construção de parâmetros de pesquisa e sua aplicação. Dessa forma, dedica-se o próximo capítulo a uma discussão sobre a pesquisa na internet, o uso de

ferramentas e softwares, a construção de parâmetros de buscas e a elaboração de visualizações das redes. Tudo isso com o objetivo de cartografar a rede de ativistas cypherpunks brasileiros.

4 CARTOGRAFIA DAS REDES

4.1 PESQUISA NA INTERNET

A popularização da internet, a partir dos anos 1990, trouxe consigo um avanço do interesse acadêmico sobre as novas possibilidades de interações sociais, culturais e políticas. Diversas pesquisas passaram a se debruçar sobre o fenômeno em busca de compreender suas diversas facetas e desdobramentos. Para isso, no entanto, foi necessário enfrentar os desafios metodológicos para a apreensão e interpretação de um novo ambiente, com dinâmica e estrutura própria.

O volume de dados, informações e conteúdos produzidos diariamente na internet é praticamente impossível de ser apreendido em sua totalidade. Nesse sentido, a pesquisa social na internet se depara com um problema comum a pesquisa social "off-line": a questão da escala. Isto é, o pesquisador, consciente das limitações da representação social e por questões pragmáticas, deve realizar um recorte da realidade de modo a tornar sua investigação possível. Nesse sentido, o problema a ser respondido deve conduzir a um desenho de pesquisa que compreenda essa limitação e identifique o recorte correto a ser utilizado.

A complexidade dos fenômenos online adiciona uma dimensão que deve ser considerada pelo pesquisador: "A internet pode ser tanto objeto de pesquisa (aquilo que se estuda), quanto local de pesquisa (ambiente onde a pesquisa é realizada) e, ainda, instrumento de pesquisa (por exemplo, ferramenta para a coleta de dados sobre um dado tema ou assunto)" (FRAGOSO, RECUERO & AMARAL, 2010, p. 17). Tais possibilidades devem ser cuidadosamente conduzidas pelo pesquisador a fim de obter os melhores resultados e não comprometer seu trabalho.

Da mesma forma, a abordagem da internet deve ser cuidadosa com o objetivo de evitar falácias e ou armadilhas teórico-metodológicas. Em primeiro lugar, é preciso ter claro a diferença entre internet como cultura e como artefato cultural. A primeira definição implica em um debate sobre o comportamento dos usuários, a formação de grupos e comunidades, identidade online. Por outro lado, a ideia de artefato cultural reforça a observação da relação da tecnologia com a vida cotidiana, demonstra que a internet se conecta com um elemento da

cultura e não um universo a parte. Essa perspectiva permite uma melhor articulação entre as fronteiras online e off-line demonstrando a fluidez de suas interfaces.

> No caso da pesquisa sobre a internet, a própria definição temática carrega o pesa de uma falácia que é preciso ter em mente todo o tempo: ao especificar a internet como universo de observação, implicitamente damos abrigo à ideia de uma ruptura entre o que está ou acontece "dentro da rede e o mundo "fora" dela. A literatura sobre o tema está repleta de afirmações que partem desse equívoco, que na maior parte das vezes passa desapercebido. (FRAGOSO, RECUERO & AMARAL, 2010, p. 54).

Nesse sentido, a pesquisa empírica na internet enfrenta um desafio ainda maior: a construção de amostras e análise dos dados. Se por um lado, autores se dedicam a teorizar o papel da internet e os desdobramentos filosóficos da interação homem-máquina; por outro, os pesquisadores devem desenvolver metodologias e técnicas confiáveis a fim de comprovar ou refutar ideias sobre a internet. Por ser, ao mesmo tempo, objeto, local e instrumento de pesquisa, a internet oferece desafios próprios e dinâmicos aos pesquisadores.

O que se buscou até aqui na presente pesquisa foi demonstrar teoricamente como: i) as tecnologias são construções sociais e, por isso, indivíduos ou grupos podem lhes dar um novo sentido e utilidade; ii) o ativismo político passou a utilizar a tecnologia como ferramenta de ação; iii) a crescente militarização do ciberespaço, considerado pelo doutrina militar como uma fronteira não-pacificada; iv) como o ativismo da internet passa a operar, ainda que não se desconecte das pautas off-line, em uma dinâmica própria; v) a forma que grupos ativistas levam seus discursos e ações para além da ideia de uma Esfera Pública Interconectada, isto é, optando por ações diretas virtuais; vi) como que, a partir de uma ideia de suspensão de direitos, a resistência online passar a operar em duas frentes, uma discursiva, denunciando as violações de direitos online, e outra prática, criando e divulgando ferramentas para os cidadãos enfrentarem tais violações. Esses pontos destacados, apresentados aqui de forma breve e grosseira, conduziram a pesquisa à busca de dados empíricos sobre o fenômeno. Dessa forma, é imperativo discutir dois pontos centrais na pesquisa empírica: sua justificativa e sua operacionalização.

Desde o início das pesquisas sociais sobre internet, diversos métodos foram discutidos, adaptados e criados para tentar abarcar a complexidades dos fenômenos e sua natureza específica. Cada metodologia busca se adequar ao objeto estudado, dentre as principais pode-se citar alguns exemplos: análise de conteúdo, análise de discurso, etnografia, estudo de caso (para objetos como blogs); análise de hyperlinks, análise de websfera e webometria (para

páginas pessoais e websites); etnografia, entrevista em profundidade e análise documental (para portais); interacionismo simbólico e semiótica (para mundos virtuais); survey e observação participante (para fóruns de discussão); análise de redes sociais, grupo focal on-line e análise de conversação (para redes sociais) (FRAGOSO, RECUERO & AMARAL, 2010, p. 49).

Para analisar o impacto do ativismo cypherpunk no Brasil algumas dificuldades devem ser enfrentadas. Em primeiro lugar, o potencial horizontal de uma rede, discutido no capítulo I a partir da obra de Alexander Galloway (2004), reside em arranjos novos que escapam ao domínio vertical e hierárquico da arquitetura da internet. Os grupos ativistas podem se articular de diversas maneiras que escapam das possibilidades convencionais de busca e obtenção de dados. Em segundo lugar, conforme define Samuel (2004), grupos hackerativistas, muitas vezes, se situam em um terreno legalmente ambíguo ou, até mesmo, ilegal. Por essa razão, aliada as características próprias da cultura hacker e, em alguns casos, um senso de humor próprio carregado de ironia e sarcasmo, algumas abordagens como entrevistas em profundidade e etnografias podem demandar muito tempo e talento do pesquisador para conseguir fontes seguras e, ainda mais, a confiança dos ativistas. Tais características devem ser consideradas juntamente com a disponibilidade de tempo e recursos para a realização da pesquisa.

Conforme discutido anteriormente, a ação dos principais grupos levantados no Brasil pode ser dividida em duas frentes: uma discursiva e outra prática. No plano dos discursos, os ativistas se organizam em torno do debate sobre sua agenda nas redes sociais e em seus próprios websites. O objetivo é produzir informações para além da mídia tradicional, difundir suas bandeiras e conscientizar a usuários da internet e a população em geral sobre tais temas. No plano prático, desenvolvem e adaptam tecnologias antivigilância e difundem seu uso por meio de treinamentos e tutoriais. Dessa forma, a presente pesquisa poderia se concentrar em um dos aspectos e, por exemplo, realizar uma análise de discurso ou uma etnografia. No entanto, recentemente, uma nova metodologia está conseguindo oferecer novos olhares sobre determinados objetos de pesquisa na internet: a cartografia virtual ou cartografia das controvérsias.

A cartografia, em seu sentido original, é a ciência da construção de mapas e cartas cartográficas. Desde sempre, uma área ligada umbilicalmente à geografia, mas que, principalmente após os trabalhos de Deleuze e Guattari, vem sendo utilizada de formas

diversas em outras áreas do conhecimento. Na pesquisa na internet, além das discussões filosóficas sobre o potencial rizomático das redes, as técnicas de Data Mining e os mais recentes esforços para a criação de visualizações das redes em mapas complexos e interativos abriram inúmeras possibilidades para a análise dos grandes debates e controvérsias travados na rede. O presente capítulo se dedica a discutir teoricamente a cartografia como ferramenta de pesquisa na internet e na Ciência Política e, em seguida, operacionalizar a obtenção e visualização de dados sobre ativismo cypherpunk no Brasil, apresentando um mapeamento dos ativistas na internet.

4.2 CARTOGRAFIA

A cartografia é, desde sempre, relacionada à confecção de mapas informando o terreno, o relevo, os rios, as vegetações de um determinado espaço. Em sua acepção inicial, cartografia lida com a representação gráfica de espaço um espaço físico e constitui uma parte essencial da Geografia. Além disso, posteriormente dados sobre as diversas sociedades foram sendo adicionados aos mapas, demonstrando as relações entre o espaço e a atividade humana. Dessa maneira, mapas passaram a informar a população, densidade demográfica, índices de desenvolvimento, entre outros. A cartografia se tornou um instrumento importante para as ciências sociais na análise e compreensão das sociedades ao longo do tempo e sua relação de ocupação e domínio do espaço físico.

Porém, a partir de Foucault e, especialmente, de Deleuze e Guatarri a cartografia passa a ter um novo sentido para a pesquisa social. Para além da representação de espaços, a cartografia começa a ser discutida e desenvolvida como um método de apreensão de fenômenos sociais, em especial os de natureza rizomática segundo a definição deleuziana. Sem sistematizar o método, os autores oferecem pistas e indicações de seu desenvolvimento e utilização.

Em primeiro lugar, é a partir dos fragmentos e referências a ideia de uma cartografia social nas obras de Foucault que Deleuze começa a desenvolvê-la. Conforme destacam Kleber Prado Filho e Marcela Montalvão Teti:

> Deleuze refere-se a Foucault como cartógrafo em um texto de 1986, mas já se apresentam elementos cartográficos numa entrevista por ele – Foucault – concedida à revista Hérodote em 1976, tratando da sua relação com o campo da Geografia. Discute-se ali certa "espacialização da história" observável em suas genealogias, bem como a aplicação da arqueologia como cartografia ou geopolítica dos

> discursos3, pistas que se tornam evidentes pelo seu emprego de “metáforas espaciais”, tais como: posição, campo, deslocamento, território, domínio, solo, arquipélago, geopolítica, paisagem, entre outras, dando mostras de uma dimensão espaço-temporal em suas análises. Há também referências à cartografia como método rizomático na “Introdução” de “Mil platôs”, conhecido texto de Deleuze e Guattari, datado de 1980. (PRADO FILHO & TETI, 2013, p. 46).

A metodologia cartográfica, conforme proposta pelos autores, não se constitui um conjunto de regras ou um modelo a ser aplicado. Pelo contrário, o objeto de pesquisa, inserido em seu próprio contexto, demanda uma abordagem específica, pois nesse contexto, objeto e método se complementam. Sendo assim, a metodologia deve ser uma estratégia flexível de análise crítica. No Brasil, o debate sobre o método cartográfico surge nos esforços de Rolnik (1986;1989); de Fonseca&Kirst (2003); de Albuquerque Júnior, Veiga-Neto & Souza Filho (2008); de Passos, Kastrup&Escóssia (2009); entre outros trabalhos. Cada uma dessas abordagens contribui para a ampliação da discussão e aplicação do método sem buscar a unificação e a hierarquização de conjunto de procedimentos, protocolos e orientações.

A cartografia social se dedica, para além da visualização de mapas estáticos, a visualização de movimentos de poder, rotas de fuga, resistências e práticas libertárias. Trata-se de apresentar diagramas de poder, demonstrando as linhas de enfrentamento e suas resistências. Os diagramas de poder podem dar visibilidade a fenômenos capilares, de natureza rizomática, ou ainda, na definição deleuziana, micropolíticos. Prado Filho e Teti (2013) destacam que a cartografia opera em nível rizomático, isto é, a partir do conceito de Deleuze e Guattari de rizoma.

Na introdução de “Mil Platôs” (2011), os autores começam a estabelecer a relação entre cartografia e o rizoma. Se por um lado, a árvore-raiz é unitária, disciplinar e vertical, por outro, o rizoma opera de maneira contrária: difuso, horizontal, múltiplo. A ideia de rizoma, e o próprio termo, são tomados da botânica, isto é, uma formação radicular como a da grama e da batata. Tal metáfora remete a possibilidade de capilaridades infinitas se expandindo horizontalmente sem um centro disciplinador para orientá-las. Mais ainda, o rizoma não é soma de unidades, mas de dimensões múltiplas e simultâneas, um rede em constante mutação que inova conectando novos pontos. Da mesma forma que o rizoma botânico, o rizoma de Deleuze e Guattari guarda sua característica subterrânea, o que dificulta, ou mesmo impede, a sua imediata visualização e compreensão de suas intricadas redes.

Para tentar clarificar a compreensão de um conceito abstrato como o rizoma, os autores apresentam suas principais características aproximativas. São eles: 1° e 2°: Princípios de conexão e de heterogeneidade; 3°: Princípio de multiplicidade; 4°: Princípio de ruptura assignificante; 5° e 6°: Princípio de cartografia e decalcomania. Esses princípios norteiam a denominação de um rizoma, mas, devido a sua própria natureza, não encerram as possibilidade de ressignificação e novas configurações semânticas.

Os dois primeiros princípios afirmam que "qualquer ponto de um rizoma pode ser conectado a qualquer outro e deve sê-lo" (DELEUZE & GUATTARI, 2011, p. 22). O rizoma é o oposto do modelo de árvore-raiz, no qual os pontos se ordenam e são gerados seguindo uma ordem ou sequência hierárquica. A rede rizomática é aberta a todos os tipos de novas conexões, por mais heterogêneas. O terceiro princípio afirma que "é somente quando o múltiplo é efetivamente tratado como substantivo, multiplicidade, que ele não tem mais nenhuma relação com o uno como sujeito ou como objeto" (DELEUZE & GUATTARI, 2011, p. 23). Essa ideia reforça a renúncia da unidade e do pensamento único em nome da multiplicidade criativa do rizoma. O quarto princípio define que "um rizoma pode ser rompido, quebrado em um lugar qualquer, e também retoma segundo uma ou outra de suas linhas e segundo outras linhas" (DELEUZE & GUATTARI, 2011, p.25). O rizoma, dessa forma, representa tanto suas linhas de segmentariedade quanto as linhas de fugas, que podem a qualquer momento se desdobrar em novas conexões. Os dois últimos princípios, quinto e sexto, tentam demonstrar que o rizoma é avesso a modelos estruturais, mais uma vez hierarquizantes e que visam explicações genealógicas. Tal modelo só pode gerar "decalques" fixos e estáticos, enquanto o rizoma só pode ser visto por meio de uma cartografia que projeta mapas variáveis e dinâmicos.

> O mapa é aberto, é conectável em todas as suas dimensões, desmontável, reversível, suscetível de receber modificações constantemente. Ele pode ser rasgado, revertido, adaptar-se a montagens de qualquer natureza, ser preparado por um indivíduo, um grupo, uma formação social. Pode-se desenhá-lo numa parede, concebê-lo como obra de arte, construí-lo como uma ação política ou como uma meditação. Uma das características mais importantes do rizoma talvez seja a de ter sempre múltiplas entradas; (...) Um mapa tem múltiplas entradas contrariamente ao decalque que sempre volta ao 'mesmo'. (DELEUZE & GUATTARI, 2011, p.30).

Dessa forma, pode-se conceber o rizoma como uma forma de resistência política que busca ressignificar o conceito e o exercício das liberdades ao enfrentar as estruturas políticas e sociais de controle, quase sempre modeladas de acordo com a árvore-raiz. No entanto, novas

formas de controle passam a operar também de maneira difusa e não-hierárquica, isto é, de maneira rizomática. Por esse motivo, Prado Filho e Teti (2003) destacam que:

> os dispositivos, como maquinarias políticas muito mais sutis, "orgânicas" e atualizadas, recusam a racionalidade verticalizada e hierarquizada dos "grandes poderes modernos", adotando também princípios de funcionamento rizomático, exigindo um enfrentamento de igual natureza, conduzido em termos de análise e ações estratégicas visando desemaranhar suas linhas, produzir rupturas, desterritorializações e reverter seus modos de operação (PRADO FILHO & TETI, 2003, p. 53).

O trecho acima demonstra que as formas de controle, por meio dos dispositivos, também podem atuar de maneira rizomática e, por essa razão, o enfrentamento deve ser feito essencialmente por meio do rizoma. Dessa forma, o rizoma, com suas linhas de fuga e resistência, enfrenta ao mesmo tempo a rigidez hierárquica das máquinas político-sociais (Estado, Capital, linguagens) e os dispositivos mais fluidos e dispersos. A partir dessa ideia, pode-se começar a traçar um paralelo entra as redes rizomáticas e as cibernéticas.

Conforme dito anteriormente, a internet apresenta uma tensão em sua arquitetura: um potencial horizontal (rizomático) de infinitas conexões e possibilidades versus uma estrutura vertical (hierárquica) que determina os caminhos, direções e disponibilidade dos fluxos de informação. Alexander Galloway (2004) busca, justamente, em Deleuze e Guattari os elementos para desenvolver essa ideia. A internet funciona, dessa forma, como um simulacro da tensão constante entre a árvore-raiz e o rizoma. Nesse sentido, a resistência cibernética é essencialmente rizomática, seja enfrentando a rigidez dos protocolos verticais criando novas formas de conexão e interação descentralizadas; ou denunciando e criando ferramentas para combater os dispositivos de controle que operam de maneiras difusa e dispersa.

Considerando as características do rizoma apontadas por Deleuze e Guattari, pode-se afirmar que a internet possui um potencial rizomático na sua essência. Em primeiro lugar, qualquer computador pode se conectar, diretamente ou não, a outro (1° e 2° características). Em segundo lugar, o potencial de uma rede distribuída consiste na múltipla capacidade criativa sem a existência de um ponto central, isto é, o múltiplo se torna sujeito em lugar do uno (3° características). Em terceiro lugar, enquanto rede distribuída, isto é, horizontal e sem um ponto central, um ponto de ruptura pode dar início a uma nova rede, novas conexões e possibilidades (4° característica). Por fim, é praticamente impossível demonstrar o funcionamento de uma rede descentralizada por meio de estruturas hierarquizantes. Isto é, se,

por um lado, é possível demonstrar graficamente, de maneira relativamente simples, o funcionamento da estrutura vertical do DNS; por outro lado, o funcionamento dinâmico de uma rede descentralizada escapa as possiblidades de uma imagem fixa ou um decalque.

Essa última característica constitui um dos principais desafios das ciências sociais ao pesquisar a internet. Pois, redes distribuídas podem surgir a qualquer momento e operarem de maneira invisível, para isso bastam dois ou mais computadores conectados. Dessa forma, seu caráter subterrâneo e disperso dificulta sua observação e análise. Um desenho de pesquisa que se dedica a tais redes deve contornar as limitações técnicas e sociais a fim de obter dados relevantes sobre sua dinâmica de funcionamento. A presente pesquisa, a partir de seu desenho, não apresenta condições materiais, técnicas e sociais de empreender tal tarefa. No entanto, conforme discutido acima, a cartografia é um processo em construção constante juntamente com o próprio objeto de estudo. Por essa razão, essa pesquisa buscará utilizar um *proxy*, apresentando razões que justifiquem tal escolha, para medir e mapear o impacto do discurso e ação dos ativistas.

A partir da ideia de cartografia e do avanço nas ferramentas para a obtenção e visualização de dados gerados pelas interações virtuais, se desenvolveu a metodologia de cartografia de controvérsias. Apresentada como um processo dinâmico e em constante construção, essa metodologia tem sido discutida e utilizada por diversos pesquisadores na Europa e, mais recentemente, no Brasil. O tópico seguinte se dedica a introduzir o debate sobre a cartografia de controvérsias, assim como apresentar seu repertório de técnicas, ferramentas e metodologias.

4.2.1 Cartografia das Controvérsias

De maneira resumida, cartografia de controvérsias é um conjunto de técnicas e ferramentas para explorar e visualizar polêmicas. Os dois principais pesquisadores da área, Bruno Latour e Tommaso Venturini, definem a cartografia de controvérsias como uma versão mais didática e prática da Teoria do Ator-Rede. Diversas instituições estão reunidas em um esforço coletivo, teórico e técnico, para desenvolver, amp

liar e difundir a cartografia de controvérsias como método de pesquisa social. Essa iniciativa resultou no projeto MACOSPOL[40] (Mapping Controversies on Science for Politics).

> MACOSPOL (Mapping Controversies on Science for Politics) is a joint research enterprise that gathers scholars in science, technology and society across Europe. Its goal is to devise a collaborative platform to help students, professionals and citizens in mapping out scientific and technical controversies. Technical democracy requires spaces and instruments to facilitate public involvement in technological and scientific issues. Such democratic equipment is yet to be assembled, even though much theoretical research has been done to envision its articulation. At the same time, digital innovations are providing an increasing number of new instruments and forums that can be used to promote public participation. MACOSPOL has been set up to facilitate the connection between these two developments, allowing the best research in science, technology and society to ally with the best research on web-based tools. (MACOSPOL, online).

O pesquisador italiano Tommaso Venturini (2010) afirma que, segundo a metodologia desenvolvida por Bruno Latour, a cartografia de controvérsias se baseia em: "just look at controversies and tell what you see" (VENURINI, 2010, p. 259). A partir dessa definição, aparentemente simples, a complexidade do método aparece. Dois problemas principais surgem e precisam ser definidos: "apenas" (just) e "controvérsias" (controversies). Em primeiro lugar, se o método se resume a apenas observação e descrição, não resta nada de teoria social ou metodologia científica. No entanto, os autores afirmam que minimalismo metodológico e conceitual é um desafio para os pesquisadores, que devem observar o objeto a ser estudado e, a partir disso, aplicar as ferramentas e teorias que melhor abarcam o problema. A partir da ênfase em "apenas" observar surgem três consequências principais.

A primeira consequência do "just" é que a cartografia de controvérsias não necessita de uma teoria ou metodologia específica. Porém, isso não significa que estas devem ser abandonadas, pelo contrário: "not imposing any specific philosophy or procedures, the cartography of the controversies invites scholars to use every observation tool at hand, as well as mixing them without restraint" (VENTURINI, 2010, p. 260). Em seguida, a segunda constatação apontada afirma que os pesquisadores não podem fingir imparcialidade e declarar neutralidade: "According to the cartography of controversies, research perspectives are never unbiased. Some viewpoints may offer a wider or clearer panorama on social landscape, but no observation can escape its origin." (VENTURINI, 2010, p.260). Por esse motivo, a cartografia de controvérsias busca a objetividade multiplicando os pontos de observação. Esse fato se liga a primeira constatação, pois, no lugar de métodos e teorias escolhidos previamente, a

[40] http://mappingcontroversies.net/

cartografia de controvérsias opta por uma promiscuidade teórico-metodológica[41]. Por último, a terceira consequência é que pesquisadores têm que rever permanentemente suas atitudes em torno do objeto. Isso significa dar voz a todos os atores envolvidos, mesmo que as opiniões em torno da controvérsia escapem a qualquer fundamento científico.

Ainda que o método afirme recuso protocolos em metodológicos pré-estabelecidos, Venturini conclui a análise do "apenas" observar de forma imperativa, com as principais recomendações para uma cartografia de controvérsias:

> 1. you shall not restrain your observation to any single theory or methodology;
> 2. you shall observe from as many viewpoints as possible;
> 3. you shall listen to actors' voices more than to your own presumptions. (VENTURINI, 2010, p.261)

O outro ponto crucial para se compreender e aplicar a cartografia de controvérsias é a própria definição de controvérsia. Segundo o MACOSPOL, controvérsias são questões não estabilizadas ou fechadas, referem-se, em geral, a incertezas compartilhadas por grupos sociais. Dessa forma, controvérsias são situações nas quais os atores discordam entre si, ou ainda, concordam em sua discordância.

> The notion of disagreement is to be taken in the widest sense: controversies begin when actors discover that they cannot ignore each other and controversies end when actors manage to work out a solid compromise to live together. Anything between these two extremes (the cold consensus of reciprocal unawareness and the warm consensus of agreement and alliance) can be called a controversy (VENTURINI, 2010, p. 264).

Ao apresentar o conceito de controvérsia dessa forma e consciente de que essa definição é um tanto quanto vaga, Venturini busca discorrer sobre as características de uma controvérsia. Primeiramente, controvérsias envolvem tipos diversos de atores humanos e não humanos (instituições, regras econômicas, leis, etc.). Justamente por isso, controvérsias formam espaços de debate híbridos: "Controversies are the place where the most heterogeneous relationships are formed" (VENTURINI, 2010, p. 264). Em segundo lugar, controvérsias mostram o social em sua forma mais dinâmica, pois, além da formação de alianças improváveis, unidades sociais aparentemente indivisíveis podem se fragmentar dando início a novas redes ou, de maneira análoga, redes dispersas podem se unir para agir como um

[41] That's why the cartography of controversies refuses to engage with any single philosophy or protocol and encourages instead theoretical and methodological promiscuity. (VENTURINI, 2010, p.260).

ator. Em terceiro lugar, devido a sua complexidade, controvérsias oferecem resistência às reduções: “In controversies, actors tend to disagree on pretty much anything, included their disagreement itself. That’s why issues are so difficult to solve, because they are impossible to reduce to a single resuming question” (VENTURINI, 2010, p. 265). Em quarto lugar, as controvérsias são debatidas, isto é, elas surgem devido a um estado de desestabilização, quando algo que não estava na superfície, oculto ou estabilizado, emerge para o centro do debate, colocando os problemas em evidência e abrindo o que o autor define como caixas-pretas[42] (black boxes). Por fim, as controvérsias são conflitos, ou seja, mesmo que não deflagrem lutas abertas, a discordância é fruto de um choque de mundos, culminando em disputas de poder. Em resumo:

> In a few words, when you look for controversies, search where collective life gets most complex: where the largest and most diverse assortment of actors is involved; where alliances and opposition transform recklessly; where nothing is simple as it seems; where everyone is shouting and quarrelling; where conflicts grow harshest. There, you will find the object of the cartography of controversies. (VENTURINI, 2010, p 266)

A complexidade das controvérsias é o que demonstra sua relevância e dificuldade de apreensão. Em primeiro lugar, as controvérsias são complexas porque essa é uma característica inerente da ação social coletiva. A variedade de atores envolvidos, especialmente não humanos, cria uma intricada rede de relacionamentos e posições que, por sua vez, cresce em complexidade cada novo argumento ou ator que toma parte na ação. No entanto, isso não significa dizer que as controvérsias são caóticas e não inexplicáveis. É possível afirmar que os atores estão buscando simplificar ou reduzir a complexidade de suas interações, atribuindo um sentido a sua ação e tornando possível sua gestão. A cartografia de controvérsias demanda um grande esforço, pois a ação coletiva é forjada em grandes esforços. Além disso, controvérsias são oportunidades e ferramentas para a observação da formação social, isto é, elas precedem a estabilização, a formação de certezas, a sedimentação de valores ou diretrizes, são o social em sua forma líquida segundo Venturini (2010):

> To observe how the social is built, scholars have no other choice than diving into controversies no matter how difficult and dangerous this could be. Controversies are complex because they are the crucible where collective life is melted and forged: they are the social at its magmatic state. (VENTURINI, 2010, p. 269).

[42] Segundo o autor, caixas-pretas são "things and ideas that would otherwise be taken for granted” (VENTURINI, 2010, p. 265).

A questão que surge após a definição de controvérsias é: como observar uma controvérsia? Como criar dispositivos de observação que ofereçam uma riqueza de detalhes e contribua para uma ampla visualização da controvérsia? Em primeiro lugar, a posição do pesquisador em relação ao objeto deve ser definida. De acordo com a Teoria Ator-rede, as controvérsias pertencem aos atores, isto é, os concernidos as constroem não os pesquisadores e cartógrafos. Segundo o autor: "Controversies belong to actors: it was actors who sow their seeds, who raised their sprouts, who nurtured their development. Scholars have no right to jump in and impose their solutions" (VENTURINI, 2010, p. 276). No entanto, pesquisadores podem expressar suas opiniões e observações sobre a controvérsia em questão, desde que isso não oculte outras vozes em nome de uma verdade ou objetividade científica.

Por outro lado, quando pesquisadores descrevem as controvérsias eles contribuem para a solidificação de alguns pontos ao trazê-los para um nível de complexidade que pode ser gerido mais facilmente. Porém, deve se ter claro que observar e descrever não são processos com objetivos diferentes, mas sim complementares. Para clarificar o processo, Venturini (2010), a partir de Latour, aponta para as principais recomendações para a prática de uma cartografia de controvérsias: 1) Perplexidade: não se deve simplificar o número de proposições a serem levadas em conta; 2) Consulta: o número de vozes escolhidas para articular uma proposição não deve ser arbitrariamente escolhido; 3) Hierarquização: deve-se discutir a compatibilidade das novas proposições entre os que já estão instituídos como uma forma de dar-lhes legitimidade; 4) Instituição: com as posições consolidadas, não se deve questionar a sua presença legítima na ação coletiva[43].

A partir da observação e descrição, o desafio seguinte é apresentar as controvérsias da melhor maneira possível. Assim como um cartógrafo vai a campo e faz anotações sobre o relevo, os rios e, com isso, começa a esboçar seus mapas, o cartógrafo social investiga a controvérsia e, a partir de suas anotações e rascunhos, começa a desenhar um mapa que possibilite a visualização do debate. Porém, da mesma forma que todo mapa apresenta uma escala, a cartografia de controvérsias construída é uma representação da realidade. Como na geografia, um mapa de uma cidade em escala 1:1 é a própria cidade, não servindo ao seu

[43] "First requirement: You shall not simplify the number of propositions to be taken into account in the discussion. Perplexity. Second requirement: You shall make sure that the number of voices that participate in the articulation of proposition is not arbitrarily short-circuited. Consultation. Third requirement: You shall discuss the compatibility of new propositions with those which are already instituted, in such a way as to maintain them all in the same common world that will give them their legitimate place. Hierarchization. Fourth requirement: Once the propositions have been instituted, you shall no longer question their legitimate presence at the heart of collective life. Institution" (VENTURINI, 2010, p. 277).

propósito. Assim também ocorre com a cartografia de controvérsias, a representação produzida deve legitimar a controvérsias e apresentar seus pontos. Além disso, ela lida com diferentes objetividades e considerações que devem ser tomadas na construção da representação.

Venturini (2012) aponta três pontos a serem considerados na apresentação da cartografia: representatividade, influência e interesse. Uma opinião ou afirmação defendida por muitos atores apresenta um grau maior de representatividade e, por isso, deve ser apresentada com um destaque maior do que outra opinião isolada. Porém, vale ressaltar que representatividade está ligada mais ao peso das opiniões do que com a contagem de atores. "Yet, maps should avoid flattening the landscape of public debate. Not all perspectives are equally supported and social cartographers should find ways to render such disparity." (VENTURINI, 2012, p. 800). Da mesma forma, as posições em um debate controverso são diferentes e os diversos atores se enfrentam tentando influenciar o movimento dessas posições, por esse motivo, atores com maior influência devem ser observados com atenção. Quanto maior a influência, maiores as chances de um ator moldar uma controvérsia.

Se, por um lado, representatividade e influência apontam para os principais atores em uma controvérsia e suas capacidades; por outro, a cartografia deve abrir espaço para atores minoritários. O interesse de tais atores, a discordância de uma minoria, é o que, muitas vezes, abre as caixas-pretas.

> It is disagreeing minorities who bring controversies into existence by refusing to settle with the mainstream and reopening the black boxes of science and technology. No matter how marginal, disagreeing viewpoints can be interesting because they offer original perspectives and question what is given for granted. Something that is very visible on a map is not necessarily very visible in the territory. Cartographers may legitimately choose to be proportional to interest instead of size. (VENTURINI, 2012, p. 801).

Após decidir como selecionar os atores e vozes que devem estar na cartografia e sua relativa posição, Venturini destaca que três preocupações na construção do mapa de controvérsias: adaptação, redundância e flexibilidade. A primeira diz respeito necessidade de tornar o mapa plano, isto é, adaptar os pontos de vistas dos diversos a uma superfície plana (horizontal), evitando a construção de grandes esquemas interpretativos (verticais). A segunda preocupação diz que é impossível um mapa conter todas as informações. As diversas questões que se sobrepõem podem, e em certo sentido devem, dar origem a vários mapas. A terceira

preocupação trata da flexibilidade do mapa, isto é, deve-se evitar a tentativa de se esgotar a controvérsia, o mapa deve permanecer aberto e flexível para novas perspectivas e ajustes.

> To sum up, the objectivity of cartographic representations depends on the quantity and the quality of the work spent to build them. What is true for buildings is true for representations as well: the better they are built (the more they adapt to their territory, the more they are redundant and flexible), the more solid they will be. (VENTURINI, 2012, p. 803).

A partir dessas definições, uma espécie de recomendações gerais e abertas para construção de uma cartografia de controvérsias, o próximo desafio é a busca por fontes, dados e pontos de vistas, a matéria-prima para a construção dos mapas de controvérsias. Nesse sentido, o avanço das interações virtuais, mediadas por máquinas, representa um grande auxílio para o esforço do cartógrafo social, pois, uma quantidade enorme de controvérsias é debatida diariamente e, graças à estrutura da mediação cibernética, seus rastros podem ser acessados e catalogados. Isso não significa dizer que a cartografia de controvérsia é um método exclusivo da pesquisa para internet, é possível realizar uma cartografia de com base em dados de revistas, jornais, declarações oficiais, etc. No entanto, instrumentos de busca de dados e o aumento expressivo de vozes inseridas nos debates virtuais abrem um novo horizonte de possibilidades para o desenvolvimento da metodologia.

Nesse contexto, duas características da interação cibernética são essenciais para contribuir na construção de uma cartografia de controvérsias: rastreabilidade e agregabilidade[44]. Isto significa dizer que tudo comunicação mediada deixa rastros, metadados e informações pertinentes para a pesquisa social. A relativa facilidade de acesso a esses rastros representa um importante impacto para as ciências sociais, uma vez que os custos para a obtenção de dados e de rastreamento de atores e pontos de vista se torna mais acessível. Já a agregabilidade se refere ao processo de conversão de um grande volume de dados para uma forma de leitura mais simples.

> To aggregate information means displaying it in a condensed form, transforming data so that few elements become representatives of many other. Several examples can be provided: synopsis and listing in writing, calculation and inference in statistics, diagrams and stylizations in design. All these techniques (and many other) are used by scientists to make complexity readable. (VENTURINI, 2012, p. 806).

[44] "traceability and aggregability" (VENTURINI, 2012, p. 804).

Dessa forma, a utilização dos dados cibernéticos para a construção de cartografias sociais oferece condições para a visualização de um grande número de interações e trocas de opiniões. Esses dados, espalhados pela rede, podem ser reunidos, processados e transformados em formatos de leitura mais simples, contribuindo para a compreensão do debate. Por fim, deve-se levar em conta a ressalva dos pesquisadores sobre a cartografia das redes: "1. search engines are not the web; 2. the web is not the Internet; 3. the Internet is not the digital; 4. the digital is not the world" (VENTURINI, 2012, p. 808). Essas recomendações chamam a atenção para os diversos níveis e tipos de interações e universos possíveis dentro das redes cibernéticas. E, ainda, ressalta a conexão desses fatos com um mundo real, não sendo possível uma separação como a que se pensou no início das pesquisas sobre internet. (FRAGOSO, RECUERO & AMARAL, 2010).

O debate metodológico sobre as cartografias sociais encontra-se aberto e em construção, como deve ser segundo seus principais pensadores. Dessa forma, o que se buscou aqui foi apresentar o estado da arte dessa metodologia e estabelecer o alicerce para a construção da cartografia do ativismo cypherpunk, objetivo dessa pesquisa. Portanto, o tópico seguinte se dedicará a discutir o caminho percorrido para a obtenção de dados e a confecção dos mapas ativistas, sempre buscando explicitar e justificar as escolhas como forma de garantir a discussão científica, permitindo assim a verificação do trajeto adotado pelo desenho de pesquisa.

4.3 CARTOGRAFANDO O ATIVISMO CYPHERPUNK

Considerando o que foi apresentado até aqui, a pesquisa desenvolverá uma cartografia do ativismo cypherpunk no Brasil. Para isso, são necessárias mais algumas considerações a respeito das escolhas metodológicas e conceituais. Essas escolham giram em torno da busca, processamento e visualização de dados, ou seja, a espinha dorsal de uma pesquisa empírica na internet. Em outras palavras, é preciso responder três perguntas-chave sobre a busca de dados na internet: O que? Onde? Como?

Em primeiro lugar, a pesquisa adota o termo "Cypherpunk" de maneira bastante ampla. Conforme debatido anteriormente, o termo se refere aos ativistas que desenvolvem e distribuem ferramentas de criptografia como forma de combater a vigilância dos Estados e uso de dados privados por corporações. O livro "Cypherpuks: liberdade e o futuro da internet"

(2013), assinado por Julian Assange e outros três ativistas (Jacob Applebaum, Andy Müller-Maguhn e Jérémie Zimmermann), é um marco para a definição dos temas que formam a agenda dos ativistas. Ainda que a origem dos cypherpunks remonte ao início da década de 1990, os casos Wikileaks (2010) e Edward Snowden (2013) amplificaram o alcance do debate e a popularidade dos grupos de ativistas. Por essa razão, a presente pesquisa considera sob o termo "cypherpunks" os diversos grupos e/ou indivíduos que defendem publicamente as linhas centrais inspiradas pelos ativistas citados. São elas: privacidade e liberdade na internet; navegação anônima; neutralidade na rede; livre expressão na internet; transparências para os governos. Não se intenta realizar um estudo de identidades, que apresente as características dos membros do grupo, ou ainda um estudo de caso, sobre algum dos coletivos citados. O que se pretende é cartografar o impacto desse discurso e demonstrar seus principais pontos na rede.

Em segundo lugar, as infinitas de conexões e possibilidades das redes cibernéticas geram a necessidade de recortes e escolhas como forma de tornar a pesquisa possível e operacional. Assim como em pesquisas off-line, o recorte do local de pesquisa é essencial na pesquisa na internet. Dessa forma, fatores teóricos, técnicos e pragmáticos influenciam essa decisão. Do ponto de vista teórico, o potencial de resistência de uma rede reside em sua característica horizontal, em redes distribuídas, na qual qualquer ponto da rede pode se conectar a outro. No entanto, tais estruturas de rede escapam da capacidade técnica de apreensão dessa pesquisa. Redes distribuídas podem se formar a qualquer momento, mantendo sua característica subterrânea (como a ideia de rizoma em Deleuze e Guattari). Isso leva a uma discussão técnica sobre a obtenção de dados.

As mídias sociais (Facebook, Twitter, Instagram, etc.) estão presentes no cotidiano das pessoas, governos e empresas. Sua estrutura, de maneira geral, visa conectar pessoas ou organizações com interesses em comum. A plataforma de operação e os recursos disponíveis variam bastante de uma para a outra. O que vale ressaltar é que as mídias sociais funcionam a partir da ideia de redes sociais, isto é, um local no qual o usuário mantém contato com sua rede de contatos, relacionamentos afetivos ou profissionais, ou temas de seu interesse. Dessa forma, extrair dados de mídias sociais se torna uma importante ferramenta para a pesquisa na internet. Para o propósito cartográfico, visando mapear o debate, duas mídias surgem como principais pontos de discussão devido ao seu alcance e popularidade: Facebook e Twitter.

Por um lado, o Facebook é a mídia social mais popular do mundo, com 1,39 bilhões de usuários ativos mensalmente[45]. Seu formato favorece a postagem de diversos tipos de conteúdos multimídia (fotos, vídeos e textos), formando um dos maiores acervos do mundo desse tipo de material. No entanto, seu formato de conexão entre perfis privilegia o contato com pessoas conhecidas em seu círculo pessoal. Além disso, as diversas alterações no algoritmo de funcionamento do Facebook demonstram que o conteúdo recebido por cada usuário pode variar bruscamente e ser manipulado, calculando as possíveis preferências de cada usuário, de acordo com os anúncios. Um exemplo disso é o estudo "Experimental evidence of massive-scale emotional contagion through social networks" (KRAMER, GUILLORY, HANCOCK, 2013), que manipulou o conteúdo oferecido a mais de 600mil usuários para tentar estabelecer uma relação entre o tipo de postagem visualizada e as emoções dos usuários.

Por outro lado, o Twitter é uma mídia social conhecida como microblog por, desde sua criação em 2007, restringir as postagens dos usuários a apenas 140 caracteres. Com 288 milhões de usuários ativos mensamente, cerca de 500 milhões de *tweets* são produzidos todos os dias[46]. O Twitter se destaca justamente por sua fluidez e rapidez de postagem e leitura. Esse fato combinado com o fato de que 80% dos usuários estão conectados via dispositivos móveis chamam a atenção para a interação rápida e dinâmica do Twitter em relação a grandes temas, eventos ou acontecimentos. O uso de *hashtags*, palavras ou frases precedidas pelo símbolo "#" facilitando o acesso ao conteúdo produzido usando a mesma *hashtag*, se tornou essencial em campanhas online ou grandes debates. Dessa forma, a arquitetura do Twitter permite, de forma mais aberta que o Facebook, a conexão e o diálogo entre usuários desconhecidos e distantes (geograficamente ou na estrutura da rede). Isto é, ao se engajar em uma discussão ou campanha é possível um usuário trocar argumentos e informações com outro que não está em sua rede de contatos, tornando assim os debates mais abertos e imprevisíveis.

Ambas as mídias sociais, Facebook e Twitter, foram amplamente utilizadas nos diversos protestos surgidos após a crise de 2008: Occupy Wall Street, Primavera Árabe 15-M, Gezi Park, Jornadas de Junho, etc (LIMA, 2013; SECCO, 2013). Da mesma forma, elas têm

[45] Dados do relatório anual do Facebook:
"Statistics: 890 million daily active users on average for December 2014; 745 million mobile daily active users on average for December 2014; 1.39 billion monthly active users as of December 31, 2014; 1.19 billion mobile monthly active users as of December 31, 2014; Approximately 82.4% of our daily active users are outside the US and Canada". (Disponível em: http://newsroom.fb.com/company-info/ acesso em 15/01/2015).
[46] Dados disponíveis em: https://about.twitter.com/company (acesso em 15/01/2015).

sido cada vez mais adotadas e discutidas no contexto de campanhas eleitorais e comunicação política. Tais fatos são razões suficientes para sustentar uma ampla agenda de pesquisa sobre os desdobramentos políticos de sua utilização. O que se pretende aqui é debater qual delas é a melhor fonte para obtenção dos dados necessários para a construção de uma cartografia sobre o ativismo cypherpunk. A partir de uma opção teórica e pragmática, a presente pesquisa adotará o Twitter como fonte de dados para construção da cartografia. Teoricamente, conforme discutido acima, o Twitter apresenta uma arquitetura mais aberta e que permite uma conversação pública mais dinâmica e interativa. Com isso, pode-se considerar o Twitter um simulacro de uma rede na qual cada ponto pode se conectar a qualquer outro. Pragmaticamente, a arquitetura do Twitter é mais amigável para a coleta de dados, aliada ao fato de que a maioria dos usuários mantém suas postagens públicas. Além disso, softwares de código aberto têm apresentado bons resultados nas buscas por dados no Twitter, diminuindo assim os custos e incentivando as pesquisas. No entanto, de maneira paralela e complementar, a pesquisa utilizará dados de páginas do Facebook que estão abertos e acessíveis de forma gratuita. Os dados complementares obtidos nas páginas do Facebook ajudarão a mapear e compreender o "ecossistema" ativista, enquanto os dados do Twitter proporcionarão uma visão do debate em si.

Definido o que buscar e onde buscar, o passo seguinte é operacionalizar a coleta e o processamento dos dados. Considerando a centralidade dessa discussão para o desenvolvimento da pesquisa, o tópico seguinte se dedicará a apresentar os procedimentos, suas limitações e virtudes, e os dados obtidos.

4.3.1 Levantamento de dados

De acordo com o desenho de pesquisa proposto, o capítulo anterior tratou da construção do conceito de privacidade, central na discussão dos ativistas, e apontou de maneira descritiva, a partir de documentos e declarações, quais são os principais grupos atuando no país. Esse ponto é essencial para a construção dos indicadores necessários para a chamada mineração de dados nas redes. Esse tópico se dedica a discutir as técnicas e ferramentas empregadas no processo e apresentar os resultados.

A construção dos indicadores para a busca de dados no Twitter não obedece a regras pré-estabelecidas. Conforme dito anteriormente, o processo de construção cartográfica deve

se adaptar a melhor estratégia para obter a melhor visualização. Dessa forma, uma pesquisa sobre os sentimentos em relação a um político, por exemplo, visando captar sua popularidade e/ou rejeição nas redes, pode ser feita a partir de uma busca por menções ao seu nome. Da mesma forma, empresas utilizam tais mecanismos para um posicionamento estratégico de suas marcas e contato direto com consumidores. No caso de uma cartografia de um debate mais amplo e controverso é necessário entender os pontos centrais em disputa e, a partir disso, construir os indicadores para as buscas.

Para o levantamento de dados sobre o ativismo cypherpunk os seguintes termos foram retirados dos sites, declarações e manifestos dos ativistas: privacidade; anonimato; criptografia; neutralidade. Além disso, optou-se por usar como indicador de busca menções diretas aos grupos citados no capítulo anterior e a temas recorrentes em suas postagens, dessa forma utiliza-se: anonymous; Assange; cryptoparty; cryptorave; Partido Pirata; Actantes; Saravá; Escola de Ativismo; Antivigilância; Snowden; Wikileaks. Justifica-se a busca pelos termos "Assange" e "Snowden" devido a sua relevância internacional na divulgação do debate sobre privacidade e internet, assim como a organização "Wikileaks". O tópico seguinte discutirá a mineração dos dados e como esses termos são utilizados como ferramentas de buscas.

4.3.1.1 Data mining

A imensa quantidade de dados disponíveis na internet aponta para a necessidade de novas ferramentas para sua apreensão e análise. A utilização de ferramentas de *data mining* e *big data* têm aumentado no campo das ciências sociais. Trabalhos como os de Javier Toret (2013) e Axel Bruns (2010; 2012) buscam combinar ferramentas de captura, análise e visualização de dados de redes sociais como forma de auxiliar a compreensão de fenômenos sociais.

De acordo com a IBM (online)[47]: "Big Data é um termo utilizado para descrever grandes volumes de dados e que ganha cada vez mais relevância à medida que a sociedade se depara com um aumento sem precedentes no número de informações geradas a cada dia." Dessa forma, armazenar e analisar Big Data é o grande desafio para empresas e pesquisadores. Nesse sentido, as ferramentas de data mining, ou mineração de dados, são

[47] Disponível em: http://www.ibm.com/midmarket/br/pt/infografico_bigdata.html (Acesso em 10/02/2015)

essenciais na busca por informações relevantes. O processo de mineração de dados consiste na busca de padrões e/ou informações relevantes em bancos de dados volumosos (big data) por meio de algoritmos específicos. Portanto, big data e data mining são complementares e sua utilização nas ciências sociais abre novos horizontes de pesquisas.

Para a presente pesquisa três etapas foram realizadas: extração (mineração) dos dados das redes sociais; análise dos dados e visualização das redes. Cada etapa conta com softwares e ferramentas específicas para sua realização. Mineração de dados com os softwares "yourTwapperKeeper" para o Twitter e "Netvizz" para o Facebook; análise dos dados com o software R, Rstudio, além de scripts

em linguagem Python; e, por fim, as visualizações das redes foram construídas a partir de software Gephi e as "word clouds" por meio do Wordle. Todos os softwares utilizados são gratuitos e de código-aberto.

4.3.1.2 YourTwapperKeeper e Netvizz

O software yourTwapperKeeper é um minerador ou crawler[48] que opera por meio de requisições a API[49] do Twitter. Dessa forma, ele envia requisições e busca tweets contendo as palavras-chave ou hashtags inseridas na busca. Devido à estrutura da API do Twitter, que limita o número de requisições e o acesso a tweets antigos, o programa demanda tempo para a criação de bancos de dados robustos e significativos. De qualquer forma, a quantidade de dados gerados é diretamente relacionada à relevância e impacto do tema, isto é, quanto mais comentado e discutido é o tema mais dados serão coletados em menos tempo.

Já o software Netvizz funciona como um aplicativo dentro do próprio Facebook e está disponível para todos os usuários. No entanto, com as últimas mudanças na política de privacidade da rede social[50], o aplicativo Netivizz deixou de oferecer algumas de suas funcionalidades anteriores que possibilitavam a obtenção de dados sobre a rede de perfis conectados a determinada página ou usuário. Em sua nova versão é possível apenas obter

---

[48] Um *crawler* é um programa que acessa automaticamente páginas da web e recolhe informações pré-determinadas.

[49] "API é o acrônimo de Application Programming Interface ou, em português, Interface de Programação de Aplicativos. Esta interface é o conjunto de padrões de programação que permite a construção de aplicativos e a sua utilização de maneira não tão evidente para os usuários." Disponível em: http://www.tecmundo.com.br/programacao/1807-o-que-e-api-.htm (acesso em: 10/02/2015).

[50] Disponível em: https://developers.facebook.com/policy/ (acesso em: 10/02/2015).

dados de páginas, preservando os dados dos perfis pessoais[51]. Mesmo assim, essa ferramenta é bastante útil para a visualização de que se pode denominar "ecossistema" de páginas: páginas com interesses e objetivos semelhantes formando comunidades.

Para a presente pesquisa, o yourTwapperKeeper foi programado para trabalhar interruptamente buscando as palavras-chave definidas no tópico anterior. Já o Netvizz forneceu dados das seguintes páginas: Agência Pública; Anonymous Brasil; Cryptoparty; Direito à Privacidade; Garoa Hacker Club; Partido Pirata; Transparência Hacker; Wikileaks. Alguns dos grupos citados no capítulo anterior não estão presentes no Facebook, por essa razão, optou-se por pesquisar páginas relevantes que mantinham contato direto com tais grupos ("Direito à Privacidade", "Garoa Hacker Club" e "Transparência Hacker"). Já a página da "Agência Pública", agência de jornalismo investigativo independente, foi selecionada por sua relação direta com a organização Wikileaks, trabalhando em conjunto na liberação de documentos secretos que envolviam o Brasil.

Ambos os softwares, yourTwapperKeeper e Netvizz, trabalham obtendo dados das redes sociais. No entanto, eles se diferem em relação ao formato de saída de tais dados, isto é, como esses dados são exportados. O yourTwapperKeeper exporta os dados em diversos formatos (tabelas para o Excel, HTML), dentre eles o formato ".csv"[52] é o mais comum para o trabalho com grandes bancos de dados. Os dados exportados em formato "csv" estão em estado bruto, necessitando de processamento e análise. Já o Netvizz exporta os dados encontrados em formato "gdf", um arquivo de grafo pronto para a visualização no software Gephi. Dessa forma, os dados obtidos das páginas do Facebook, por meio do Netvizz, passam diretamente para a etapa de visualização. Enquanto os dados do Twitter passam por uma fase de processamento e análise por meio dos softwares R, Rstudio e Python.

O yourTwapperKeeper operou por quase dois meses, entre janeiro de 2015 e março de 2015, sendo interrompido por eventuais quedas de energia. Cabe ressaltar que o processo de captura retroativa de tweets é bem mais lento que o processo em tempo real, por essa razão a maioria dos tweets reflete a discussão no período de busca. A tabela abaixo demonstra a quantidade de tweets capturados durante período. Algumas buscam geraram um volume

[51] Para a presente pesquisa denomina-se "página" as chamadas "Like Pages" do Facebook, às quais os usuários e outras páginas se conectam por meio do "curtir" (like). Já os usuários são denominados "perfis pessoais" ou apenas "perfis" e se conectam a outros "perfis" por meio dos laços de amizade e às páginas por meio do "curtir". No entanto, por razões práticas, o interesse principal reside na relação entre "páginas" como forma de identificar comunidades e padrões.

[52] Comma Separated Values: dados separados por vírgulas ou outros marcadores. Esse formato é aceito em diversos softwares de processamento de dados.

muito grande de tweets, porém com muitas redundâncias (linhas repetidas). Após a análise do script, que exclui dados duplicados, chegou-se ao número correto de tweets. Por exemplo, inicialmente a busca por "antivigilância" apontava para cerca de 20 mil tweets, porém, após a exclusão dos dados duplicados esse número caiu drasticamente.

Quadro 2 – Número de Tweets encontrados por palavra-chave nas buscas do software yourTwapperKeeper.

Palavra-chave	Número de Tweets capturados
Anonimato	26776
Anonymous	213263
Antivigilância	714
Assange	40972
Ciberativistas	10982
Criptografia	5983
Cryptoparty	3990
Cryptorave	401
Cypherpunk	1919
Neutralidade	4241
Partido Pirata	4101
Privacidade	38577
Snowden	97748
Wikileaks	807554

4.3.2 Processamento e Análise com R, Rstudio e Python.

Após realizar a extração dos dados do Twitter, o software yourTwapperKeeper exporta um arquivo "csv" com os seguintes dados: text, to_user_id, from_user, id, from_user_id, iso_language_code, source, profile_img_url, geo_type, geo_coordinates_0, geo_coordinates_1, created_at, time. De maneira simplificada, o software fornece o texto do tweet, o perfil destinatário (quando houver), o perfil de origem, a língua utilizada, o dispositivo utilizado para enviá-lo, as coordenadas geográficas (quando houver) e a hora da envio. Portanto, para obter informações relevantes a partir desses dados é necessário um processo de análise e limpeza, uma vez que, devido ao volume de dados, a análise manual é praticamente impossível.

O software R e sua versão gráfica mais simplificada Rstudio[53] foram utilizados com o objetivo de extrair dos arquivos "csv" as relações de conexões entre perfis. Isto é, quais perfis

[53] "R is a language and environment for statistical computing and graphics. (...) R provides a wide variety of statistical (linear and nonlinear modelling, classical statistical tests, time-series analysis, classification,

se conectam, quais perfis são mais relevantes na rede, etc. Para isso, foi utilizado um script para o R chamado "Tweetgraph", que lê o arquivo, identifica as interações: menções (ATs) e retweets (RTs). Na linguagem do Twitter, menção é quando um tweet é enviado para outro perfil; e retweet é quando o conteúdo de um tweet é reproduzido integralmente por outro perfil, expandindo assim seu alcance. Esses dois tipos de interação são importantes para a análise, pois demonstram quem está interagindo e debatendo e quais são os perfis com maior alcance e relevância na rede da discussão. Dessa forma, ao executar no software R o script "Tweetgraph", após identificar as conexões entre os tweets, ele exporta um arquivo em formato "graphml" pronto para a visualização no software Gephi. O script "Tweetgraph" é o mesmo utilizado nas pequisas do LABIC[54] (Laboratório de Imagem e Cibercultura), da Universidade Federal do Espírito Santo, e do MediaLab[55], da Universidade Federal do Rio de Janeiro.

Além do R, foi utilizado um script para linguagem de programação Python chamado "parse_tweets". O script lê o arquivo "csv", corrige as linhas repetidas e extrai dados importantes como: principais hashtags, principais menções, principais usuários, localização geográfica, etc. Além disso, gera um arquivo com as principais palavras e hashtags encontradas nos tweets. Esse arquivo é utilizado para a criação das "nuvens de palavras" no software Wordle. Dessa forma, na presente pesquisa, o script "Tweetgraph" foi utilizado no software R para a criação das visualizações de rede do Twitter; já o script "parse_tweets", em linguagem Python, foi utilizado para extrair as principais palavras e hashtags para a criação das nuvens de palavras. Todos os scripts estão disponíveis nas páginas do LABIC[56] e do MediaLab[57] no repositório GitHub.

Portanto, após a discussão sobre a obtenção e o tratamento dos dados, a fase seguinte é a da confecção das visualizações das redes. Observar o funcionamento dinâmico das redes, as conexões e as relações de poder estabelecidas é fundamental para o desenvolvimento da Ciência Política em uma era de big data.

---

clustering) and graphical techniques, and is highly extensible. R is available as Free Software under the terms of the Free Software Foundation's GNU General Public License in source code form." Disponível em: http://www.r-project.org/ (acesso em: 05/01/2015).

[54] http://labic.net

[55] http://medialabufrj.net/

[56] https://github.com/ufeslabic

[57] https://github.com/medialabufrj/

4.4 VISUALIZAÇÕES DE DADOS

4.4.1 Nuvens de Palavras (Wordle)

Uma ferramenta importante para a análise do debate travado nas redes sociais é a visualização das principais palavras e hashtags utilizadas pelos perfis. Capturar termos repetidos pode fornecer um panorama dos principais pontos em debate e disputa. Obviamente, outras metodologias operam de maneira mais rígida e sistemática ao analisar os discursos das partes envolvidas. No entanto, ao extrair um volume de dados de dezenas de milhares de tweets, em alguns casos centenas de milhares, a captura das principais palavras e hashtags mencionadas fornece uma visão geral do debate, abrindo caminho para elaboração de hipóteses mais plausíveis e investigações mais detalhadas. Em uma cartografia, a visualização da nuvem de palavras opera em uma escala maior, funcionando de maneira similar a uma foto de satélite de um terreno. Isto é, permitindo uma visualização macroscópica do terreno e oferecendo indicações para pesquisas em escala reduzida.

Os dados obtidos do Twitter e analisados pelo script "parse_tweets", em linguagem Python, fornecem as principais menções para a análise do programa "Wordle[58]". O software elabora visualizações em nuvem das principais palavras respeitando a proporcionalidade entre elas. Isto é, quanto mais menções uma determinada palavra, maior ela aparecerá na nuvem. O script de análise apresenta alguns problemas relacionados à língua portuguesa, pois não reconhece alguns caracteres particulares do idioma como cedilha e acentos gráficos. Como não foi possível contornar esse problema, optou-se por manter os termos na nuvem de palavras considerando que a compreensão é minimente comprometida.

As nuvens de palavras apresentadas na sequência estão em ordem alfabética a partir da palavra-chave utilizada na busca. Por isso, as duas primeiras nuvens são referentes à busca por "antivigilância", a primeira formada pelas hashtags e a segunda pelas palavras mais comuns. O termo está vinculado diretamente ao perfil da Oficina Antivigilância. A baixa quantidade de tweets encontrada no período pesquisado pode indicar uma pequena penetração do Boletim Antivigilância no debate do Twitter. Apesar de se constituir como um dos únicos boletins regulares com notícias e discussões sobre o tema no Brasil, seu alcance parece restrito a uma comunidade já formada, não levando a discussão a um público maior. As nuvens de palavras, tanto as de hashtags quanto a de termos, indicam que o perfil reproduz muitos conteúdos em língua inglesa, funcionando com um hub de distribuição. Palavras-

[58] http://www.wordle.net/ (acesso em: 20/01/2015).

chave como “privacidade”, “anonimato”, “dados pessoais” “direitos humanos” demonstram a participação no debate. Já a produção original de conteúdo é demonstrada em palavras como “dicas”, “ferramentas” e “proteção”.

Figura 1 – Nuvem de Palavras das principais hashtags da busca por “Antivigilância” no Twitter

Figura 2 – Nuvem de palavras dos principais termos da busca por “Antigilância” no Twitter.

As pesquisas pelo termo “Assange” visavam encontrar relação entre citações ao fundador da organização “Wikileaks”, e um dos principais representantes do movimento cypherpunk, ao debate sobre privacidade e controle na internet. No entanto, nota-se um traço comum ao debate sobre privacidade na internet e transparência de governos, confirmado também mais adiante no caso Snowden e no caso Manning, a discussão sobre as personalidades, em grande medida alimentadas por polêmicas, se sobrepõem aos fatos objetivos em que elas estão envolvidas. Isto é, as principais hashtags e menções a “Assange” tratam de sua vida pessoal, enquanto apenas uma pequena parte faz relação ao trabalho ativista. As narrativas pessoais se misturam e, em vários momentos, ofuscam e confundem o debate objetivo sobre os temas propostos. Isso se confirma com as hashtags “Suécia”, onde Julian Assange responde a processos, e “Ecuador”, país que concedeu asilo político ao ativista e o abriga em sua embaixada em Londres. Já as hashtags “Manning”, “Snowden” e “Whistleblower” estão ligadas às campanhas pela liberdade de ativistas.

Figura 3 – Nuvem de Palavras das principais hashtagas da busca por “Assange”.

Figura 4 – Nuvem de Palavras com os principais termos encontrados na busca por "Assange".

As buscas pelo termo "Criptografia", central no discurso ativista de defesa da privacidade, resultaram principalmente em palavras e hashtags ligadas a empresas e serviços que violam a privacidade e a criptografia. A discussão sobre os controles dos mecanismos de criptografia também está presente, em especial a tensão entre segurança e navegação anônima, especialmente em casos ligados ao terrorismo. Por essa razão, estacam-se as hashtags "Código Penal" e "Ley Antiterrorista" (em espanhol). O nome do presidente Barack Obama também surge entre os principais termos devido ao crescente debate nos EUA sobre a regulação da internet[59].

[59] "Net neutrality" has been built into the fabric of the Internet since its creation — but it is also a principle that we cannot take for granted. We cannot allow Internet service providers (ISPs) to restrict the best access or to pick winners and losers in the online marketplace for services and ideas. That is why today, I am asking the Federal Communications Commission (FCC) to answer the call of almost 4 million public comments, and implement the strongest possible rules to protect net neutrality." Declaração oficial de Barack Obama. Disponível em: https://www.whitehouse.gov/net-neutrality (acesso 20/01/2015).

Figura 5 – Nuvem de Palavras das principais hashtags encontradas na busca por "Criptografia".

Figura 6 – Nuvem de Palavras dos principais termos encontrados na busca por "Criptografia".

Juntamente com a discussão sobre o uso de ferramentas criptográficas, o debate sobre a garantia da neutralidade da rede é essencial para se compreender o raio de ação dos ativistas. O Instituto Brasileiro de Defesa do Consumidor, em consonância com outros órgãos e ativistas, define neutralidade da rede como "o princípio que determina que todos sejam tratados com igualdade, sem que haja benefício para uns e não para outros na hora de navegar ou que haja limitação para clientes específicos." (IBDC, online). O tema foi bastante discutido durante a elaboração do texto do Marco Civil da Internet (LEI Nº 12.965, DE 23 DE ABRIL DE 2014) e está incluído na redação final. Para os ativistas, a neutralidade da rede garante que

internautas tenham acesso ao conteúdo que desejarem, sem a interferência das operadoras. Por essa razão, a neutralidade da rede é defendida como garantia de princípio democrático e de pluralidade de vozes. Na prática, trata-se de impedir a formação de grandes monopólios na criação de conteúdo para a internet, preservando o acesso a fontes alternativas de informação.

As hashtags encontradas estão ligadas diretamente a essa disputa no campo normativo. Elas formam o bloco de pressão pela garantia da neutralidade da rede. A hashtag "net neutrality" surge justamente no momento em que o governo norte-americano e ativistas discutem o tema. Os termos encontrados também demonstram a preocupação dos ativistas com a regulação da neutralidade na internet tanto no Brasil quanto nos Estados Unidos.

Figura 7 – Nuvem de Palavras com as principais hashtags da busca por "Neutralidade".

Figura 8 – Nuvem de Palavras dos principais termos encontrados na busca por "Neutralidade".

A busca por "Partido Pirata" retornou tweets relacionados à campanha de coleta de assinaturas para a formalização do partido e sua possível candidatura em 2016. Esse fato reforça a diferença entre os Piratas e os demais grupos ativistas: a via eleitoral. Entre as principais palavras se destaca a "Campus Party"[60], evento de tecnologia que ocorre anualmente em São Paulo e local de origem das primeiras reuniões em prol da fundação de um partido pirata brasileiro.

[60] http://beta.campus-party.org/ediciones/brasil/

Figura 9 – Nuvem de Palavras dos principais termos encontrados nas buscas por “Partido Pirata”.

A mineração de tweets oferece ainda a possibilidade de combinação de termos como forma de tornar a busca mais específica. Por exemplo, o termo “privacidade” pode produzir resultados diversos, apontando para outros debates. Dessa forma, optou-se pela busca combinada dos termos “privacidade” e “internet”. Assim, as nuvens de palavras criadas refletem de maneira mais próxima o debate que ativistas, empresas, governos e cidadãos travam nas redes. Entre as principais hashtags encontram-se novamente “marco civil”, “Brasil”, “segurança”. Aparecem também, com grande peso, menções a “Wikileaks” e “Assange”, assim como discussões menções a “Mark Zuckerberg” (criador do Facebook) sobre violações de privacidade por parte do “Facebook”. As hashtags “cpbr8” e “Campus Party” indicam que o evento é um polo de discussões sobre a relação entre privacidade e internet.

Figura 10 – Nuvem de Palavras das principais hasgtags encontradas nas buscas por "Privacidade + Internet".

Figura 11 – Nuvem de Palavras dos principais termos encontrados na busca por "Privicidade + Internet".

Como forma de comparação, a nuvem de palavras do termo "privacidade" apresenta pequenas diferenças em relação a busca combinada. Observa-se que termos como "casal" e

"foto", "vida" ganham peso, demonstrando a preocupação cotidiana com a privacidade. No entanto, termos como "Assange", "internet", "google" continuam aparecendo, o que sugere que o debate sobre privacidade, em geral, não se desvincula da preocupação com internet.

Figura 12 – Nuvem de Palavras dos principais termos encontrados na busca por "Privacidade".

Optou-se por buscar o termo "Snowden" devido a grande repercussão do caso e todo o debate público que se seguiu. Grupos ativistas utilizam os documentos liberados por Edward Snowden como base para seu discurso. Dessa forma, a constante citação ao nome poderia indicar quais outros temas estão em debate. Observou-se novamente a relação entre os termos "Snowden", "Assange" e "Manning", personagens principais do debate ativista sobre liberdade na internet. Além disso, destaca-se o termo "NSA" (National Security Agency), fonte dos documentos de Edward Snowden e o termo "suveillance" (vigilância). O período de buscas coincidiu com a premiação[61] do documentário "Citizenfour[62]", de Laura Poitras e Glenn Greenwald, sobre Edward Snowden. Já a hashtag "asksnowden" faz referência foi utilizada em uma ação de perguntas dos internautas para Edward Snowden.

[61] http://oscar.go.com/nominees/documentary-feature/citizenfour
[62] https://citizenfourfilm.com/

Figura 13 – Nuvem de Palavras das principais hashtags encontradas na busca por “Snowden”.

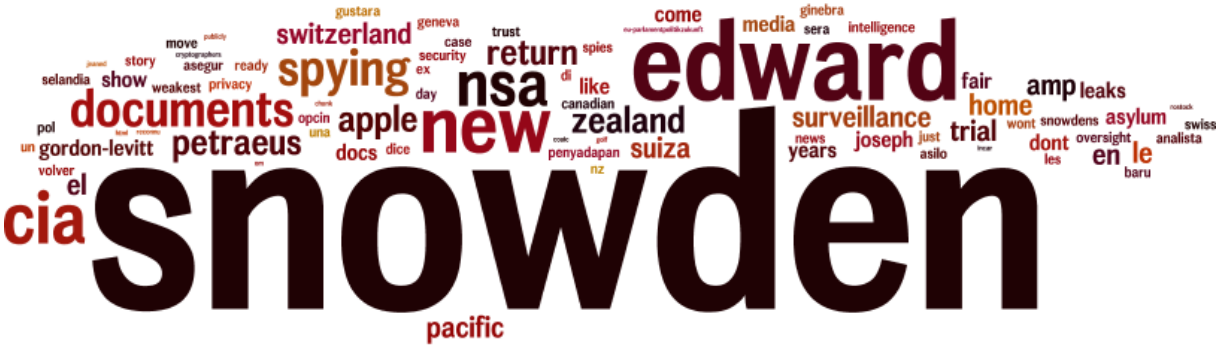

Figura 14 – Nuvem de Palavras dos principais termos encontrados na busca por “Snowden”.

Por fim, a nuvem de palavras da busca por “wikileaks” parece apontar para o epicentro de todo o debate, uma vez que o termo apareceu em várias vezes em outras buscas. Por essa razão, observa-se a ocorrência de quase todos os termos relacionados anteriormente. Campanhas pela liberdade de ativistas, denúncias de espionagem e a discussão sobre as particularidades do caso de Julian Assange. Vale ressaltar a hashtag “globogolpista” em referência a emissora de televisão Globo.

Figura 15 – Nuvem de Palavras das principais hashtags encontradas na busca por “Wikileaks”.

Figura 16 – Nuvem de Palavras com os principais termos da busca por “Wikileaks”.

As nuvens de palavras apresentadas acima oferecem um panorama dos principais termos discutidos no Twitter relacionados a presente pesquisa. A partir delas, não é possível medir as tendências e os sentimentos envolvidos na discussão, isto é, não se atribui valoração positiva ou negativa aos tweets. Porém, essa visão geral do debate é complementada pela análise de “autoridades” e “hubs” do debate. Dessa maneira, podem-se observar quais perfis pautam o debate e quais apenas reproduzem conteúdo. O tópico seguinte se dedica a apresentar a visualização desses dados.

4.4.2 Grafos e Autoridades

Os dados obtidos pelo yourTwapperKeeper e analisados pelo script “Tweetgraph” no software R podem ser visualizados na forma de grafos no software Gephi. Segundo o site do projeto: “Gephi is an interactive visualization and exploration platform for all kinds of networks and complex systems, dynamic and hierarchical graphs.” (GEPHI, online). O software gratuito e de código-aberto tem sido bastante usado em recentes estudos sobre fenômenos sociais em rede (BASTIAN, HEYMANN, JACOMY, 2009). Além da visualização das redes formadas pelas conexões entre perfis, o software permite cálculos estatísticos e algoritmos para a detecção de padrões, comunidades, relevância e autoridade dentro das redes.

Em primeiro lugar, é necessária uma breve discussão sobre o conceito de grafo. A Teoria dos Grafos é um ramo da matemática que se dedica ao estudo da relação entre objetos de um determinado conjunto (FEOFILOFF, KOHAYAKAWA, WAKABAYASHI, 2011). Atribui-se ao artigo de Leonard Euler, publicado em 1736, sobre as sete pontes de Königsberg o nascimento da teoria dos grafos. Segundo a história, a cidade prussiana de Königsberg foi construída entre ilhas cortadas por um rio. Ao todo havia sete pontes ligando as ilhas e seus moradores se desafiavam a percorrer a cidade sem repetir nenhuma ponte. O enigma dos moradores é resolvido por Euler, que concluiu ser impossível percorrer toda a cidade sem repetir uma ponte. Para isso, ele transforma as partes de terra firme em pontos (vértices ou nós) e os conecta com as pontes (arestas). Devido a esse modelo de visualização do problema do conjunto de pontes e terra firme é atribuído o nascimento de uma Teoria dos Grafos.

De acordo com a teoria, grafos são estruturas formadas a partir da notação G(V, A), na qual V é um conjunto de vértices (nós) e A é o conjunto de pares não ordenados de V, isto é, as arestas. Por exemplo, considerando dois nós (a, b) e uma aresta que os conecta, denominada (ab), aresta (ab) incide em a e em b, ou ainda, a e b são as pontas da aresta (ab). Dessa forma, pode-se representar um grafo a partir do seu conjunto de vértices V = {1,2,3,4,5} e seu conjunto de arestas A = {1,2}, {1,3}, {1,5}, {2,4}, {2,5}, {3,4}.

Ao extrair dados das redes sociais e, por meio do processamento, convertê-los em grafos o que se objetiva é entender as relações entre os atores (nós) a partir de suas interações (arestas). A estrutura em rede das interações virtuais demanda análises desse tipo. A teoria dos grafos e os avanços nos softwares de visualização permitem o estudo das relações

estabelecidas em redes sociais de maneira dinâmica e lidando com um grande volume de atores e interações (nós e arestas).

Portanto, após a transformação dos dados primários em uma tabela de grafos, formadas pelos atores e suas interações, é necessário ampliar o Quadro 2. O script tweetgraph utilizado no software R divide as interações em dois tipos: o primeiro cria as arestas a partir das interações de menções, isto é, quando um ator menciona o outro diretamente; já o segundo cria as arestas a partir dos retweets, isto é, quando um ator reproduz integralmente o conteúdo produzido por outro ator para sua própria rede de seguidos, ampliando assim seu alcance e endossando o conteúdo compartilhado.

Quadro 3 – Número de tweets capturados e quantidade de nós e arestas encontrados pelo processamento no software R.

Palavra-chave	Número de Tweets capturados	Número de Nós (RTs)	Número de Arestas (RTS)	Número de Nós (ATs)	Número de Arestas (ATs)
Anonimato	26776	8536	9115	5448	3887
Anonymous	213263	65693	69276	19847	14260
Antivigilância	714	253	224	47	33
Assange	40972	11381	13720	2434	2036
Ciberativistas	10982	4607	5302	1242	1332
Criptografia	5983	1233	1059	452	294
Cryptoparty	3990	1640	1963	264	184
Cryptorave	401	72	73	47	52
Cypherpunk	1919	458	399	212	170
Neutralidade	4241	1252	1194	382	230
Partido Pirata	4101	1846	1850	390	245
Privacidade	38577	18845	20755	5441	3168
Snowden	97748	28704	33229	5300	3804
Wikileaks	807554	23047	27980	5546	5133

A partir da tabela contendo todos os nós e suas interações, o software Gephi cria as visualizações dos grafos. Além disso, diversas análises estatísticas e algoritmos de distribuição estão disponíveis para os estudos. Para a presente pesquisa, optou-se por utilizar na análise dos dados do Twitter os algoritmos de autoridade, que mede o quanto um ator possui peso e influência sobre os demais nós em uma rede, e de modularidade, que analisa a formação de comunidade ou clusters, isto é, grupos de atores com maior afinidade entre si e laços mais consolidados. Em alguns casos também se fez necessário à aplicação de filtros de

grau para restringir o volume de dados e facilitar a manipulação e visualização dos grafos. O filtro de grau elimina os nós que não atingem um número mínimo ou máximo de conexões.

A visualização dos grafos apresenta diversas informações personalizáveis dependendo do objetivo da pesquisa. O tamanho e as cores dos nós, assim como dos rótulos (nomes dos nós) pode ser determinado por diversas variáveis. Para o presente trabalho, optou-se pela seguinte classificação. Destaca-se, de maneira simples, que a tabela seguinte funciona como legenda para a compreensão e leitura dos grafos.

Quadro 4 – Variáveis utilizadas na construção dos grafos dos dados do Twitter.

Unidade	Variável
Tamanho do Nó	Autoridade
Cor do Nó	Modularidade
Tamanho do Rótulo	Autoridade
Cor do Rótulo	Grau

Considerando isso, quanto maior a autoridade de um nó maior será seu tamanho e o tamanho de seu rótulo. Já a cor do nó é determinada pela comunidade a qual ele faz parte. Em alguns casos, comunidades consistentes não são encontradas, o que leva a uma dispersão das cores dos nós. Por fim, a cor do rótulo é determina pelo grau, número de conexões, que o nó faz, variando de uma escala que vai da cor preta ao vermelho. Portanto, quanto mais vermelho a cor do rótulo maior o grau daquele nó dentro da rede. Já as arestas mantém a cor do seu nó de origem, facilitando a visualização de comunidades.

Para cartografar o debate a partir a dos termos selecionados para as buscas, optou-se por identificar as principais autoridades em cada tema. Isto é, o software Gephi executa cálculos sobre a rede formada pelos grafos e indica, em uma escala de 0 a 1, qual nó é mais apontado por outro nós. Ou seja, qual nó produz conteúdo que é mais reproduzido por outros nós, demonstrando assim seu poder e influência sobre aquela rede.

Para a distribuição visual dos grafos dois algoritmos foram utilizados: “Force Atlas” e “Fruchterman-Reingold”. O primeiro trabalha aproximando ainda mais gráficos vizinhos e, ao mesmo tempo, afastando grafos mais distantes. O resultado são visualizações com formas diversas e variáveis. A distribuição “Force Atlas” se demonstrou muito útil para a visualização de comunidades, uma vez que destaca semelhanças e diferenças entre os nós. Já o segundo algoritmo, Fruchterman-Reingold, distribui os grafos em 360°, formando assim

uma visualização circular. Essa distribuição facilita a leitura mais geral dos grafos e da autoridade da rede. Em alguns casos, utilizou-se o algoritmo “Force Atlas”, como teste de comunidades, em seguida, utilizou-se o algoritmo “Fruchterman-Reingold” para uma melhor visualização da rede. A partir dessas considerações metodológicas é possível desenvolver as visualizações dos grafos nos tópicos seguintes.

4.4.2.1 Anonimato

A visualização da rede formada pelas menções e retweets do termo “anonimato” se demonstrou bastante dispersa, com o debate dividido em pequenos pólos e poucas autoridades. Isso se deve ao fato do termo se outros temas diferentes da discussão sobre as formas de navegação na internet. Outro problema encontrado é a dificuldade de separação entre os tweets de língua espanhola, uma vez que a palavra “anonimato” está presenta nas duas tanto em português quanto em espanhol. Da toda forma, esse fato apontou para a principal autoridade na rede retweets: o perfil @mexleaks (uma página mexicana de divulgação do Wikileaks). Ainda que a visualização seja inconclusiva sobre o debate sobre “anonimato” no Brasil, ela aponta para a necessidade de novas estratégias para abordar o tema nas minerações de dados. Por fim, demonstra que mesmo em língua espanhola, o Wikileaks é a principal autoridade sobre o tema.

Para a rede de menções foi utilizado o filtro de grau com os parâmetros 2 (mínimo) e 16 (máximo). Ou seja, estão visíveis apenas os grafos com mais de duas arestas. Da mesma forma para o grafo de retweets os parâmetros foram: 2 (mínimo) e 504 (máximo). Portanto, estão visíveis apenas nós que foram retweetados no mínimo duas vezes, sendo 504 o perfil com maior número de retweets. Ambos os grafos foram criados com a distribuição do algoritmo “Fruchterman-Reingold”.

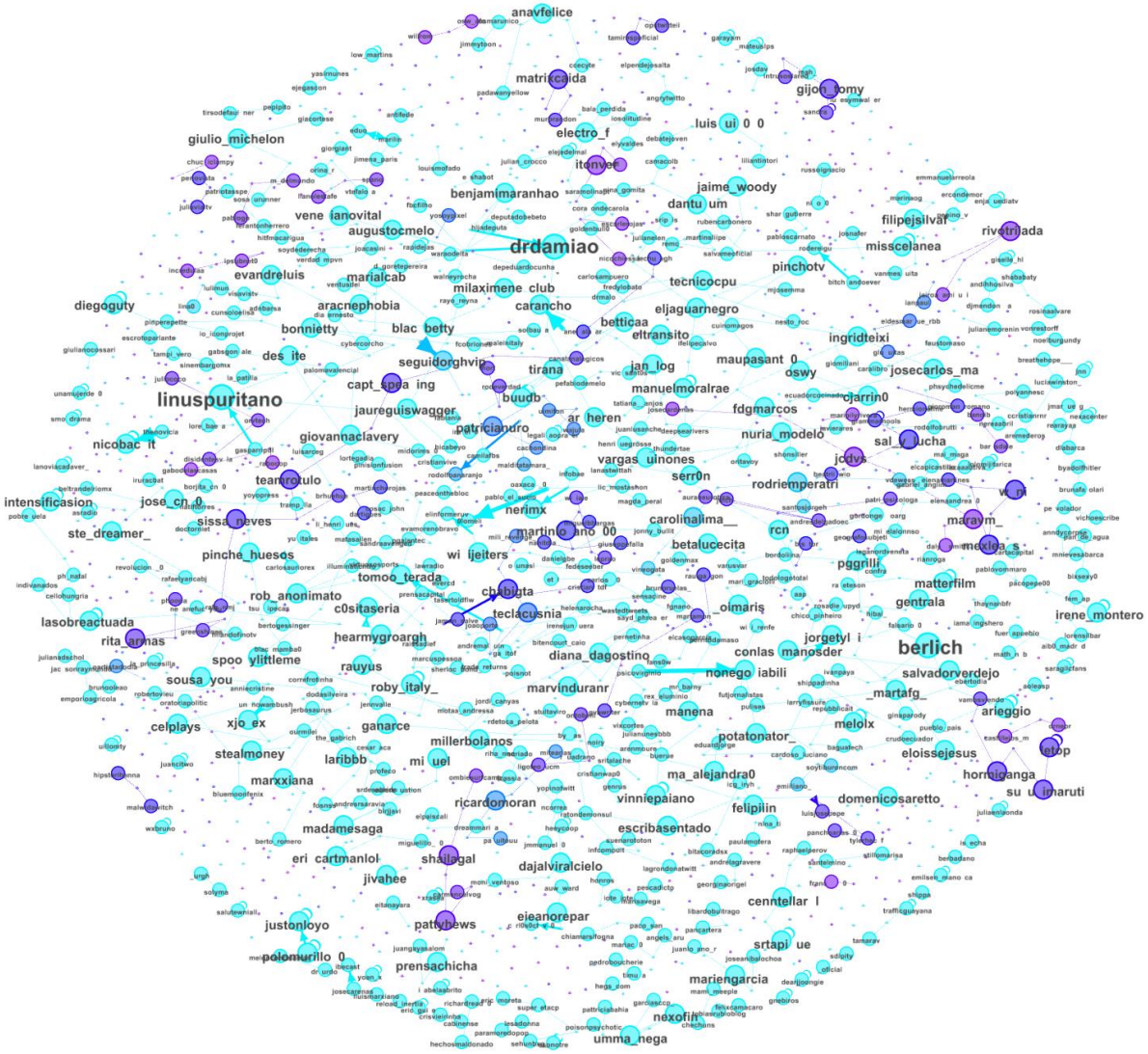

Figura 17 – Rede de grafos das menções ao termo “Anonimato” no Twitter.

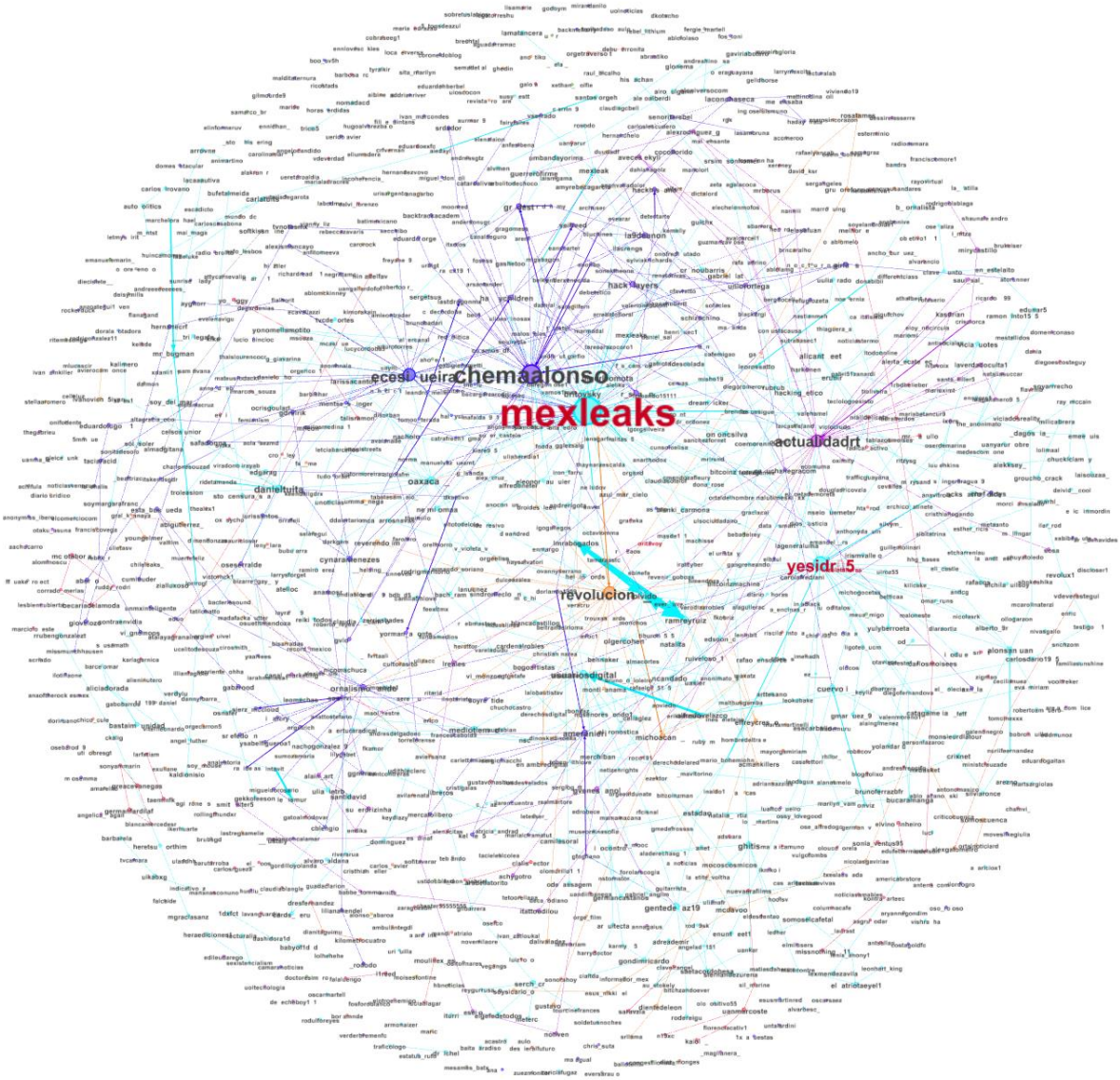

Figura 18 – Rede de Grafos dos Retweets do termo “Anonimato” no Twitter.

4.4.2.2 Anonymous

Os dados encontrados para o termo “anonymous” foram um dos mais volumosos, juntamente com o termo “Wikileaks”, porém com o maior número de nós e arestas. Em primeiro lugar, o termo “anonymous” é utilizado por grupos em todo o mundo, mantendo sua grafia em inglês e compartilhando seus propósitos. Dessa forma, uma visualização sobre o debate abrange os grupos mais relevantes na rede. Por essa razão, a utilização de filtros com parâmetros maiores for necessária para a viabilidade da visualização dos grafos. Os valores para os filtros foram: 33 (mínimo) e 6425 (máximo).

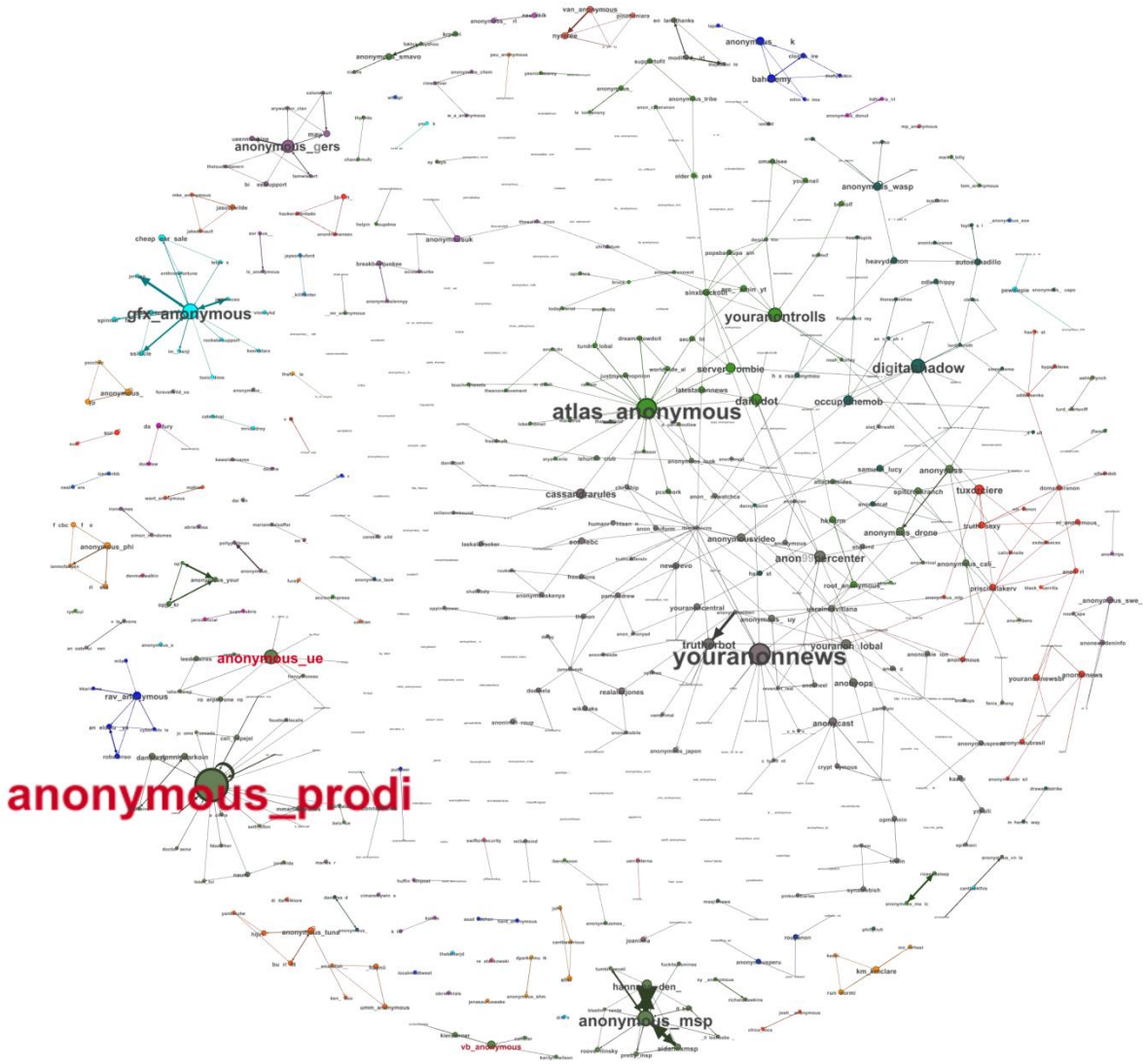

Figura 19 – Rede de Grafos das menções ao termo “Anonymous” no Twitter.

Ao contrário dos grafos sobre “anonimato”, é possível indicar as principais autoridades nos grafos sobre as menções a “anonymous”. Observa-se, em primeiro lugar, que as principais autoridades são perfis ligados as principais operações do grupo. Devido a postura do grupo em preferir a dispersão e o anonimato, não é possível afirmar que são perfis oficiais. Porém, sua atividade mais atuante oferece indícios para essa hipótese.

Quadro 5 – Autoridades nas menções ao termo “Anonymous”.

Perfis	Autoridade
anonymous_prodi	0,02

Youranonnews	0,013
atlas_anonymous	0,012
gfx_anonymous	0,009
anonymous_msp	0,009

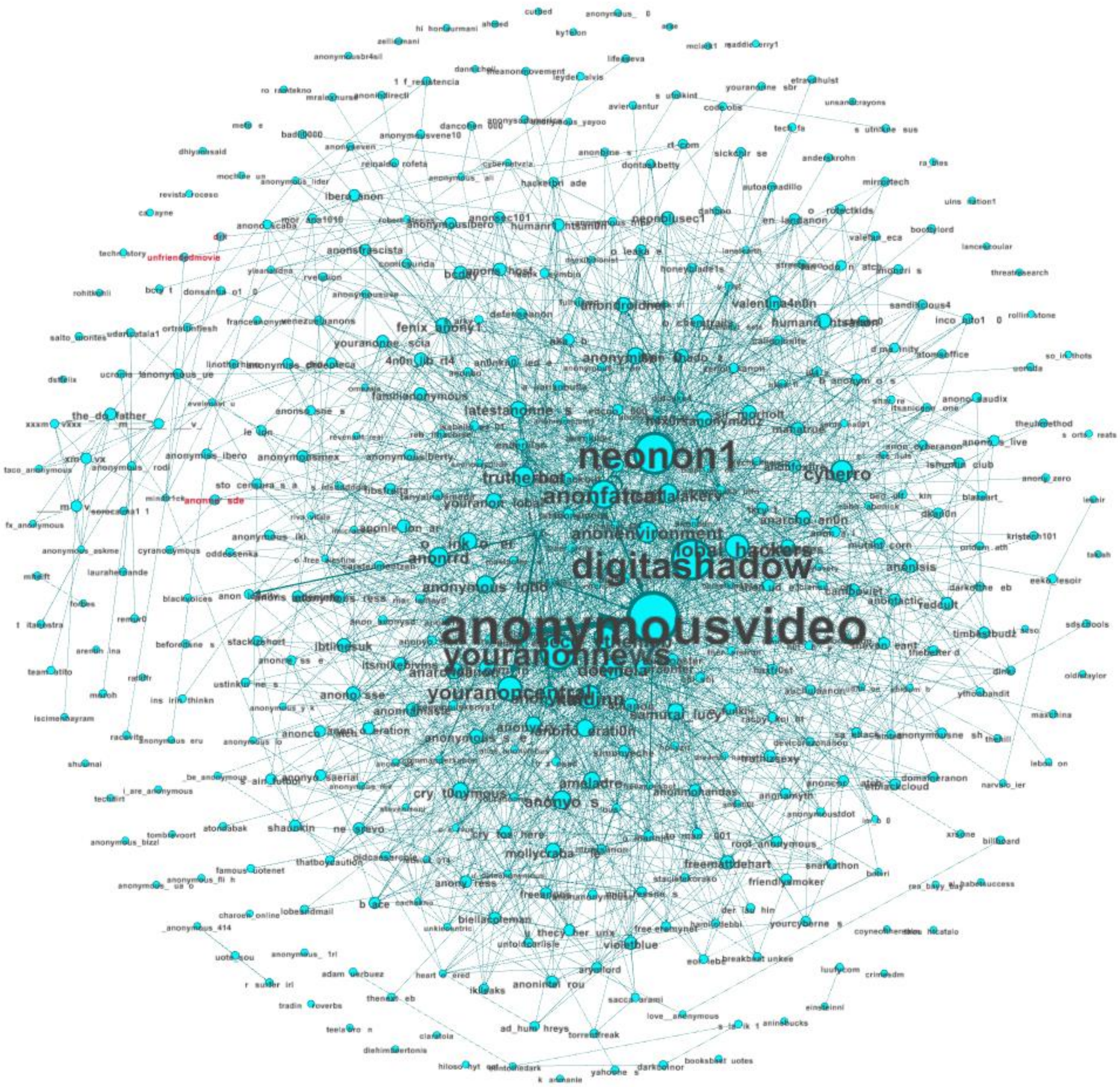

Figura 20 – Rede de Grafos dos Retweets do termo "Anonymous" no Twitter.

De maneira semelhante, as autoridades da rede de retweets seguem o mesmo padrão. Destaca-se o perfil "anonymousvideo", especializado em divulgar vídeos relacionados aos temas do grupo. O fato desse perfil ser a principal autoridade na rede de retweets indica a importância do conteúdo audiovisual na divulgação do grupo, criando muito mais engajamento que o conteúdo unicamente textual.

Quadro 6 – Autoridades nos retweets ao termo "Anonymous".

Perfis	Autoridade
Anonymousvideo	0,035
Youranonnews	0,033
neonon1	0,031
Digitashadow	0,031
anonfatcat	0,028

4.4.2.3 Antivigilância

A oficina e o boletim antivigilância, conforme apresentado no capítulo anterior, surgem como um polo de distribuição de conteúdo e debate no ativismo da internet. Porém, o volume de citações diretas ao tema é bem inferior quando comparado aos outros termos pesquisados. Mesmo assim, é possível mapear os principais e autoridades envolvidos na divulgação e debate dos temas antivigilância.

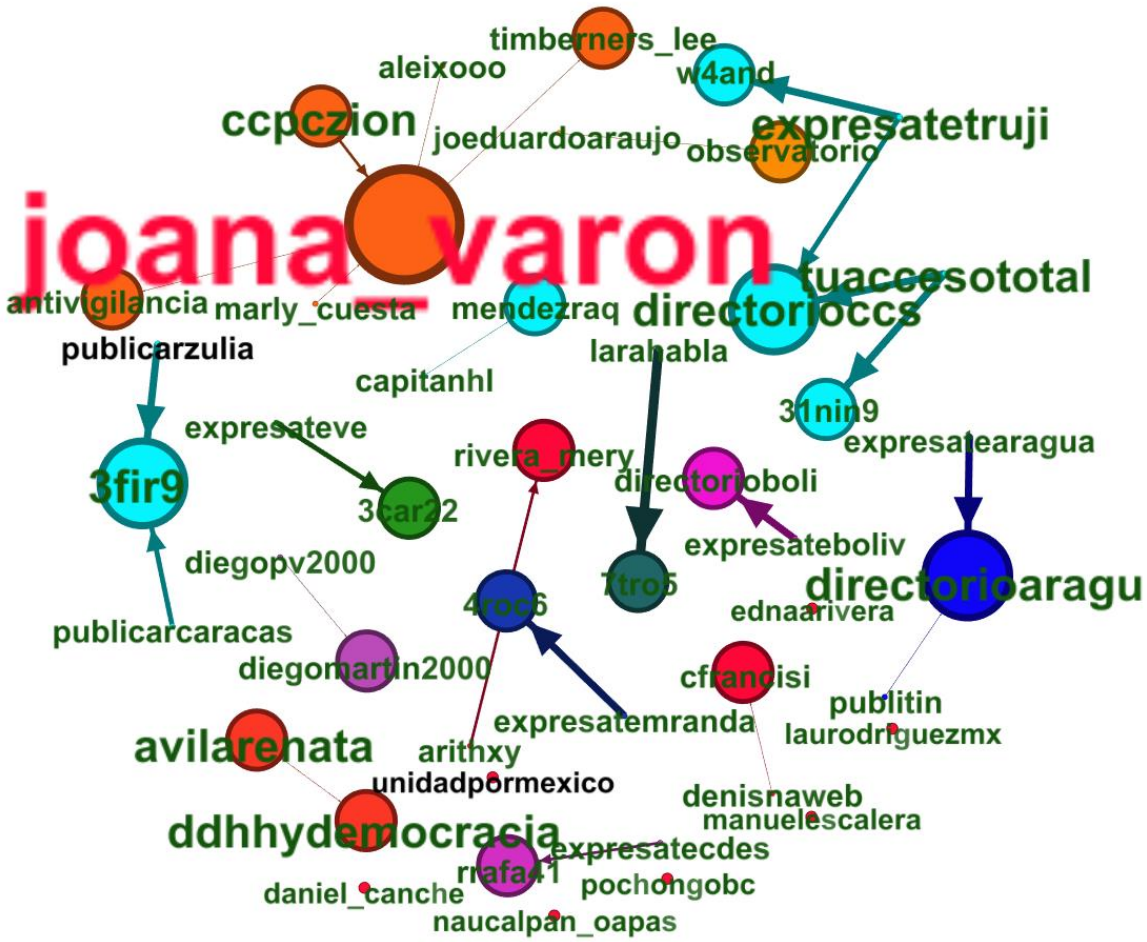

Figura 21 – Rede de Grafos das menções ao termo "Antivigilância" no Twitter.

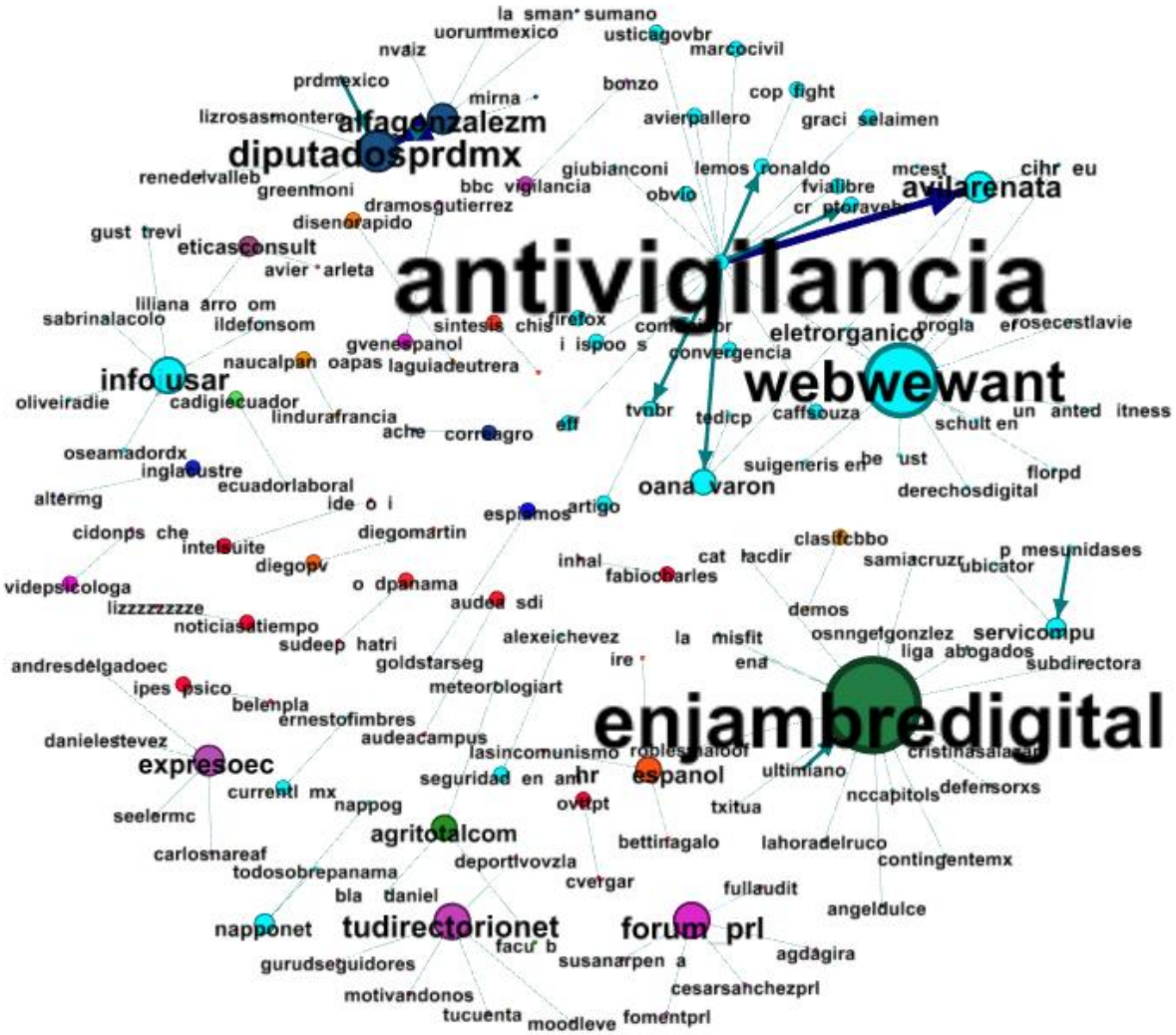

Figura 22 – Rede de Grafos dos retweets do termo "Antivigilância" no Twitter.

O perfil oficial da campanha global "web we want" (web que queremos) surge como principal autoridade na rede, seguido pelo perfil da advogada e ativista guatemalteca Renata Avila. Destaca-se também a ativista brasileira Joana Varon, colaboradora do boletim antivigilância. A análise dos grafos formados a partir do termo "antivigilância" sugere a formação de um pequeno cluster em torno do tema, isto é, um grupo de perfis que debate mais entre si do que com outros grupos. O pequeno alcance do debate parece confirmar essa hipótese.

Quadro 7 – Autoridades nos retweets ao termo "Antivilância".

Perfis	Autoridade
Webwewant	0,121
Avilarenata	0,047
Agritotalcom	0,037
joana_varon	0,037
cryptoravebr	0,019
Antivigilancia	0,019

4.4.2.4 Assange

O ativista Julian Assange tem sido o rosto do movimento cypherpunks e do ativismo da internet de maneira geral. Por essa razão, a pesquisa por citações ao seu nome é uma tentativa de captar algumas nuances do debate, ou ainda, expandir percepções já captadas. Para isso, utilizou-se o filtro com valores: 5 (mínimo) e 243 (máximo) para as menções; e 12 (mínimo) e 2312 (máximo) para os retweets.

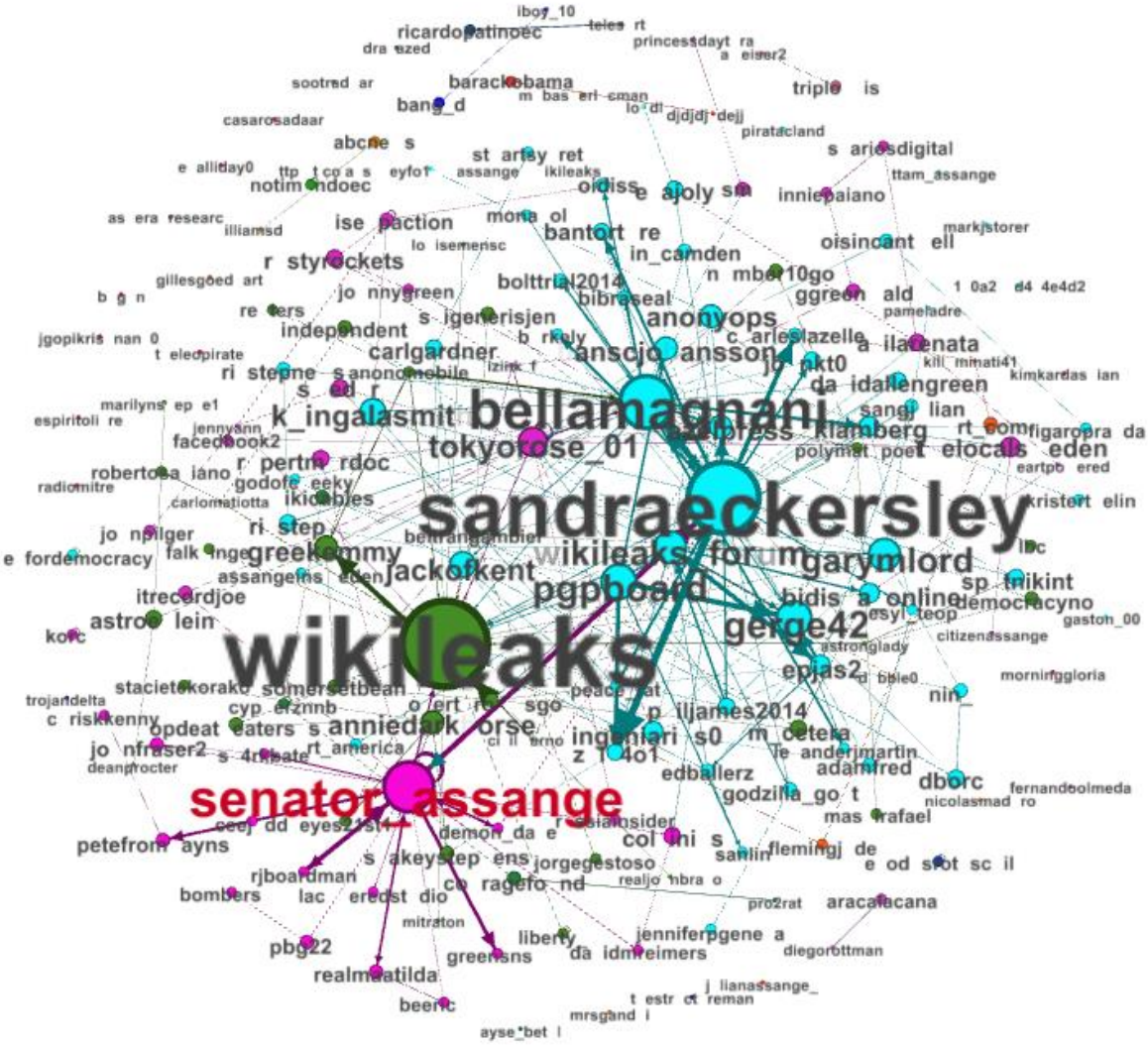

Figura 23 – Rede de Grafos das menções ao termo “Assange” no Twitter.

Quadro 8 – Autoridades nas menções ao termo “Assange”.

Perfis	Autoridade
Wikileaks	0,058
Sandraeckersley	0,048
Bellamagnani	0,035
senator_assange	0,032
gerge42	0,022

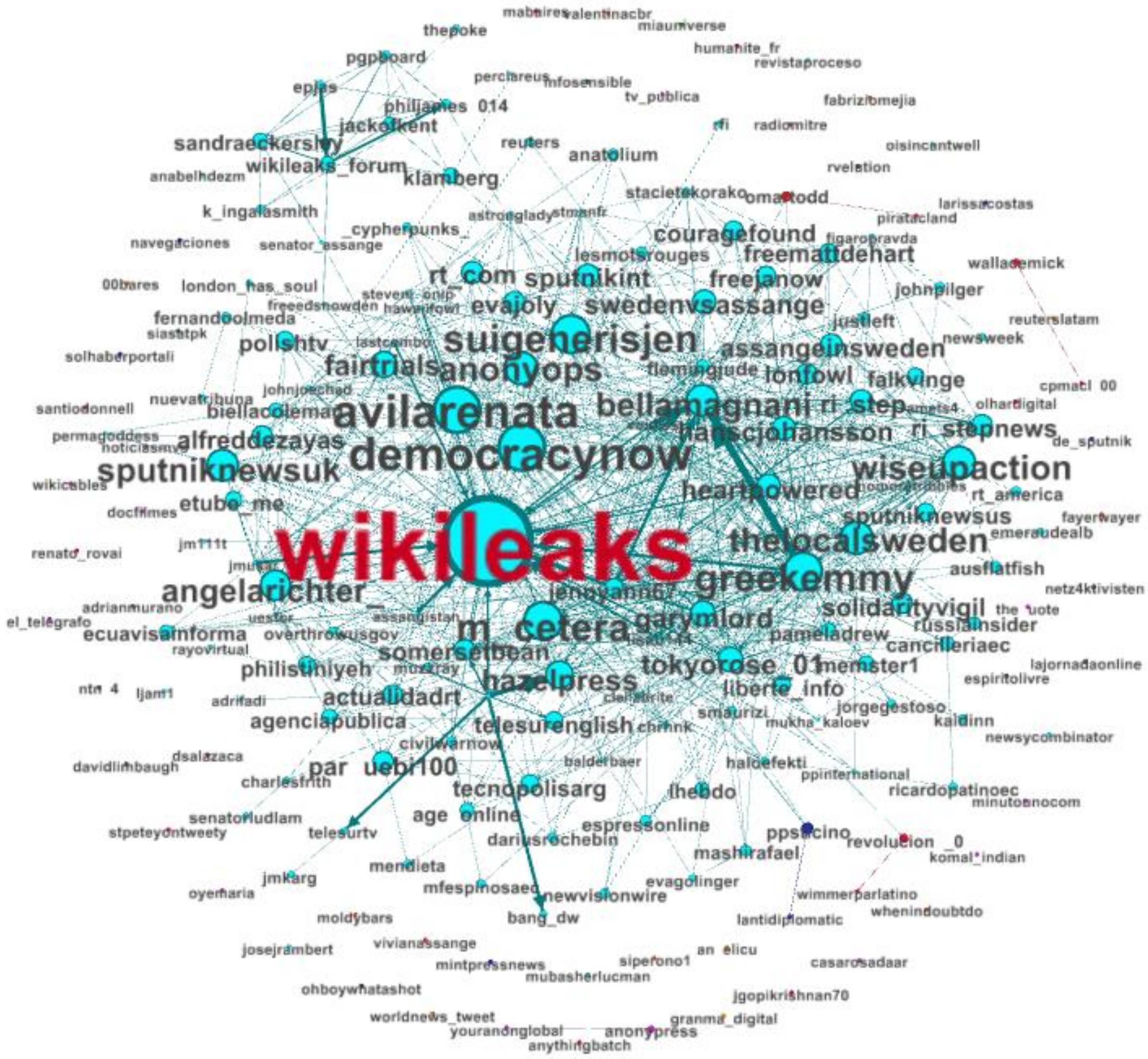

Figura 24 – Rede de Grafos dos retweets do termo “Assange” no Twitter.

Quadro 9 – Autoridades nos retweets ao termo “Assange”.

Perfis	**Autoridade**
Wikileaks	0,065
Avilarenata	0,033
Democracynow	0,033
Greekemmy	0,027
suigenerisjen	0,027

A análise não apresenta surpresas e confirma a autoridade dos perfis oficiais do Wikileaks. Destaca-se mais uma vez a ativista Renata Avila e o perfil “Democracy Now”, jornal independente transmitido diariamente pela internet e financiado por meio de doações dos seguidores.

4.4.2.5 Ciberativistas

Para a confecção dos grafos sobre ciberativistas, optou-se por uma metodologia um pouco diferente. Por meio de levantamento bibliográfico, participações em eventos e citações recorrentes, criou-se uma lista com os principais ciberativistas brasileiros. Além disso, foram incluídos os principais expoentes globais do ativismo cypherpunks como Jacob Applebaum (@ioerror) e Jérémie Zimmermann (@jerezim), além de Peter Sunde (@brokep), fundador do site de compartilhamento de conteúdo Pirate Bay, e Glenn Greenwald (@ggreenwald), jornalista e ativista responsável pela publicação dos documentos de Edward Snowden.

Para a seleção dos ativistas, foram utilizados os seguintes critérios: 1) participação ativa no Twitter; 2) relevância acadêmica; 3) participação em palestras e debates em eventos sobre internet, como cryptorave ou Campus Party. Dessa forma, chegou-se a seguinte lista: Bernardo Gutiérrez (@bernardosampa) jornalista e pesquisador; Diego Aranha (@dfaranha) criptógrafo; Henrique Parra (@henrique_parra) pesquisador; Joana Varon (@joana_varon) pesquisadora e ativista; Lucas Teixeira (@eletrorganico) ativista; Marcelo Branco (@MarceloBranco) ativista; Mídia Ninja (@midiaNINJA) coletivo de jornalismo independente; Pablo Ortellado (@pablo_ortellado) pesquisador; Paulo Rená (@prenass) ativista; Ronaldo Lemos (@lemos_ronaldo) advogado e colunista; Sergio Amadeu (@samadeu) pesquisador.

Após selecionar os principais ativistas, o software de busca capturou os tweets de seus perfis. Em seguida, os tweets foram reunidos em um único arquivo, que passou pelo processamento no software R. Dessa forma, foi possível identificar as interações entre os ativistas e ainda apontar para outros nós relevantes que não estavam incluídos na lista inicial. Por exemplo, ativistas como Renata Avila surgiram na rede como nós importantes.

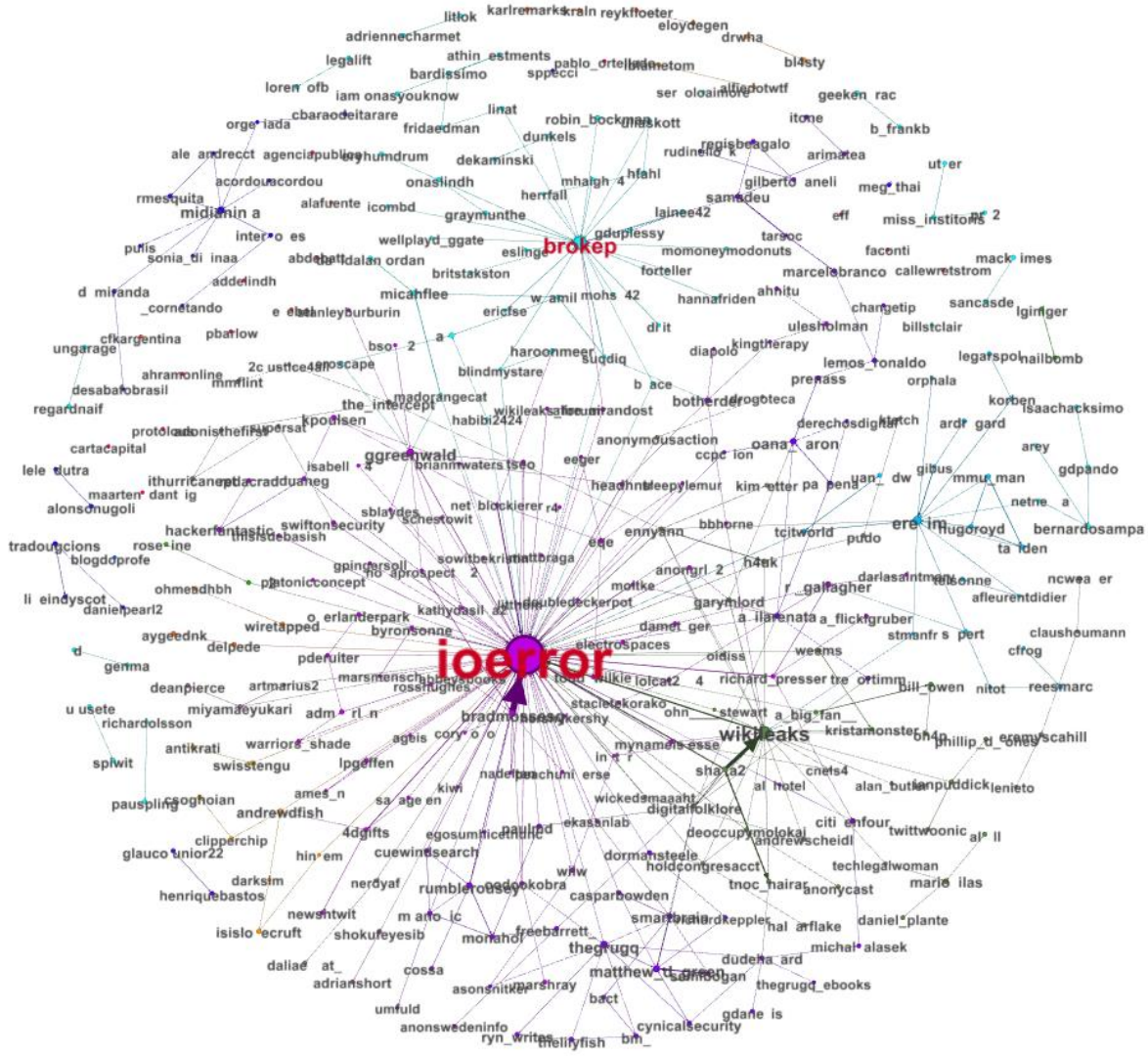

Figura 25 – Rede de Grafos das menções aos principais ciberativistas do Twitter.

Quadro 10 – Autoridades na rede de grafos dos principais ciberativistas.

Perfis	Autoridade
Ioerror	0,184
Brokep	0,108
Jerezim	0,043
wikileaks	0,027
midianinja	0,027
lemos_ronaldo	0,017
samadeu	0,015
ggreenwald	0,015
bradmossesq	0,010
bernardosampa	0,008
rj_gallagher	0,007
thegrugq	0,007
matthew_d_green	0,007

prenass	0,006
joana_varon	0,006
Botherder	0,006
Marcelobranco	0,006
Avilarenata	0,005
Andrewdfish	0,005
Swiftonsecurity	0,005
pablo_ortellado	0,005

.

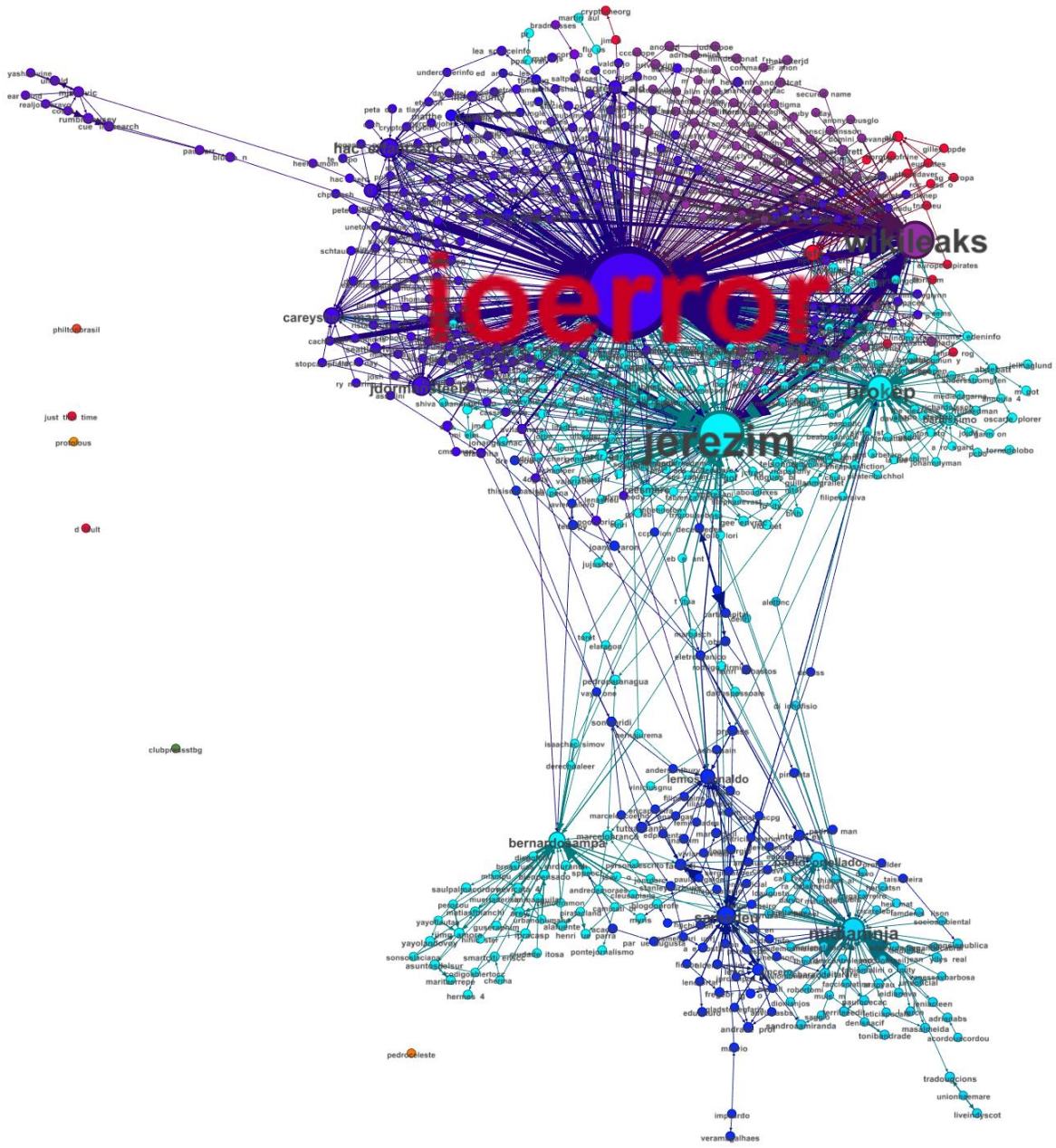

Figura 26 – Rede de Grafos dos retweets dos principais ciberativistas do Twitter.

Quadro 11 – Autoridades na rede de grafos do retweets dos principais ciberativistas.

Perfis	Autoridade
ioerror	0,202
jerezim	0,092
wikileaks	0,070
brokep	0,042
Midianinja	0,035
hackerfantastic	0,025
samadeu	0,025
jdormansteele	0,025
bernardosampa	0,019
careyshenkman	0,018
fsfe	0,017
pablo_ortellado	0,015
lemos_ronaldo	0,014
wilw	0,012
ggreenwald	0,011
reesmarc	0,009
bardissimo	0,009
jennyann67	0,006
casparbowden	0,006
68ardr1gard	0,006
lenoxx_sincero	0,006

Para a visualização dos grafos dos retweets, optou-se pela distribuição “Force Atlas”. Com isso, ficam evidentes os grupos formados em torno dos perfis e suas ligações. Além disso, reforça a visualização e presença do grupo de ativistas brasileiros. Obviamente, ativistas mundialmente conhecidos são os principais polos de distribuição de conteúdo. No entanto, a visualização dos clusters e os dados dos números de autoridade demonstram a relevância do ativismo brasileiro em comparação ao global. O coletivo Mídia Ninja e os pesquisadores Sérgio Amadeu e Bernardo Gutiérrez estão entre as dez maiores autoridades na rede de grafos formadas com os dados coletados. Além disso, vale destacar o peso na rede dos pesquisadores Pablo Ortellado e Ronaldo Lemos.

4.4.2.6 Criptografia

A rede de grafos do termo cartografia se demonstrou bastante dispersa para as menções. Poucos perfis conseguiram uma concentração maior de menções e autoridade na

rede. O destaca são as menções ao perfil "@telegram_br", aplicativo de mensagens instantâneas criptografadas.

Já em relação aos retweets, uma dinâmica nova e interessante pode ser notada. Nenhum grupo ativista ou de mídia independente aparece como autoridade no debate. Pelo contrário, o debate é pautado pelos perfis de grupos de comunicação tradicional ou seus cadernos e sites dedicados a tecnologia. Por essa razão, aparecem "@estadao" do Grupo Estadão, "@olhardigital" ligado ao grupo UOL, "@_info" revista do grupo Abril. Em contrapartida, destacam-se como autoridade o Observatório da Imprensa (@observatorio) e o perfil do pesquisador Sérgio Amadeu da Silveira (@samadeu).

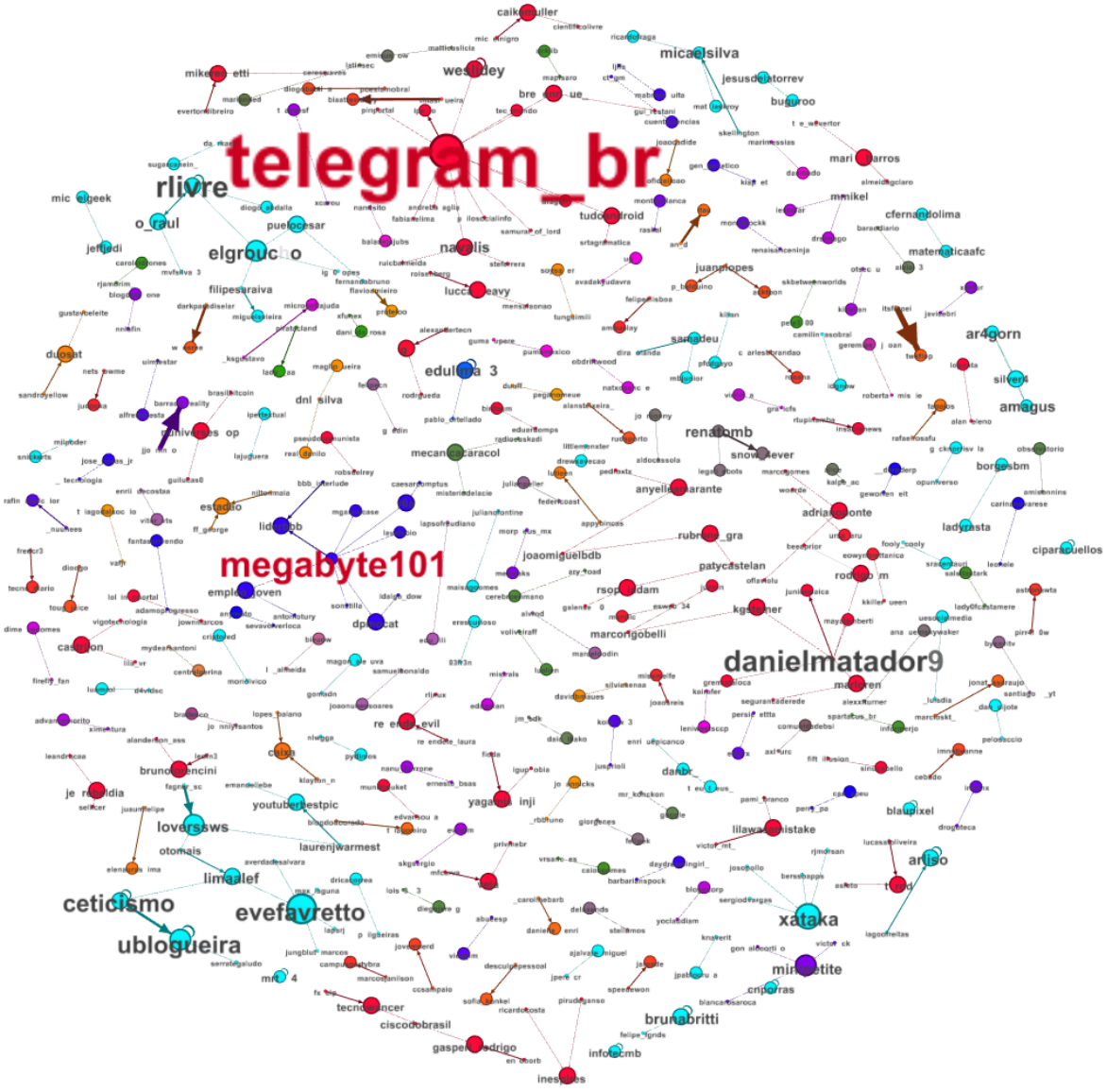

Figura 27 – Rede de Grafos das menções ao termo "Criptografia" no Twitter.

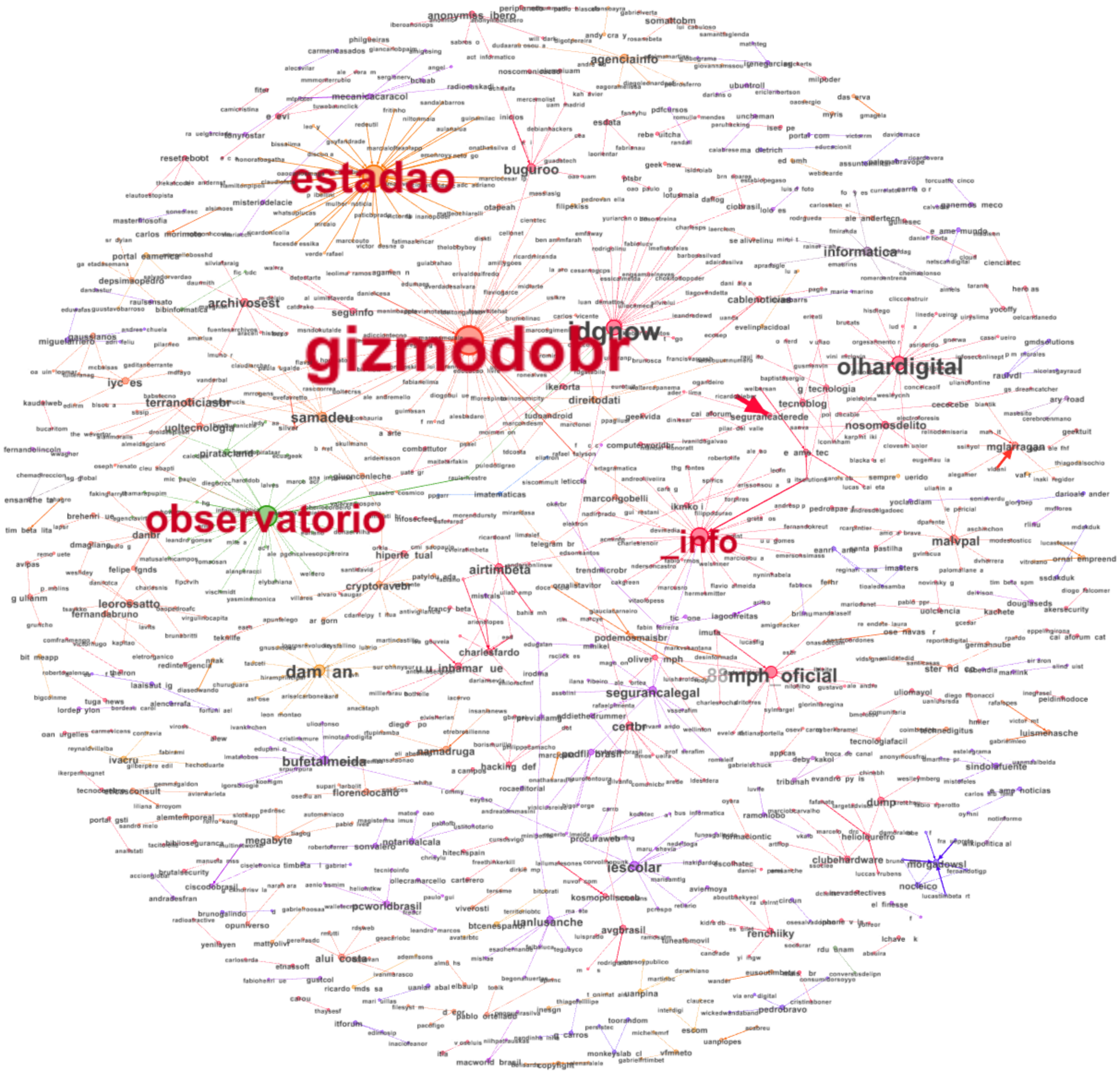

Figura 28 – Rede de Grafos dos retweets do termo "Criptografia" no Twitter.

Quadro 12 – Autoridades na rede de grafos do retweets do termo "criptografia".

Perfis	Autoridade
gizmodobr	0,046
estadao	0,035
Observatório	0,032
Info	0,027
Idgnow	0,022
olhardigital	0,020
Samadeu	0,011

4.4.2.7 Cryptoparty

Seguindo o padrão observado até agora, a visualização dos grafos das menções é bastante disperso. O principal destaque é o perfil do senador australiano Scott Ludlam. Essa tendência é confirmada nos grafos dos retweets sobre a criptoparty. Os retweets se concentram em torno de três autoridades: @senatorludlam, @ cryptopartybln e @ cryptopartyec. Por essa razão, optou-se pela distribuição "Force Atlas" com o objetivo de destacar os clusters formados.

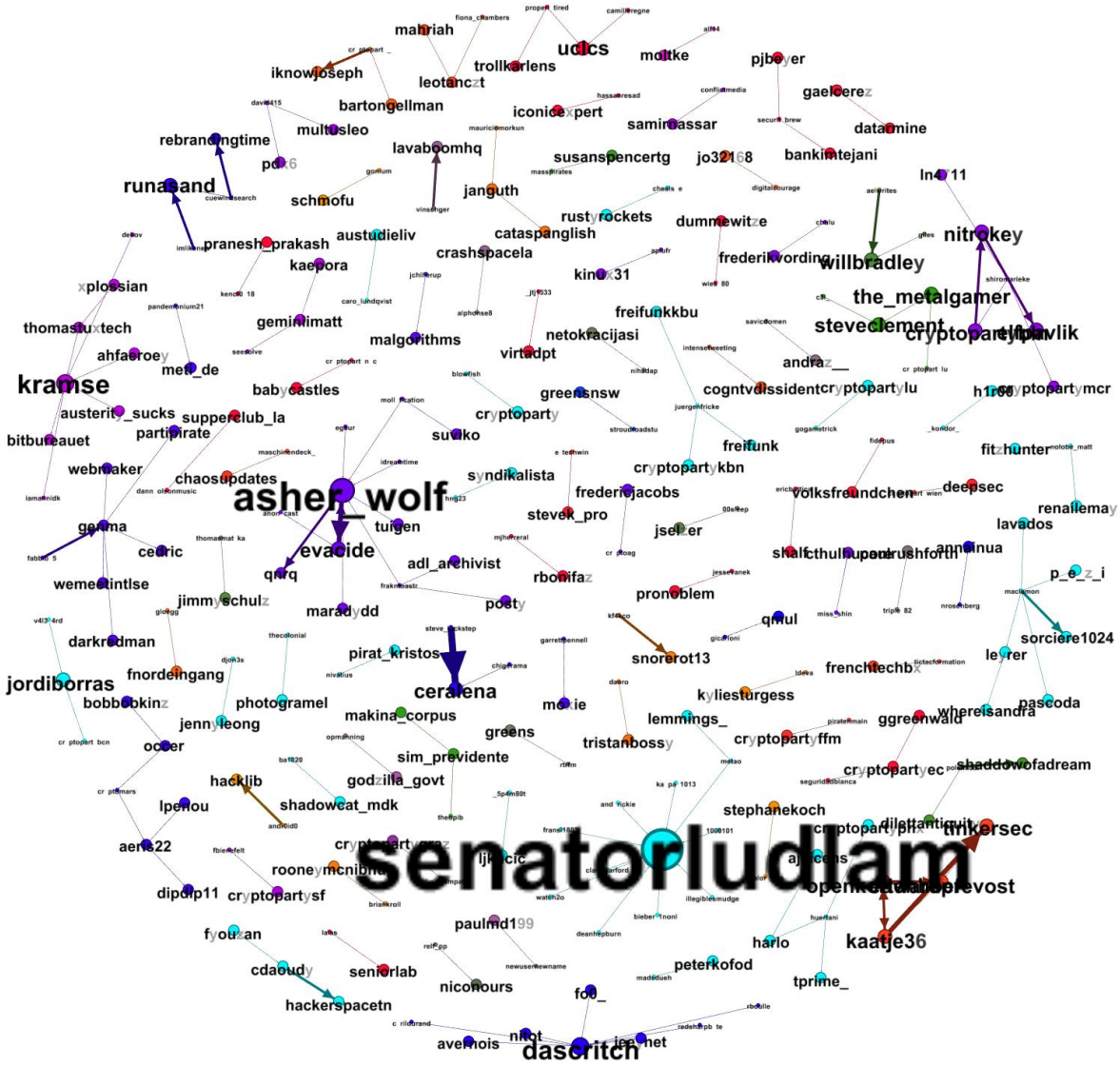

Figura 29 – Rede de Grafos das menções ao termo "Cryptoparty" no Twitter.

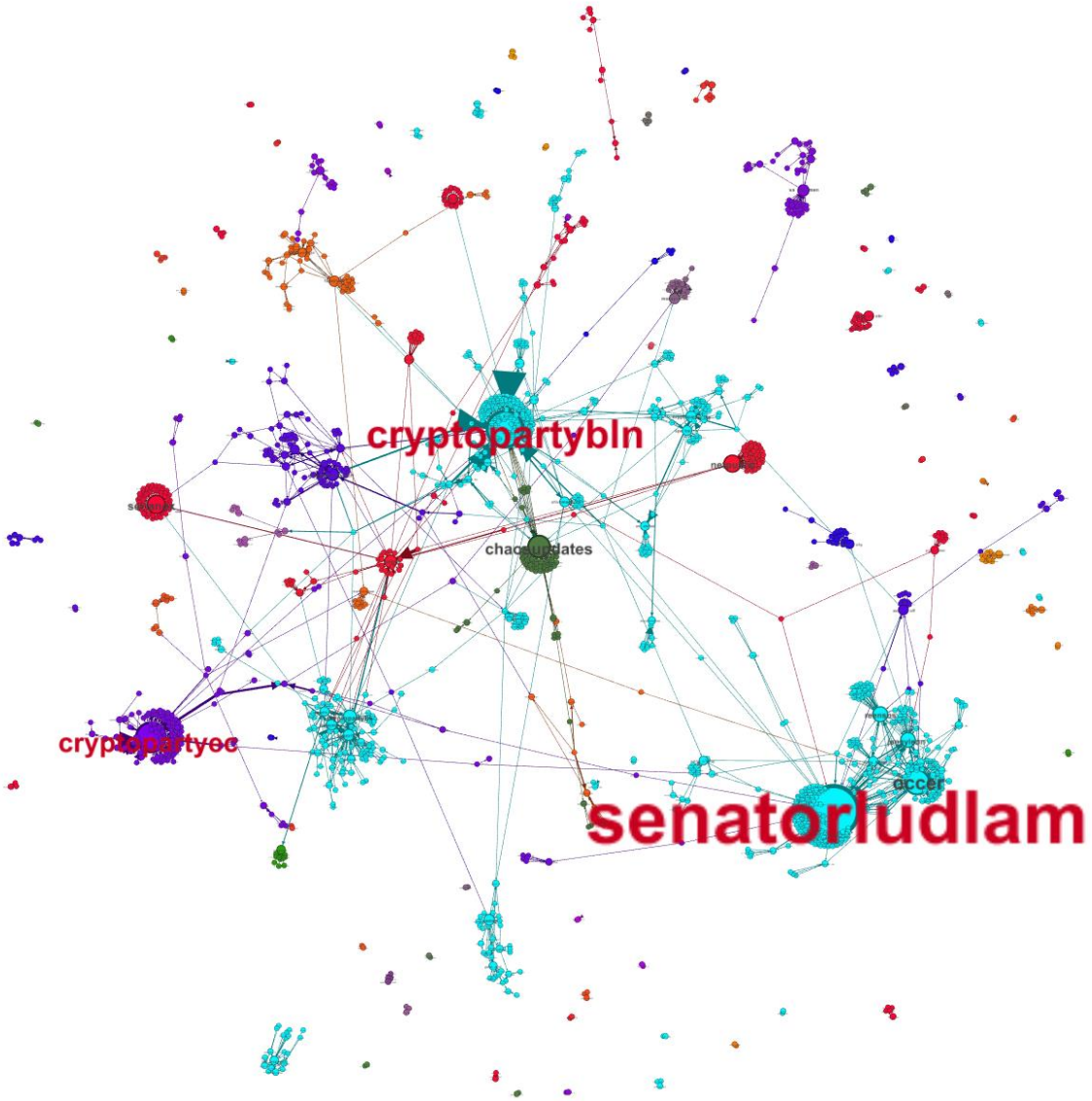

Figura 30 – Rede de Grafos dos retweets do termo “Cryptoparty” no Twitter.

Quadro 13 – Autoridades nos retweets do termo “Cryptoparty”.

Perfis	Autoridade
Senatorludlam	0,074
cryptopartybln	0,051
cryptopartyec	0,040
occer	0,032
Chaosupdates	0,028
cryptoravebr	0,008

As três principais autoridades concentram em torno de si a maioria dos retweets captados com o termo “cryptoparty”. Em primeiro lugar, o senador australiano do partido

"Greens[63]" que ao longo de sua carreira tem se dedicado a temas como liberdades individuais e proteção ambiental. Em seguida os perfis das cryptoparties de Berlim e do Ecuador, demonstrando o caráter internacional do evento e a troca de experiência entre os ativistas. A proeminência da cryptoparty de Berlim é explicada pelo perfil do Chaos Computer Club[64] (@Chaosupdates), um dos maiores coletivos de hackers da Europa. A criptoparty brasileira aparece com um peso menor na rede.

4.4.2.8 Cryptorave

As principais menções ao termo "cryptorave" captadas pela mineração giram em torno do perfil homônimo. No entanto, o perfil oferece pouca informação relevante para a presente pesquisa. Esse fato chama a atenção para as possíveis ambiguidades ou redundâncias que a busca automática de conteúdo pode gerar, cabendo sempre ao pesquisador a tarefa final de análise e teorização. Mesmo assim, o algoritmo de modularidade, que identifica comunidades, aponta por meio da cor vermelha os perfis: @criptoravebr, @brokep e @samadeu. Estes sim envolvidos com o debate sobre privacidade.

---

[63] "The Australian Greens, commonly known as The Greens, is an Australian green political party. The party was formed in 1992 and is today a confederation of eight state and territory parties. Other than environmentalism the party cites four core values: ecological sustainability, social justice, grassroots democracy and peace and non-violence." Disponível em: http://en.wikipedia.org/wiki/Australian_Greens (Acesso: 20/02/2015).

[64] "Chaos Computer Club (abbreviated as CCC) was founded in 1981 and is one of the longest established and most influential civil society organisations dealing with the security and privacy aspects of technology in the German-speaking world. Organized in 25 so-called "Erfakreisen" (regional hackerspaces) and even more smaller "Chaostreffs", CCC hackers work decentralized. We are a non-profit association and have about 5,500 members." Disponível em: http://ccc.de/ (Acesso 20/02/2015).

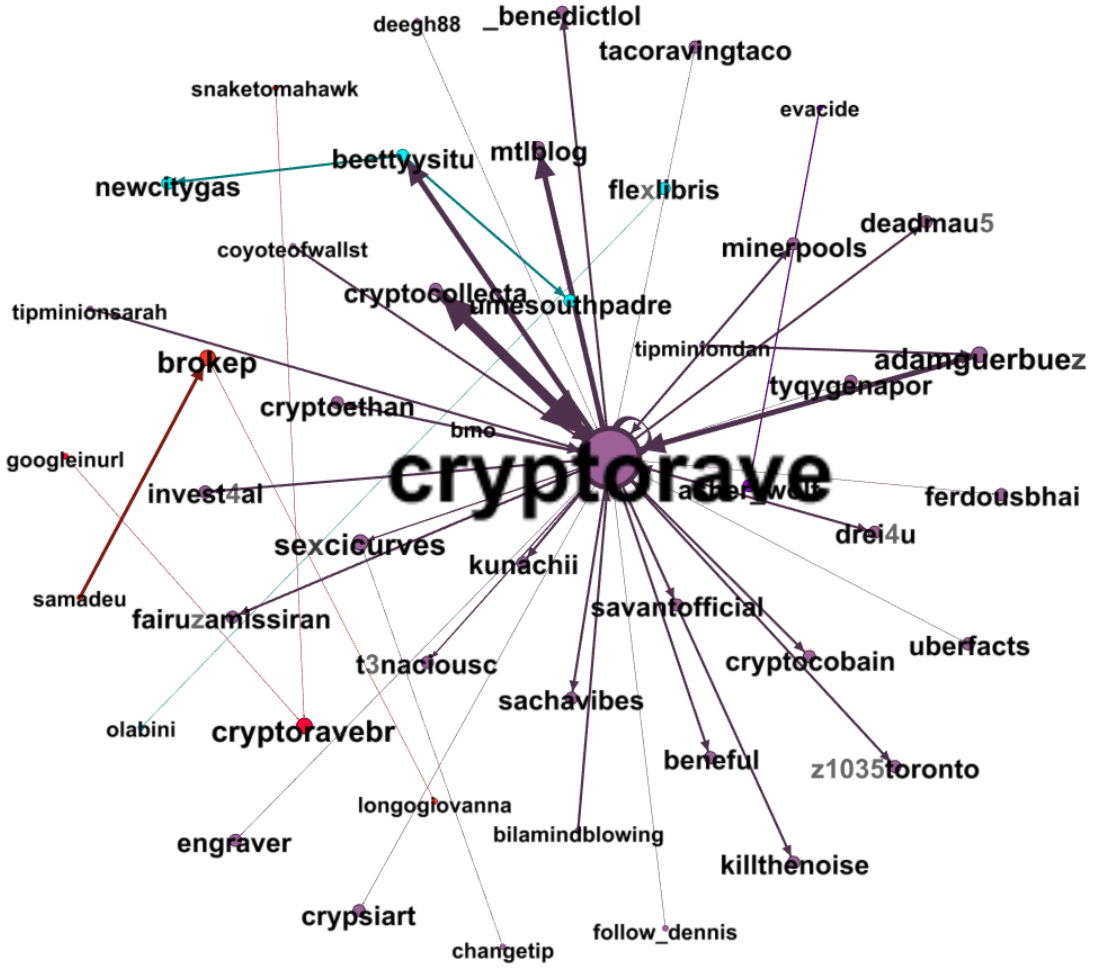

Figura 31 – Rede de Grafos das menções ao termo "Cryptorave" no Twitter.

Os grafos dos retweets demonstraram-se mais elucidativos em relação ao debate sobre privacidade e criptografia. A principal autoridade encontrada é o perfil oficial da Electronic Frotier Foundation[65] (@eff), organização pioneira na defesa da liberdade de expressão e privacidade na rede. Em seguida o perfil da Cryptorave brasileira, criada em 2014, que segundo os próprios ativistas é o maior evento de tipo no mundo. As outras autoridades da

[65] "The Electronic Frontier Foundation is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. We work to ensure that rights and freedoms are enhanced and protected as our use of technology grows". Disponível em: https://www.eff.org/about (acesso em: 20/02/2015).

rede são perfis ativistas, como Pedro Ekaman (@pedroekman) do coletivo Intervozes[66] e o vídeo-ativista Rafucko[67] (@rafucko).

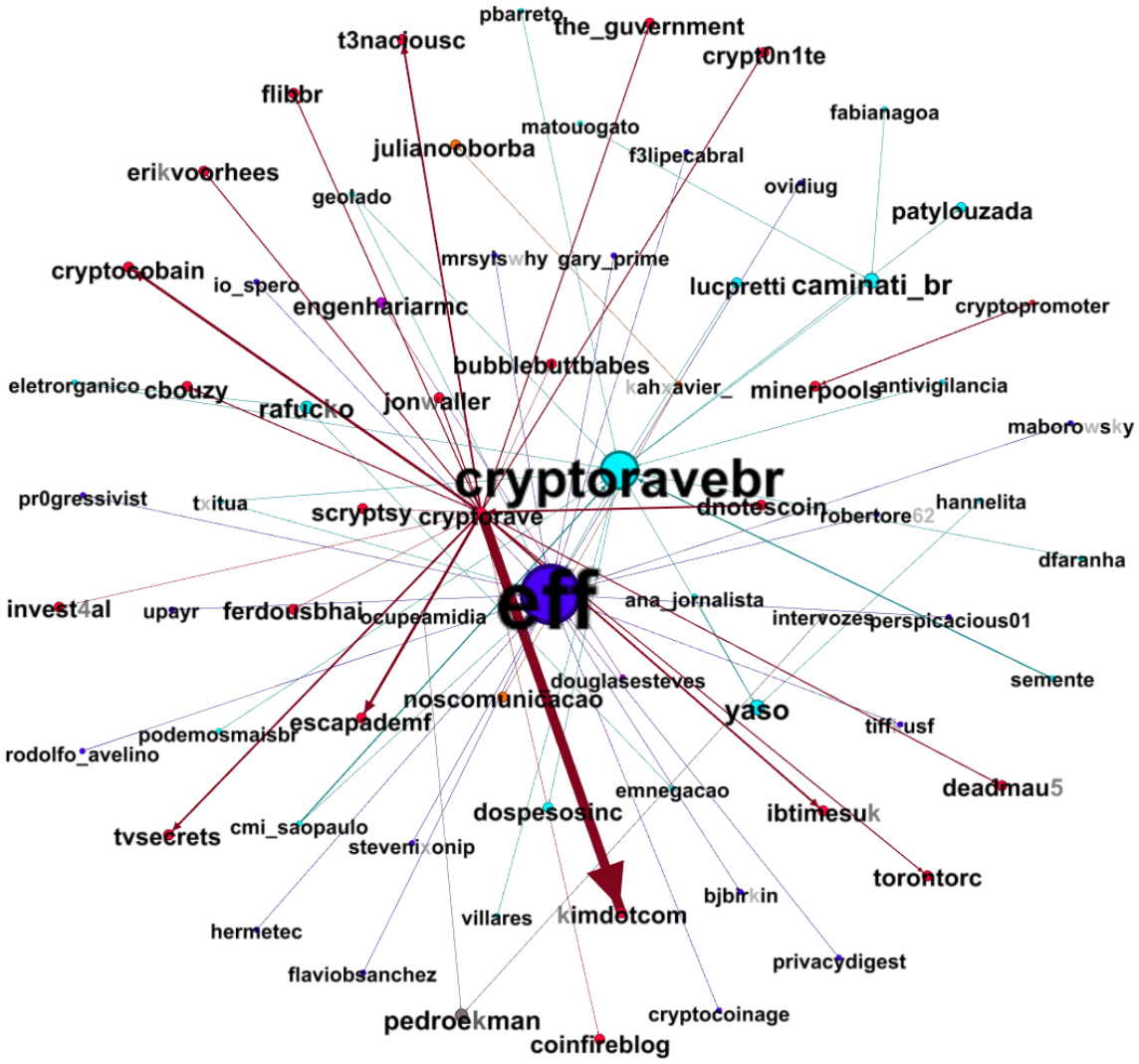

Figura 32 – Rede de Grafos dos retweets do termo "Cryptorave" no Twitter.

Quadro 14 – Autoridades nos retweets do termo "Cryptorave".

Perfis	Autoridade
eff	0,215
cryptoravebr	0,131
yaso	0,037
caminati_br	0,037
pedroekman	0,028
rafucko	0,028

[66] http://intervozes.org.br/
[67] http://rafucko.com/

4.4.2.9 Cypherpunk

De maneira semelhante a busca por “cryptorave”, a principal autoridade encontrada na busca por “cypherpunk” é um perfil pessoa sem informações relevantes para a pesquisa. Novamente, os grafos dos retweets são mais ilustrativos e apontam para os perfis que pautam o debate.

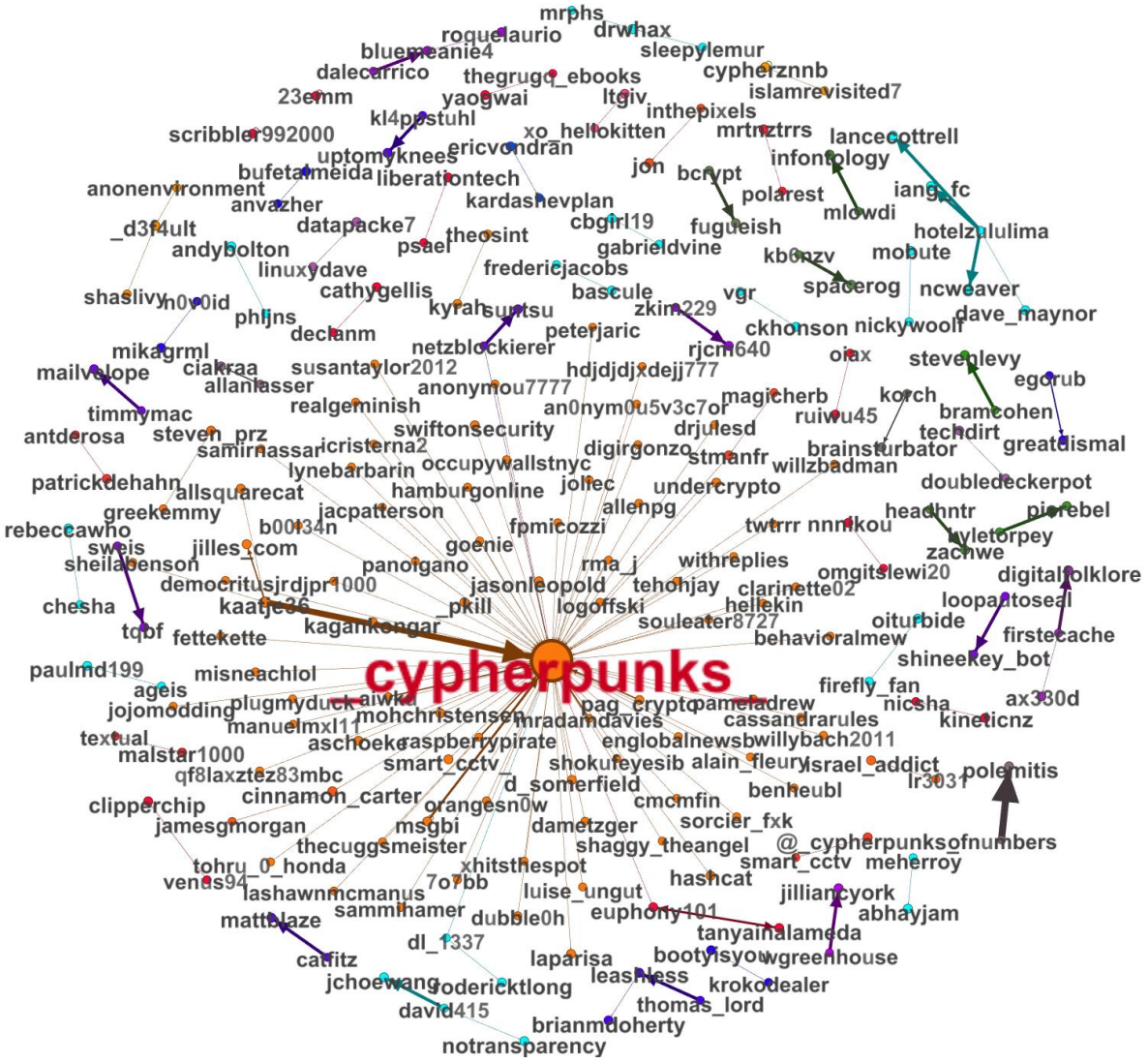

Figura 33 – Rede de Grafos das menções ao termo “Cypherpunk” no Twitter.

A principal autoridade na rede é o perfil @_d3f4ult, relacionado a questões de privacidade na internet e a ataques coordenados com o “Anonymous”, como por exemplo instruções para ataques a determinados alvos. Em segundo lugar, o perfil @_cypherpunks_ apresenta semelhanças com o anterior, porém com mais seguidores e um blog próprio para a

postagem de conteúdo. Os outros perfis principais pertencem a ativistas e simpatizantes das ideias cypherpunks.

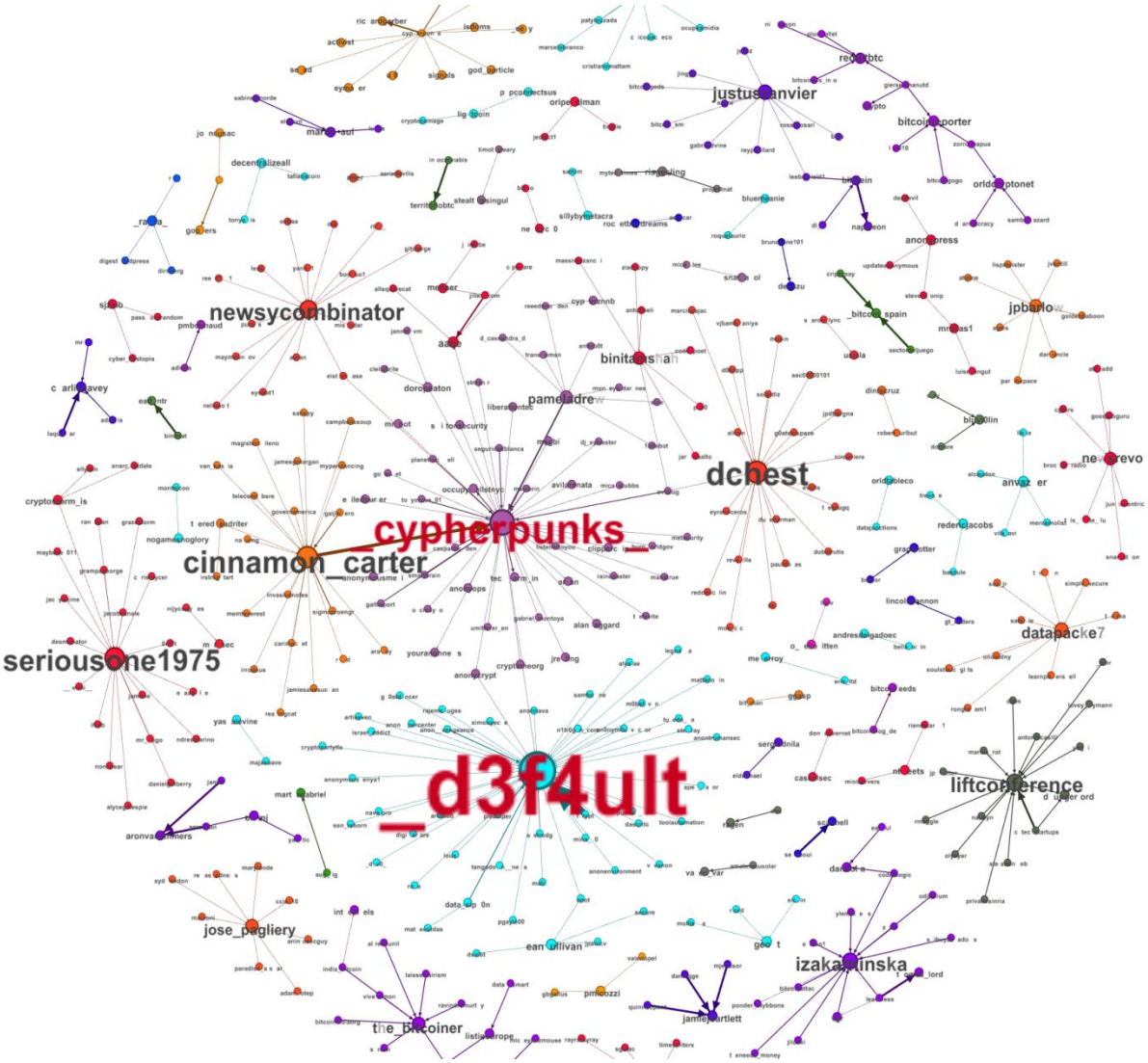

Figura 34 – Rede de Grafos de retweets do termo “Cypherpunk” no Twitter.

Quadro 15 – Autoridades no retweets do termo “Cypherpunk”.

Perfis	Autoridade
_d3f4ult	0,087
cypherpunks	0,052
dchest	0,042
cinnamon_carter	0,040
seriousone1975	0,038

4.4.2.10 Neutralidade

Seguindo o padrão já observado, os grafos das menções ao termo "neutralidade" é pouco explicativo. Vale destacar o perfil de Flávia Lefevre (@flavialefevre), representante do terceiro no Comitê de Gestão da Internet, e o de Danilo Gentili (@danilogentili), humorista que fez críticas a proposta de neutralidade do Marco Civil.

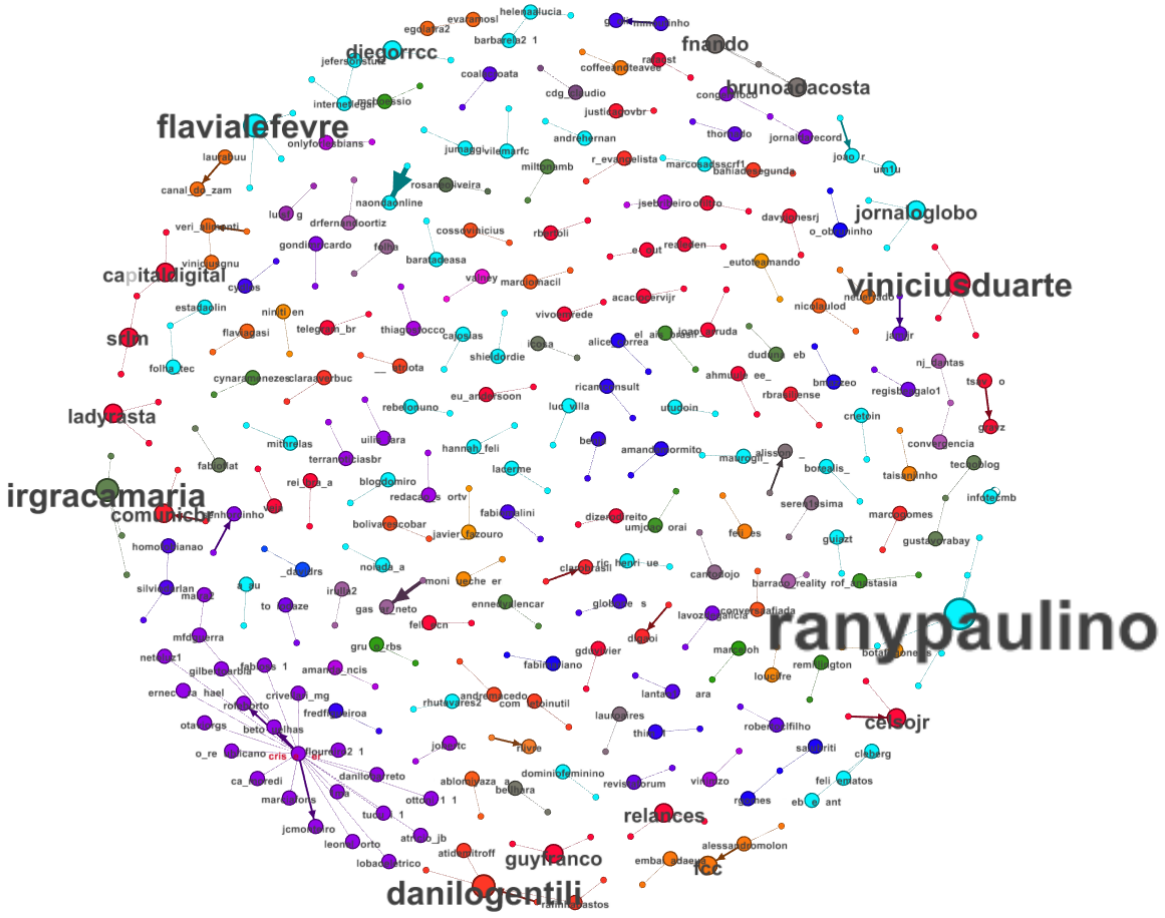

Figura 35 – Rede de Grafos das menções ao termo "Neutralidade" no Twitter.

Já os grafos dos retweets apontaram para algumas autoridades. Em primeiro lugar, o perfil de Thomas Conti (@_thomasconti), pesquisador da UNICAMP. Em seguida, Tiago Soares[68] (@Elgroucho) e Cardoso[69] (@cardoso), ambos blogueiros. Destaca-se ainda a presença de um veículo de mídia tradicional, Carta Capital (@cartacapital), e o blog do

[68] http://www.oplanob.org/
[69] http://contraditorium.com/

jornalista Paulo Henrique Amorim, (@conversaafiada), da base de apoio virtual dos governos petistas.

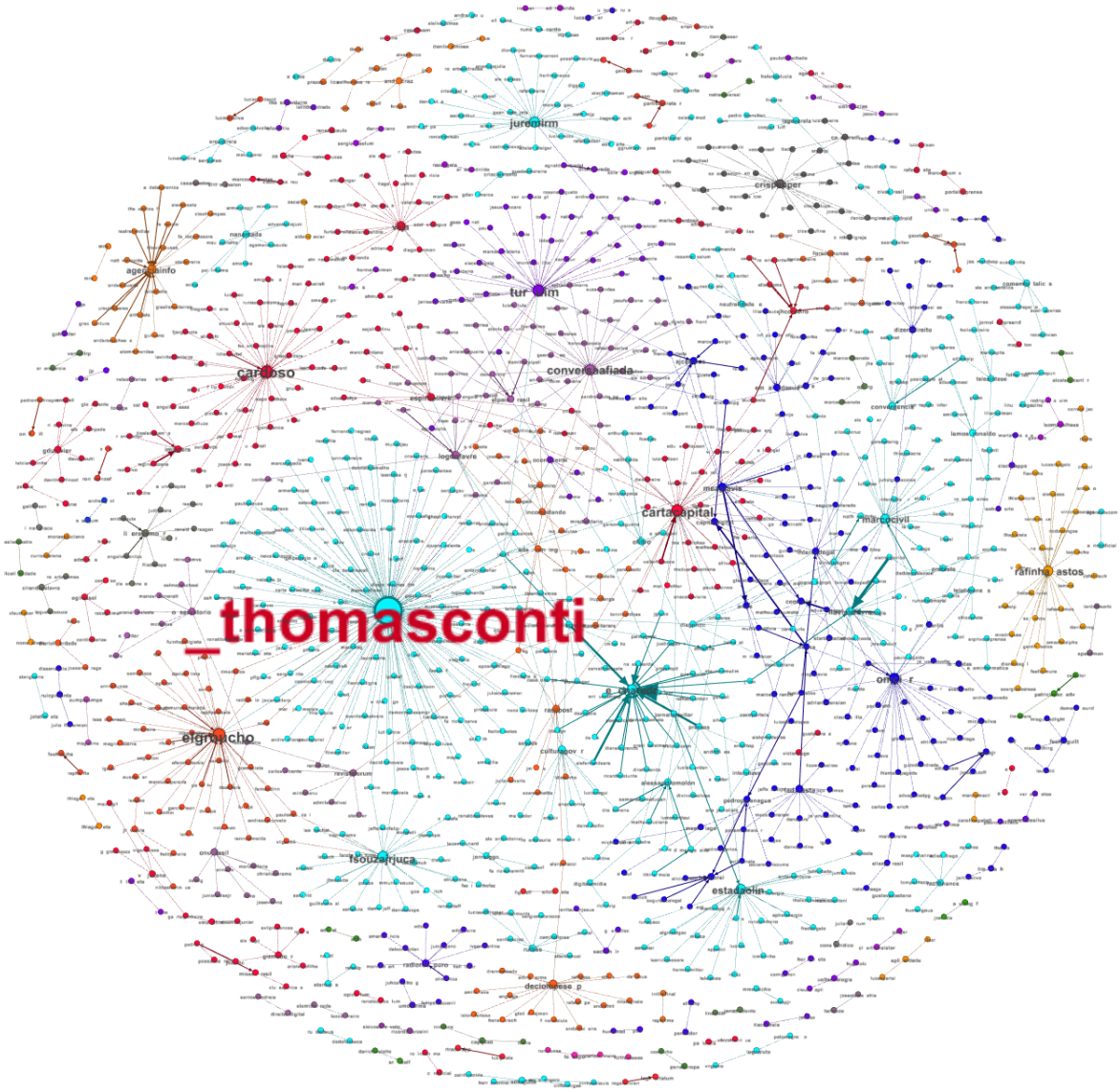

Figura 36 – Rede de Grafos de retweets do termo “Neutralidade” no Twitter.

Quadro 16 – Autoridades nos retweets do termo “Neutralidade”.

Perfis	Autoridade
_thomasconti	0,101
Elgroucho	0,030
Cardoso	0,030
turquim5	0,026
Cartacapital	0,025
Conversaafiada	0,022

4.4.2.11 Partido Pirata

Os dois perfis do Partido Pirata concentram as principais menções, conforme os grafos abaixo. Vale destaca que o perfil @partidopiratabr pertence a organização no Brasil, enquanto @partido_pirata pertence aos piratas da Espanha. Aqui, mais uma vez, palavras cognatas entram nas buscas e aparecem nos resultados finais. Nesse caso, por se tratar de uma organização que opera como uma rede internacional, o fato não chega a comprometer a análise, apontando para as relações entre coletivos de dois países.

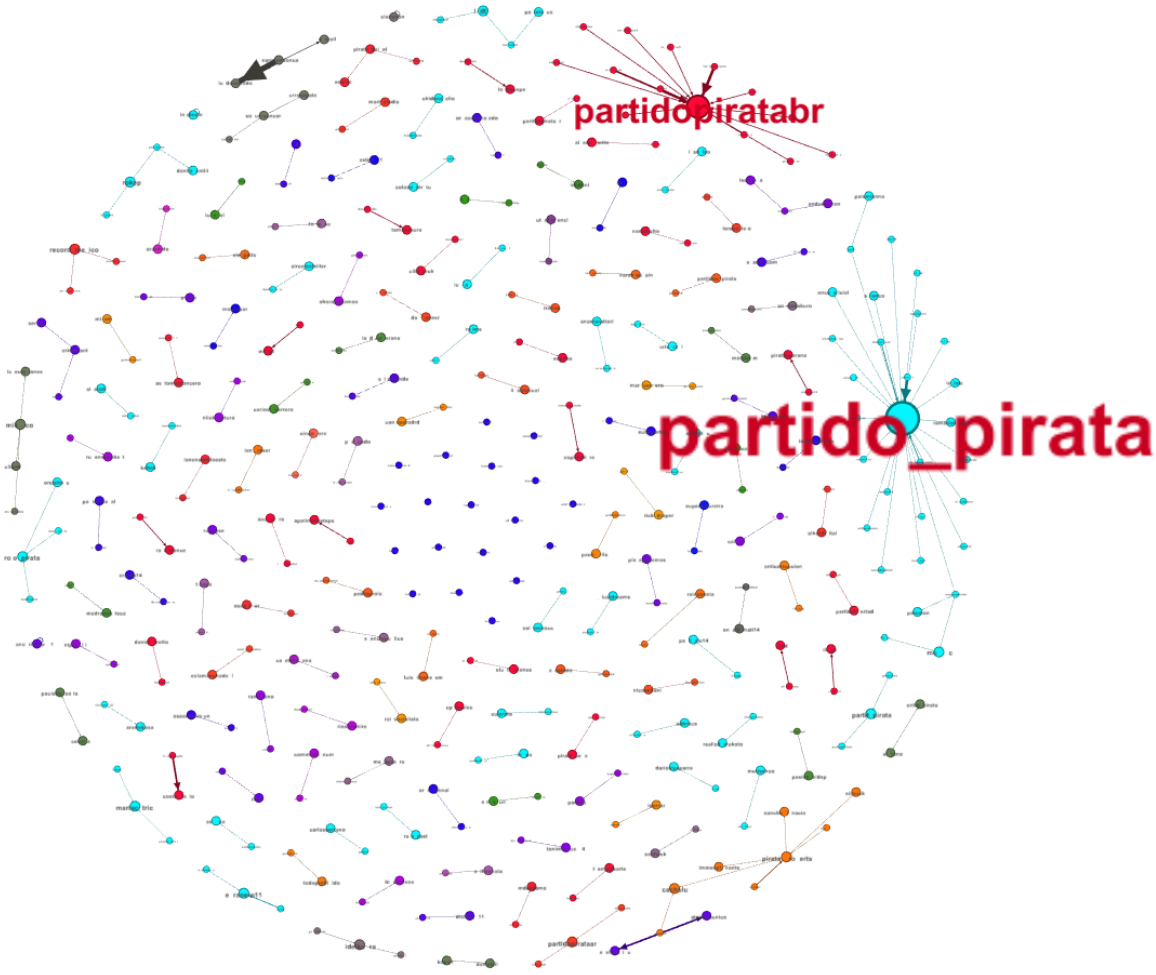

Figura 37 – Rede de Grafos das menções ao termo "Partido Pirata" no Twitter.

Os grafos dos retweets confirmam a autoridade dos perfis oficiais do Partido Pirata e demonstram a autoridade da organização brasileira. A segunda maior autoridade (@ bukaneros92) é um perfil de ligado ao partido na Espanha. Ressalta-se também a presença de

perfis de veículos de mídia, como a revista Exame (@exame_com) e revista Info (@_info), demonstrando que a atenção dada ao partido por parte de veículos tradicionais ainda é concentrada em publicações relacionadas a tecnologia e internet.

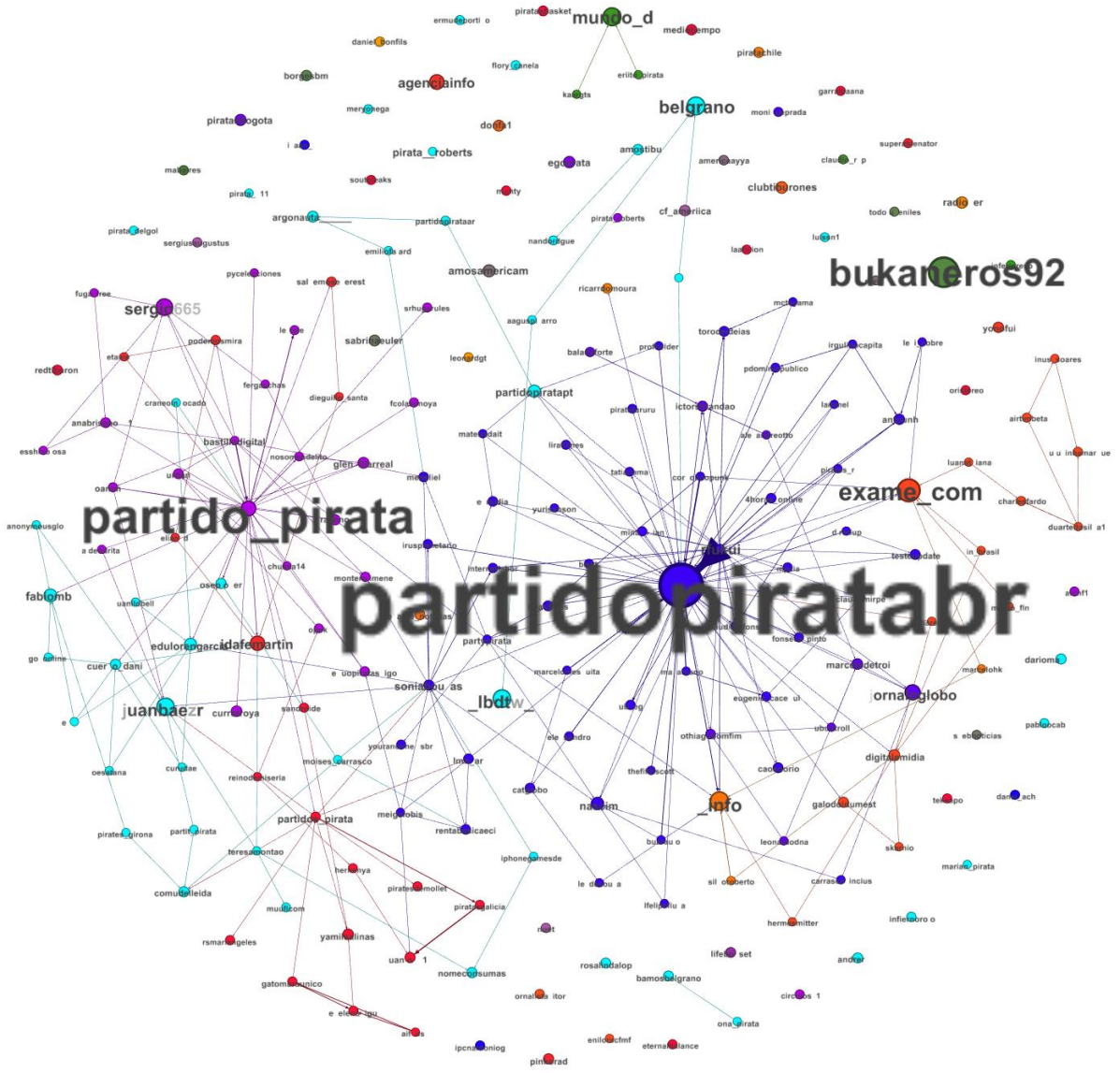

Figura 38 – Rede de Grafos dos retweets do termo “Partido Pirata” no Twitter.

Quadro 17 – Autoridades no retweets do termo “Partido Pirata

Perfis	Autoridade
Partidopiratabr	0,085
bukaneros92	0,053
exame_com	0,035
_info	0,024
mundo_d	0,023

4.4.2.12 Privacidade

O volume de dados gerados pela busca por privacidade dificultou a extração de informações relevantes para a pesquisa. Devido as diversas possibilidades de abordagem da discussão, os grafos de menções ficaram diluídos e sem apontar para uma autoridade expressiva. A maior autoridade encontrada foi o blogueiro Lucas Ranngel (@lucasranngel), porém sua expressividade se deve a comentários sobre a privacidade de celebridades.

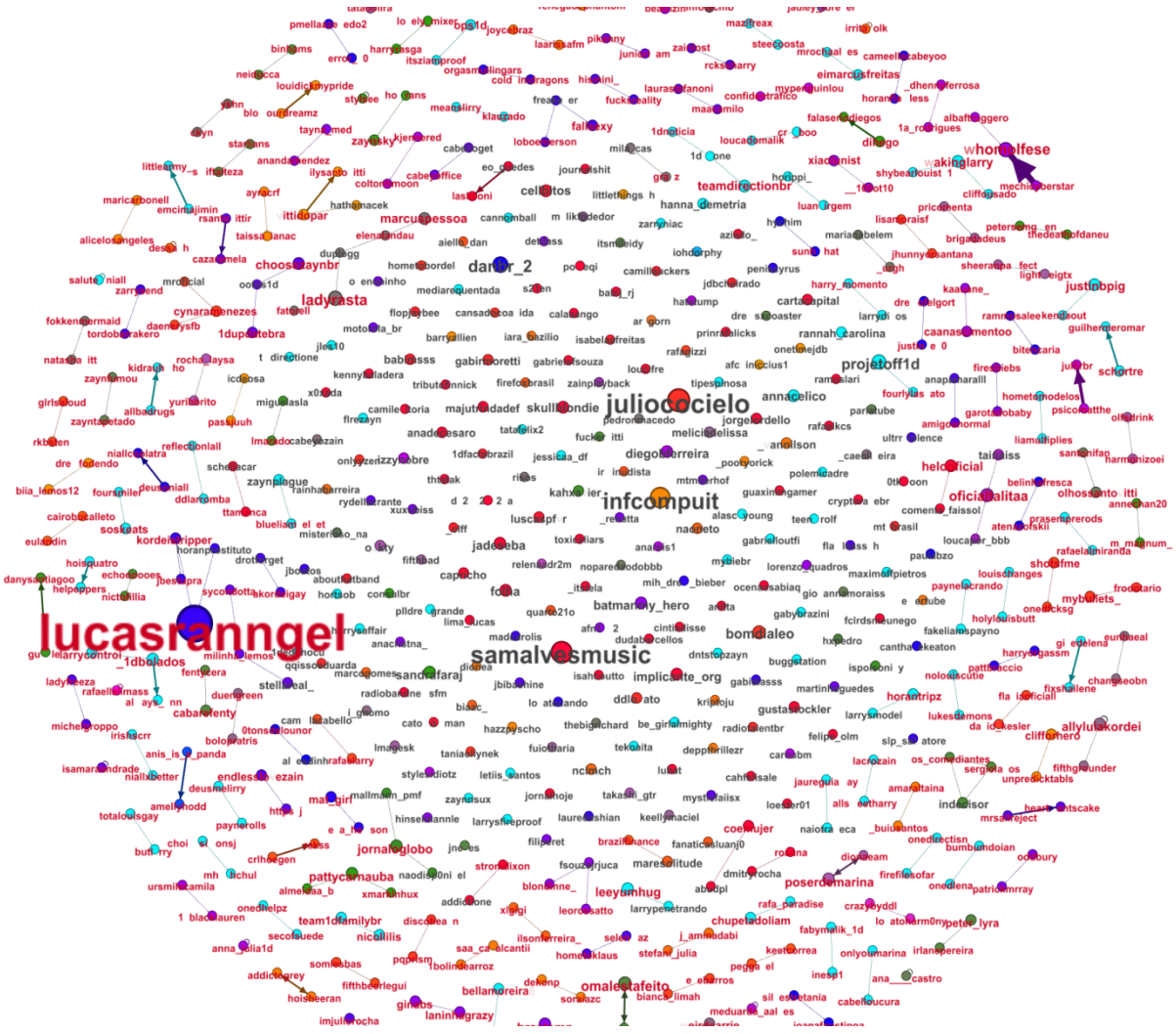

Figura 39 – Rede de Grafos das menções ao termo "Privacidade" no Twitter.

Já os grafos dos retweets apontaram novamente para um veículo de mídia tradicional como principal autoridade: Carta Capital (@cartacapital). Aparece também com relevância dentro do debate sobre privacidade e internet o perfil oficial da consulta pública sobre a

regulamentação do Marco Civil da Internet (@dadospessoais) e a publicação independente sobre internet e política Espírito Livre (@espiritolivre).

Ainda se faz necessária uma pequena observação metodológica. As buscas pelo termo "privacidade" bastante promissoras desde o início da mineração dos dados. Em geral, as menções ao termo estavam relacionadas a internet ou dados pessoais. No entanto, devido à própria imprevisibilidade das redes sociais, o tema entrou em discussão em grupos de adolescente e blogs sobre celebridades, obviamente com outro viés. Ainda que o resultado reflita a discussão no período captado sobre privacidade e internet, o conteúdo político do debate está diluído em outras discussões. Mesmo assim, o destaque de autoridades ligadas ao tema demonstra a força da discussão.

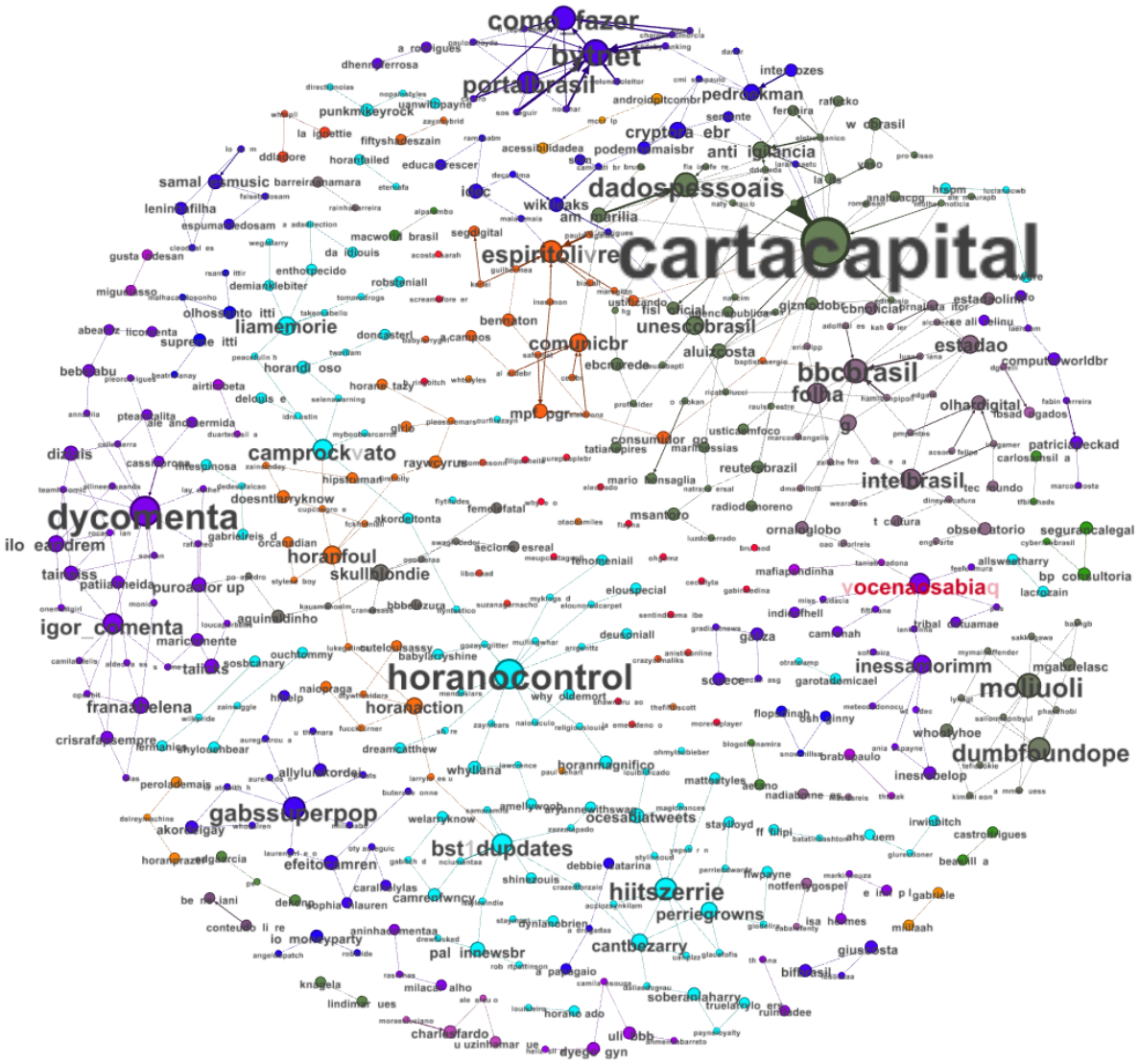

Figura 40 – Rede de Grafos dos retweets do termo "Privacidade" no Twitter.

Quadro 18 – Autoridades nos retweets do termo “Privacidade”.

Perfis	Autoridade
cartacapital	0,032
Brasillm	0,019
Dycomenta	0,017
Horanocontrol	0,017
Bytnet	0,014
dadospessoais	0,013
espiritolivre	0,011

4.4.2.13 Snowden

O grafo de menções ao termo “Snowden” demonstra que a autoridade mais citadas é o jornalista Glenn Greenwald, responsável pela publicação dos documentos da NSA liberados por Edward Snowden.

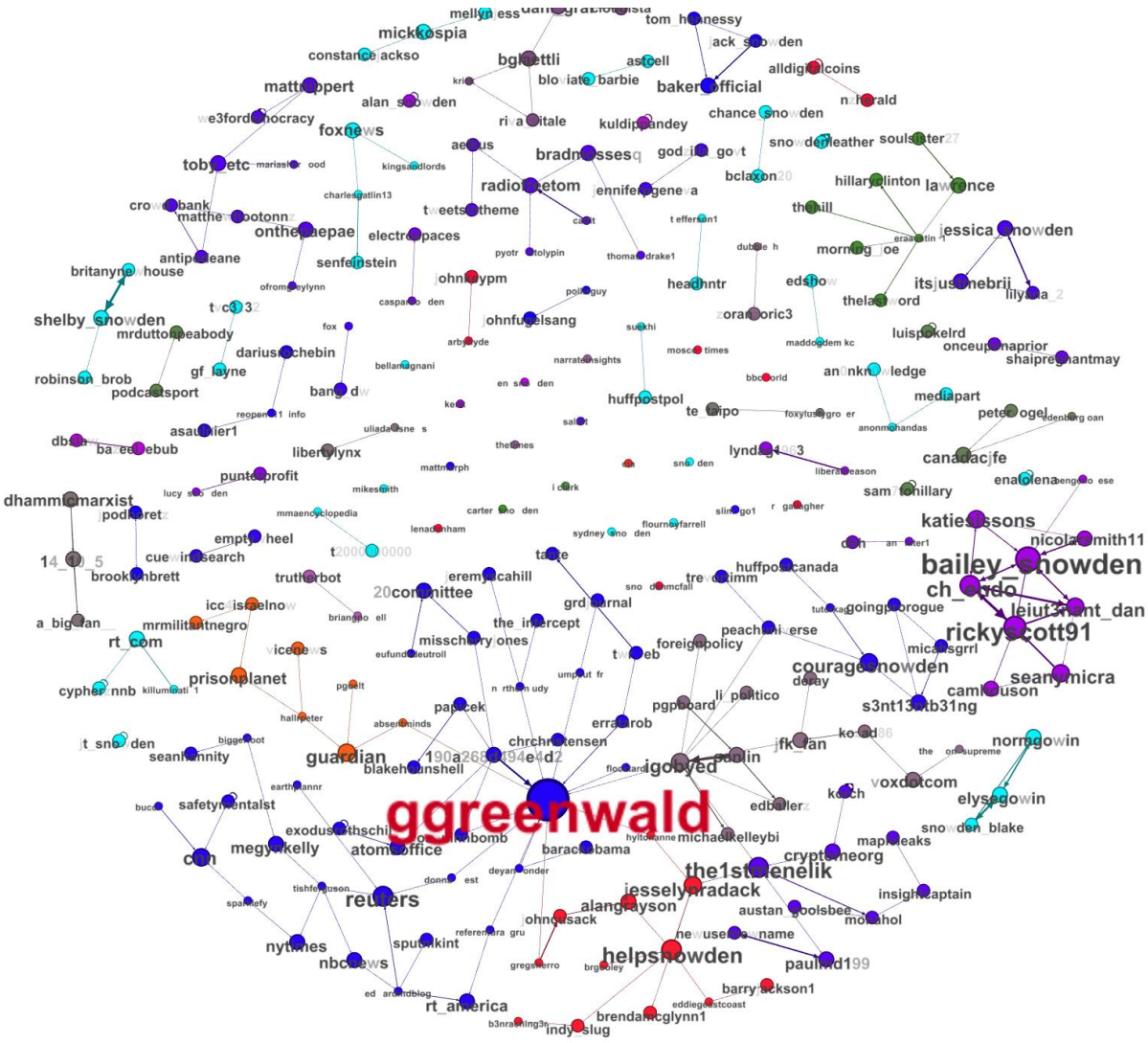

Figura 41 – Rede de Grafos das menções ao termo “Snowden” no Twitter.

Já os grafos de retweets apontam para um cluster, uma espécie de bunker virtual de defesa e apoio a Edward Snowden. Dentre as cinco primeiras autoridades três são jornalistas ativistas: Glenn Greenwald (@ggreenwald), Ryan Gallagher (@rj_gallagher) e Morgan Mayhem (@headhntr). Todos ligados direta ou indiretamente à publicação independente "The Intercept" (@the_intercept). Destaca-se ainda a relevância da organização Wikileaks no debate sobre Edward Snowden. Outros perfis também aparecem devido a participação em campanhas de apoio e solidariedade, como: @helpsnowden e @couragesnowden.

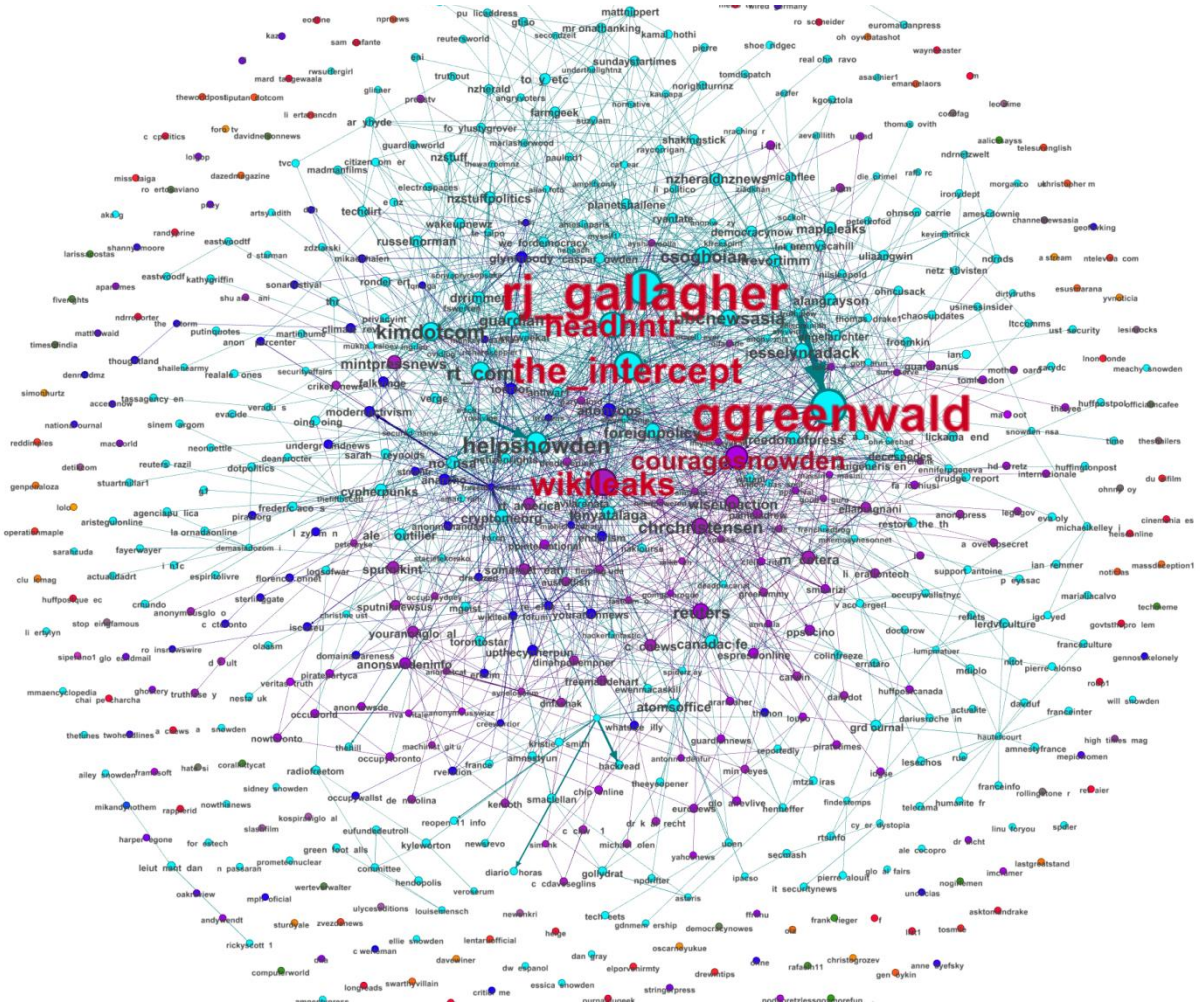

Figura 42 - Rede de Grafos dos retweets do termo "Snowden" no Twitter.

Quadro 19 – Autoridades nos retweets ao termo "Snowden".

Perfis	Autoridade
Ggreenwald	0,038
rj_gallagher	0,038
the_intercept	0,028
Wikileaks	0,026
Headhntr	0,025

4.4.2.14 Wikileaks

Os grafos de menções demonstram que o debate sobre o Wikileaks se concentra em torno dos dois perfis oficiais: @wikileaks e @wikileaks_forum.

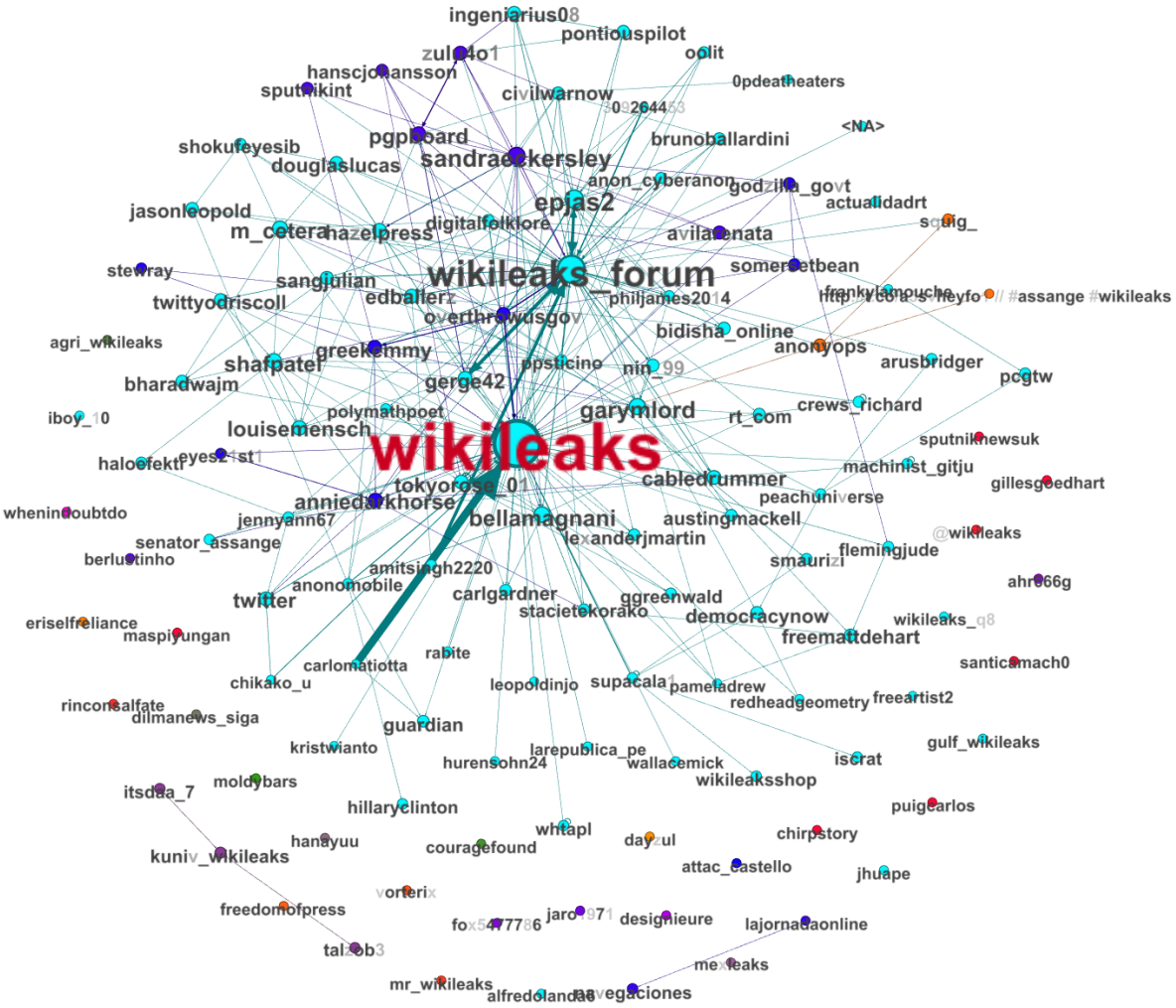

Figura 43 – Rede de Grafos das menções ao termo "Wikileaks" no Twitter.

As autoridades encontradas na rede de retweets, além do próprio Wikileaks (@wikileaks), apontam para veículos de mídia independente como: Global Trade Watch (@pcgtw), New Matilda (@newmatilda), La Jornada (@lajornadaonline). Além do perfil em língua espanhola da agência de notícias russa RT (@actualidadrt). O jornalista Glenn Greenwald surge novamente como uma autoridade, reforçando seu papel no debate global sobre privacidade, liberdade e internet.

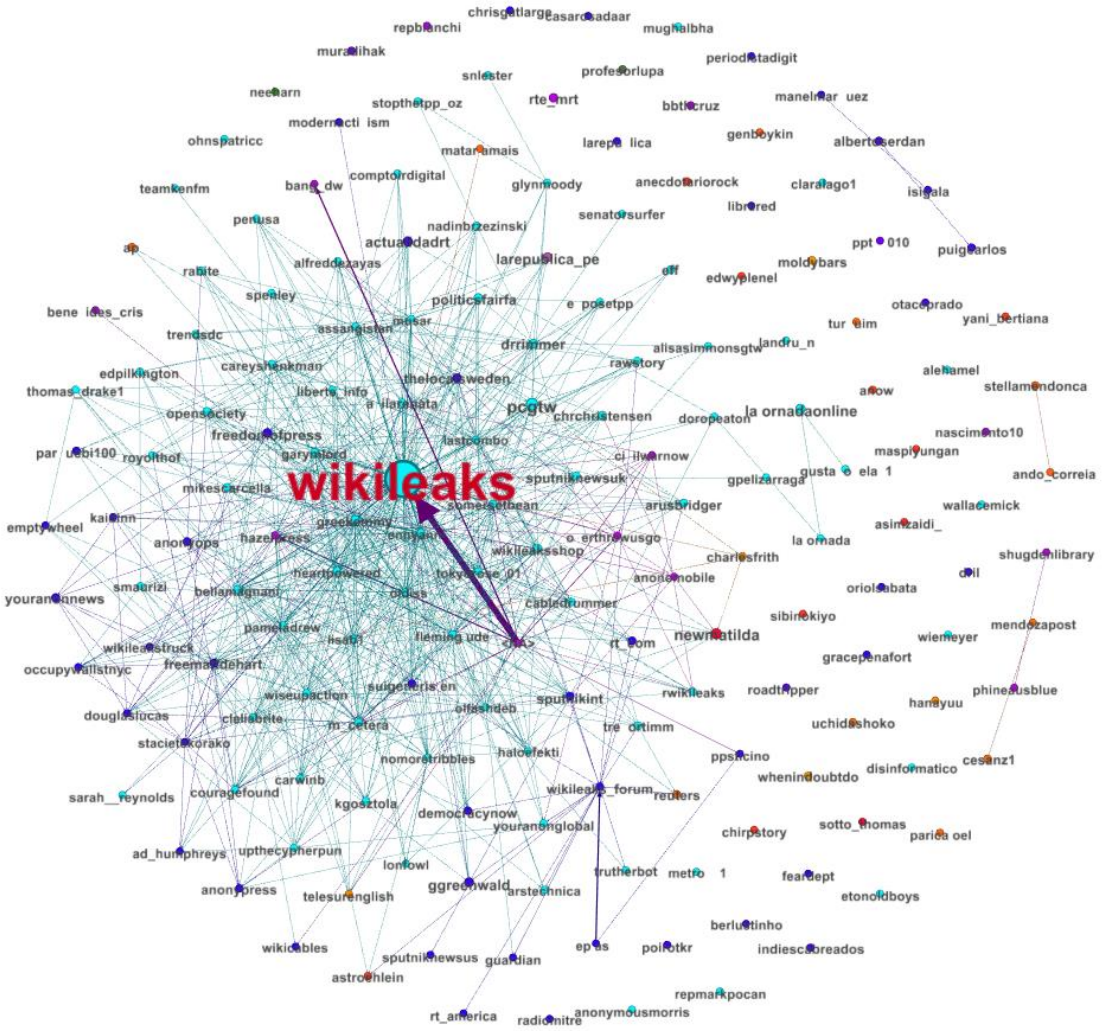

Figura 44 – Rede de Grafos dos retweets do termo “Wikileaks” no Twitter.

Quadro 20 – Autoridades nos retweets ao termo “Wikileaks”.

Perfis	Autoridade
wikileaks	0,163
pcgtw	0,025
newmatilda	0,016
lajornadaonline	0,013
actualidadrt	0,011
Ggreenwald	0,011

4.4.3 Netvizz e ecossistemas ativistas no Facebook

O aplicativo Netvizz obtém os dados de páginas do Facebook e suas conexões com outras páginas. A partir disso, é possível visualizar quais páginas estão conectadas entre si, formando comunidades com interesses e objetivos semelhantes. Observar essas comunidades ajuda a posicionar os grupos ativistas e entender seu papel, peso e relevância dentro dos clusters.

No entanto, para a visualização dos dados do Facebook os parâmetros devem ser adaptados. A ideia de autoridade não é relevante, uma vez que o conteúdo produzido pelas páginas não é reproduzido por outras. Por essa razão, observa-se outra variável calculada pelo software Gephi: centralidade de intermediação (betweenness centrality). O algoritmo calcula o diâmetro da rede, isto é, a maior distância de grafo entre dois nós quaisquer da rede. Feito isso, é calculado a frequência que um nó aparece nos caminhos mais curtos entre nós da rede. Dessa forma, quanto mais central o nó mais vezes ele aparece nos caminhos entre nós aleatórios.

A partir disso, a visualização dos grafos do Facebook obedece a seguinte orientação.

Quadro 21 – Variáveis dos grafos do Facebook.

Unidade	Variável
Tamanho do Nó	Grau
Cor do Nó	Modularidade
Tamanho do Rótulo	Centralidade de Intermediação
Cor do Rótulo	Grau

O aplicativo Netvizz realiza uma busca por páginas conectadas em dois níveis. Por exemplo, a partir da página inicial X o software encontra as páginas “A, B e C” conectadas a ela. Em seguida, encontra as outras páginas conectadas a “A, B e C”, aumentando assim o tamanho da rede. Dessa forma são gerados os nós e as arestas para a visualização. A tabela a seguir indica os valores encontrados para as páginas pesquisadas.

Quadro 22 – Número de nós e arestas coletadas das páginas do Facebook.

Páginas	Número de Nós	Número de Arestas
Agência Pública	312	1202
Anonymous Brasil	196	730
Cryptoparty	755	4235
Direito à Privacidade	464	3665

Electronic Frontier Foundation	62	236
Garoa Hacker Club	999	5014
Observatório do Marco Civil	203	1835
Partido Pirata	780	9975
Wikileaks	232	1577

A escolha das páginas pesquisadas obedeceu a uma dinâmica diferente da pesquisa no Twitter. Como a ferramenta de buscas utilizada, Netvizz, não oferece opções de busca por conteúdo – outros softwares proprietários oferecem essa opção para o Facebook e outras redes socais, porém não foram utilizados na presente pesquisa – foi necessário a pré-seleção das páginas a serem observadas. Partindo da definição inicial dos grupos apresentados no capítulo 2 foram encontradas as páginas: Anonymous Brasil, Cryptoparty e Partido Pirata. Outros grupos estavam ausentes do Facebook. No caso da página da Cryptoparty Brasil seu conteúdo e alcance eram mínimos e, por isso, optou-se pela página da Cryptoparty internacional.

Em seguida, devido à relevância do tema para o debate foi selecionada a página oficial da organização Wikileaks. Pela mesma razão, a página da Agência Pública foi selecionada. A Agência Pública é um veículo de mídia independente, mantido por doações e campanhas de financiamento coletivo, voltado para o jornalismo investigativo. Por sua atuação independente, foi escolhida como parceira do Wikileaks para a liberação de documentos com conteúdo relacionado ao Brasil. Já a organização Electronic Frontier Foundation foi escolhida em razão de sua relevância global e constante colaboração com os eventos e ativistas brasileiros.

Devido a sua dinâmica diferente, novos atores e páginas surgem na pesquisa no Facebook. Enquanto temas como, por exemplo, o Marco Civil podem entrar em debate no Twitter com diversos atores, uma página do Facebook dedicada ao tema constantemente produz conteúdo sobre a questão. Por isso, foram selecionadas as páginas: “Direito à Privacidade”; “Garoa Hacker Club” e “Observatório do Marco Civil”. A hipótese é que a partir delas é possível encontrar outras páginas relevantes sobre o tema.

4.4.3.1 Agência Pública

O mapeamento da página da Agência Pública no Facebook revelou todo um ecossistema de mídia independente e jornalismo investigativo. Observa-se também a

formação de clusters por idioma. Os clusters laranja e vermelho de língua inglesa, o cluster azul claro de língua espanhola e os clusters azuis escuros e verdes de língua portuguesa.

Dentre os nós mais centrais da rede, isto é, aqueles aparecem mais vezes no caminho entre dois nós aleatórios, estão: “Agência Pública”; “Organized Crime and Corruption Reporting Project”; “Global Investigative Journalism Network”; “Nota de Rodapé”; “Repórter Brasil”; “El Faro”.

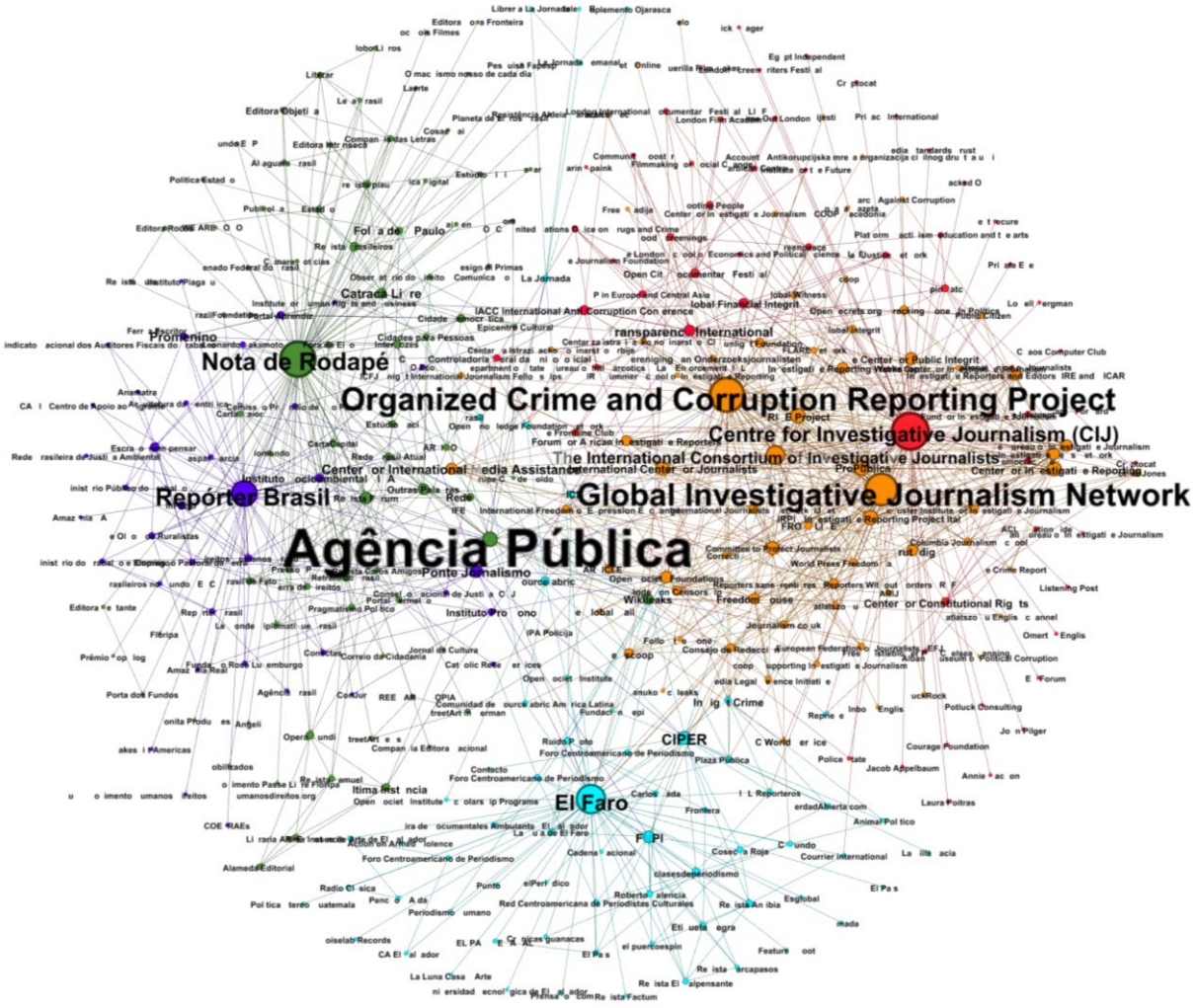

Figura 45 – Rede de páginas encontrada a partir da página “Agência Pública”.

4.4.3.2 Anonymous Brasil

Assim como em outros países, o Anonymous Brasil possui várias páginas e nenhuma é considerada oficial. O movimento horizontal e sem rostos aparece de forma tão diversa na

rede que parece confirma o caráter a anárquico da organização. Para o mapeamento, foi selecionada a página com maior número de seguidores e maior alcance das postagens: Anonymous Brasil.

A partida página “Anonymous Brasil” foi possível identificar um cluster de páginas ativistas diversas (azul escuro). O teor das páginas varia desde “Black Bloc RJ” até páginas como “Sou Brasileiro”, destacando-se também outras páginas do anonymous como a “Anonymous BR”. Além disso, foi possível identificar outro cluster (azul claro e verde) relacionado a campanhas contra violência no trânsito e impunidade. Já os clusters vermelho e laranja estão organizados em torno das páginas “Facebook”. O cluster vermelho contém páginas de cunho mais técnico, voltadas para a produção de conteúdo e aplicativos para a rede social. Já o cluster laranja se conecta a páginas diversas, incluindo artistas, marcas, eventos e celebridades. Tais páginas foram mantidas na visualização, pois impactam nos cálculos sobre a rede.

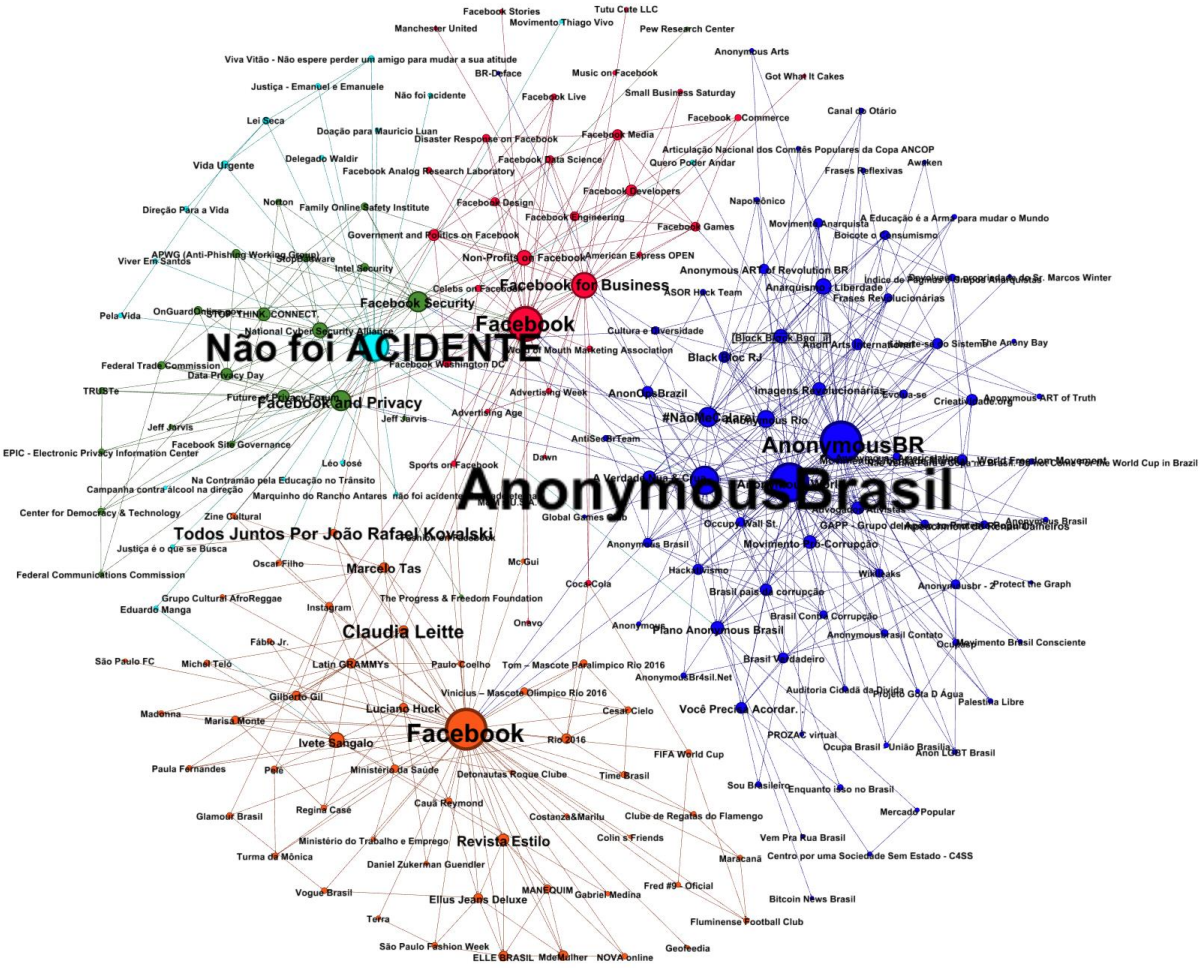

Figura 46 – Rede de páginas encontrada a partir da página “Anonymous Brasil”.

4.4.3.3 Cryptoparty

A partir da página da "Cryptoparty" internacional foi possível visualizar todo um ecossistema de páginas ligadas à tecnologia, mídias sociais e ativismo criptográfico. Nesse caso, a preponderância alemã fica evidente com enorme cluster formado em torno das páginas "Social Media Week Berlin" e "Design akademie berlin Hochschule für Kommunikation und Design". Já o cluster de cor roxa representa as iniciativas de cryptoparty em todo o mundo. Formando uma rede de troca de experiências, técnicas e ferramentas.

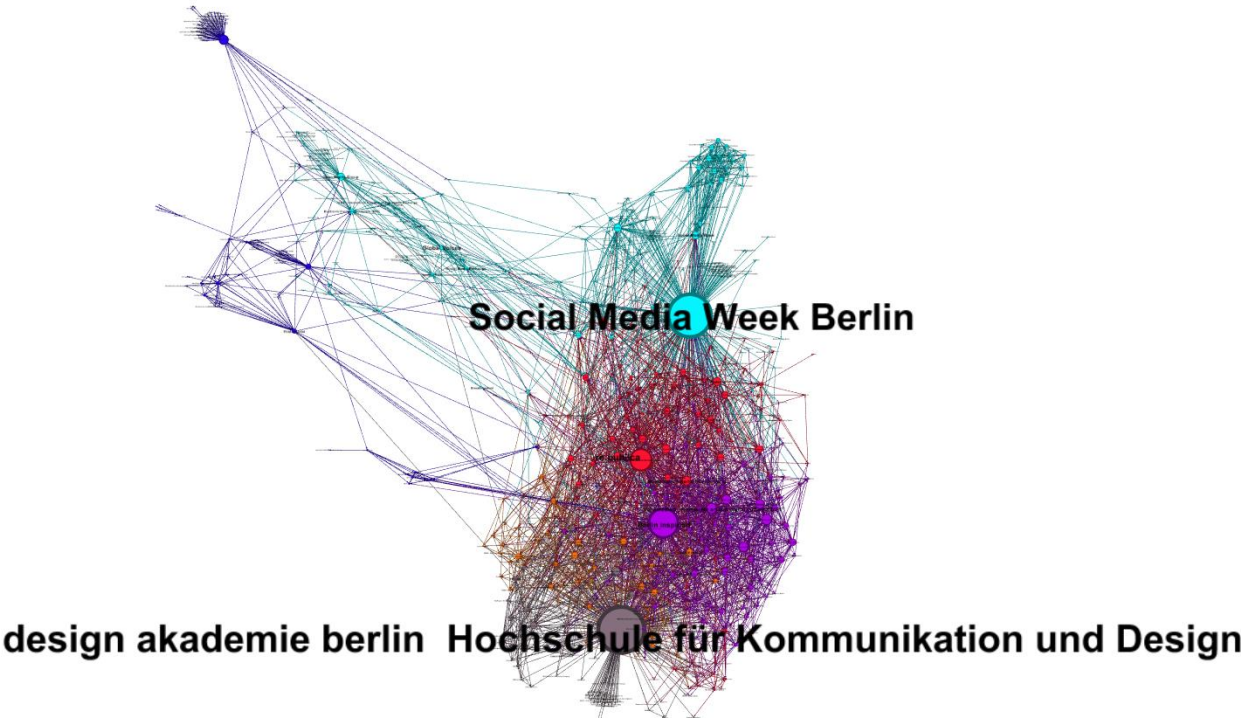

Figura 47 – Rede de páginas encontrada a partir da página "Cryptoparty".

4.4.3.4 Direito à privacidade

A página "Direito à Privacidade" aparentemente não possui grande relevância no contexto do Facebook. Com poucos seguidores e postagens, ela passa despercebida em meio ao debate. Porém, por meio dela, foi possível identificar um ecossistema internacional de páginas de defesa da privacidade e dos direitos digitais. A partir do ranking de centralidade na rede, a página "Identity Theft Resource Center" aparece em primeiro lugar, uma organização

voltada para o auxílio e orientação de vítimas de crimes virtuais, especialmente roubo de identidades. Seguindo a mesma a linha, aparece a página “Justice and Privacy Rights”. Chama a atenção às diversas páginas da ACLU (American Civil Liberties Union), organização norte-americana de proteção dos direitos civis.

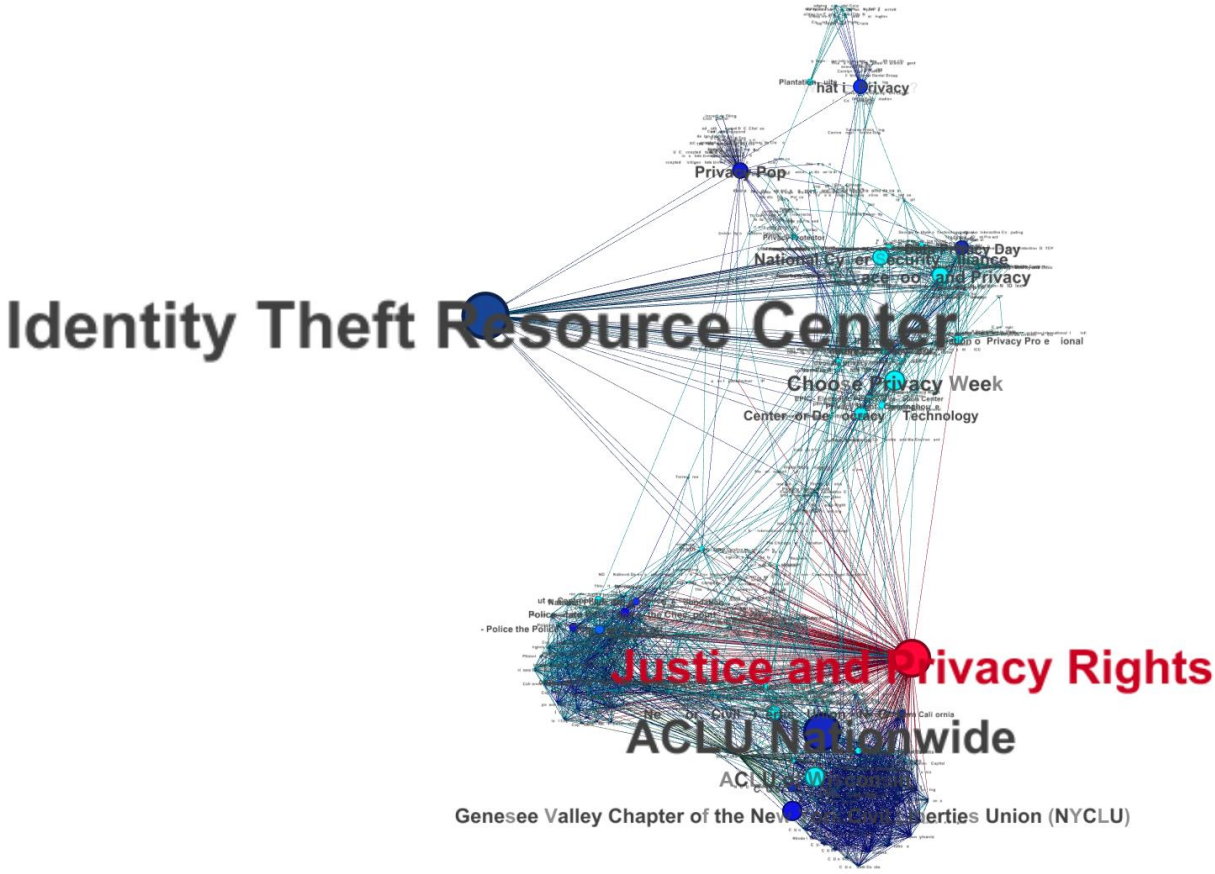

Figura 48 – Rede de páginas encontrada a partir da página “Direito à privacidade”.

4.4.3.5 Electronic Frontier Foundation

Fundada em 1990, a EFF (Electronic Frontier Foundation) é uma das principais organizações engajadas na defesa da privacidade e liberdade de expressão na internet. A análise de sua rede no Facebook demonstra um ecossistema de páginas ligadas diretamente à liberdade de imprensa e de expressão, direitos civis e combate a corrupção. Prova disso são as cinco primeiras páginas no ranking de centralidade: “IFEX - International Freedom of Expression Exchange”; “Electronic Frontier Foundation (EFF)”; “Foundation for Individual Rights in Education”; “International Day to End Impunity”; “Committee to Protect Journalists”.

Figura 49 – Rede de páginas encontrada a partir da página "Electronic Frontier Foundation".

4.4.3.6 Garoa Hacker Club

Garoa Hacker Club é um hackerspace. Segundo o próprio grupo um hackerspace é: "um espaço comunitário, aberto e colaborativo que disponibiliza infraestrutura para a realização de eventos e projetos em diversas áreas relacionadas à tecnologia ou que a criatividade nos permitir, fomentando a troca de conhecimento e o compartilhamento de ideias." (GAROA HACKER CLUB, 2015). De maneira simples, o Garoa Hacker Club se encaixa na definição clássica de hackers, isto é, pessoas interessadas em tecnologia e no desenvolvimento de novas ferramentas e formas de aplicação dos aparatos.

A partir da página do "Garoa Hacker Club" no Facebook foi possível identificar um ecossistema de páginas voltadas para a tecnologia e, em especial, *hacking*. Páginas sobre instruções de montagem de experimentos, linguagem de programação, invenções e inventores e coisas do gênero. Uma análise da rede de páginas encontradas pode ser útil para desmistificar a conotação negativa em torno do termo "hacker" amplamente difundida pela

mídia tradicional. Os interesses comuns das páginas encontradas são inovação, criatividade e tecnologia.

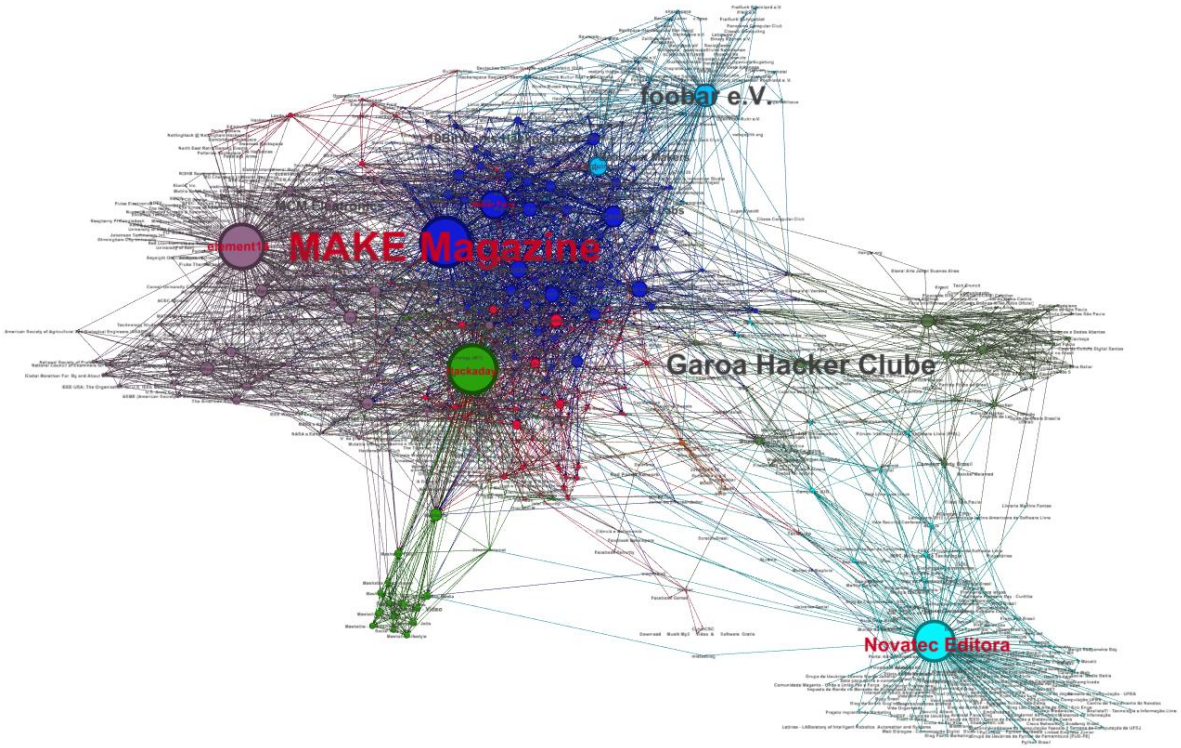

Figura 50 – Rede de páginas encontrada a partir da página “Garoa Hacker Club”.

4.4.3.7 Observatório do Marco Civil

O Observatório do Marco Civil é, segundo sua própria definição, uma “Plataforma online, sem vínculos político-partidários, criada para acompanhar a saga da "Constituição da Internet" nos Tribunais brasileiros.” (OBSERVATÓRIO DO MARCO CIVIL, 2014). A partir de sua rede de páginas no Facebook é possível identificar todo o ecossistema de páginas oficiais do governo brasileiro, isto é, páginas ligadas aos três poderes. Esse fato demonstra a luta legal do ativismo da internet, a busca pela materialização e positivação de direitos e a sua constante vigilância com o debate nas esferas governamentais. As páginas mais centrais nessa rede são: “Superior Tribunal de Justiça (STJ)”, “Palácio do Planalto”, “Ministério Público Federal – MPF”, “Conselho Nacional de Justiça (CNJ)”, “Ministério da Cultura”.

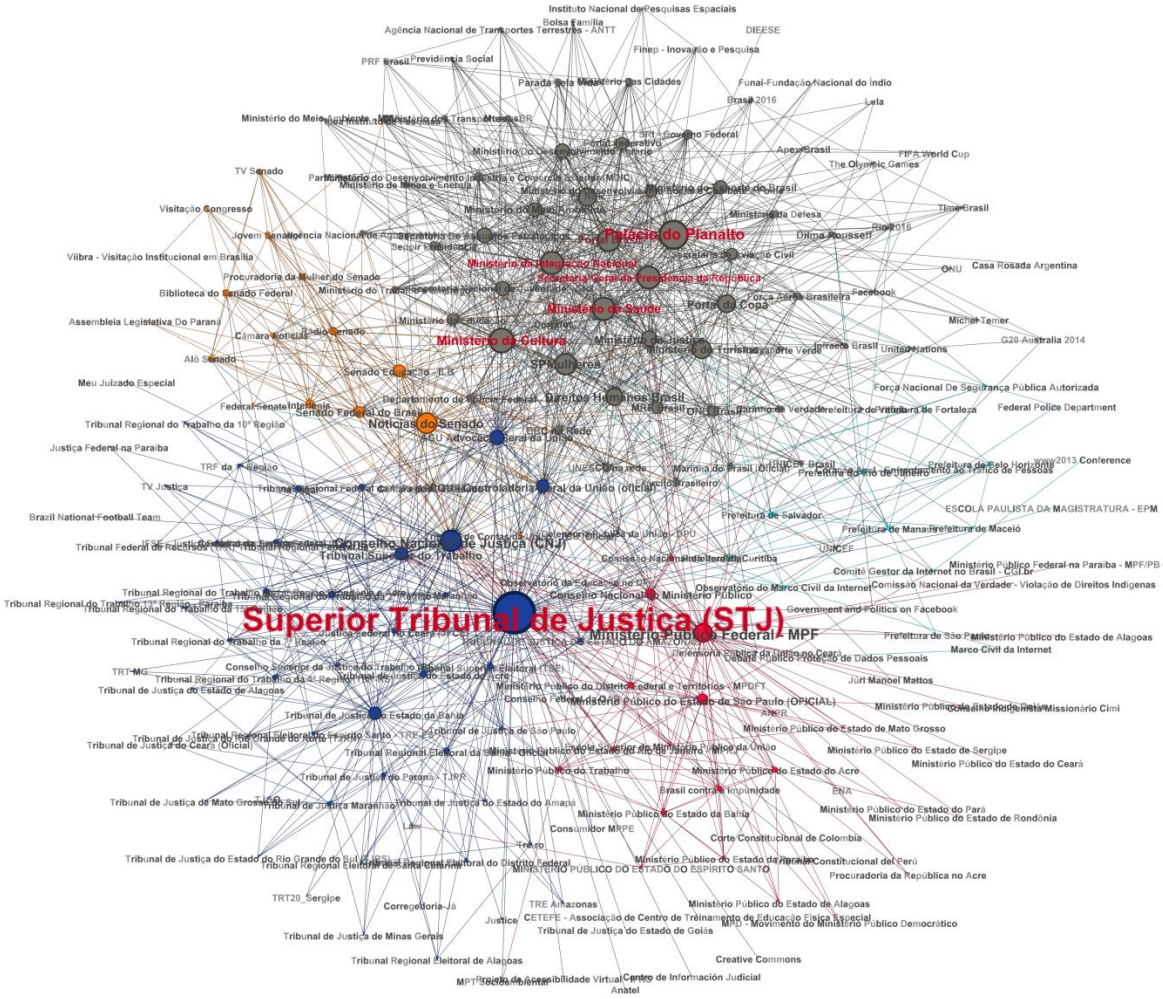

Figura 51 – Rede de páginas encontradas a partir da página "Observatório do Marco Civil".

4.4.3.8 Partido Pirata

A rede de páginas do Partido Pirata oferece uma visão ampla da rede global de partidos espalhados pelo mundo. O cluster vermelho, com destaque para o "Piratenpartei", representa as organizações na Europa. Já o cluster verde e azul as organizações nas Américas, em especial no Brasil. As páginas mais centrais da rede são: "Piratenpartei", "Partido Pirata do Brasil", "Piratpartiet", "Česká pirátská strana", "Pirate Parties International".

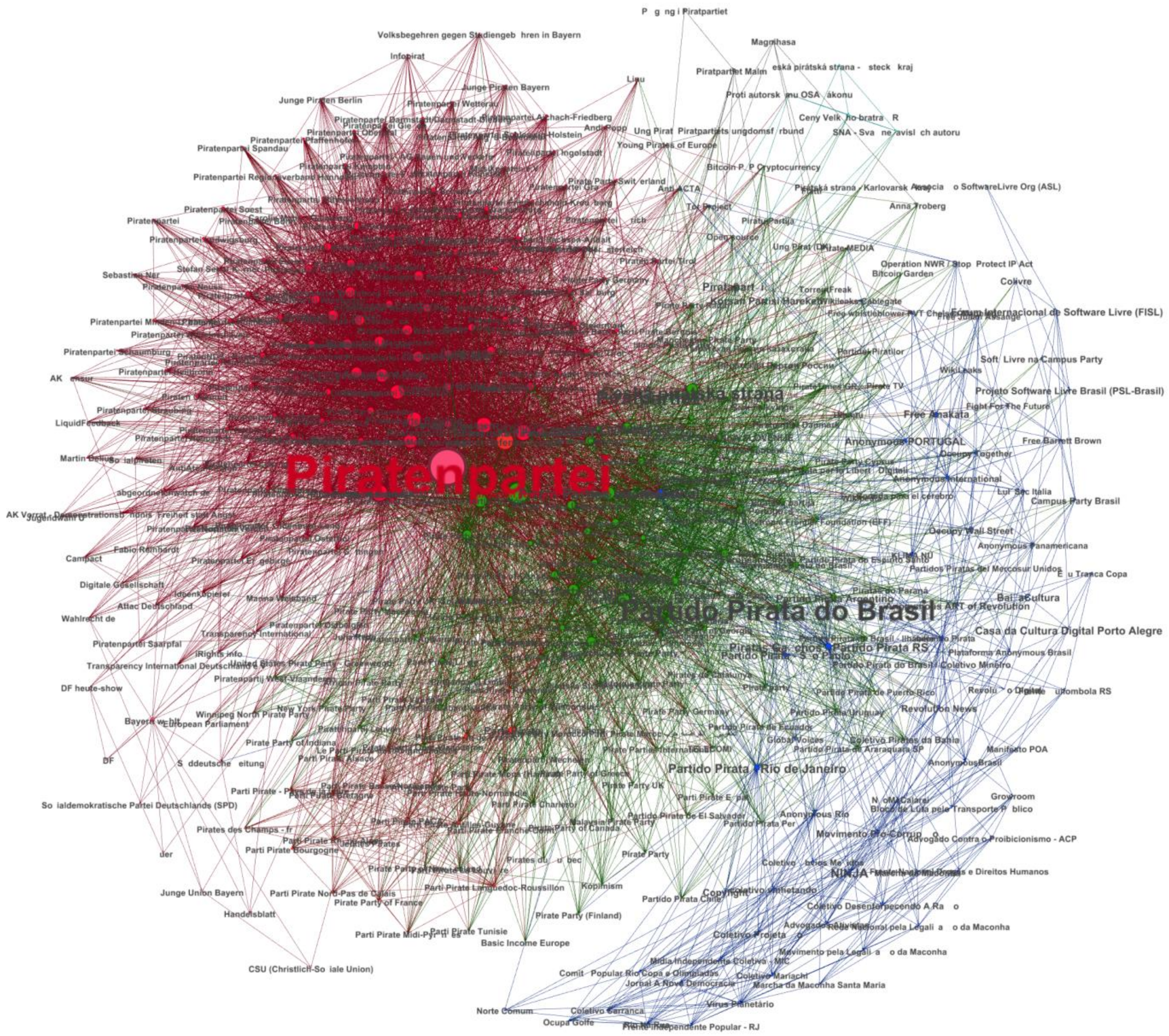

Figura 52 – Rede de páginas encontradas a partir da página "Partido Pirata".

4.4.3.9 Wikileaks

A rede de páginas do Wikileaks aponta para um ecossistema de organismos de defesa de direitos civis e liberdade individuais, ativistas e intelectuais engajados. As páginas mais centrais da rede são: "Center for Constitutional Rights", "The Nation Magazine", "Truthout", "FIERCE", "Naomi Klein".

Figura 53 – Rede de páginas encontradas a partir da página “Wikileaks”.

5 CONSIDERAÇÕES FINAIS

A crescente interdependência entre os processos sociais e as inovações tecnológicas é um tema que norteará agendas de pesquisas em diversas frentes. O modo como avanços técnicos desencadeiam ressignificações e novas demandas sempre foi objeto de investigação, porém o aprofundamento desse processo nos últimos anos ainda está além da capacidade analítica, tanto teórica quanto empírica, dos cientistas sociais. Ter isso em mente é o primeiro passo para continuar desenvolvendo novos métodos, técnicas e agendas de pesquisa cada vez mais interdisciplinares.

O fenômeno do ciberativismo é uma faceta dessa série de novas configurações. A apropriação de ferramentas tecnológicas e sua utilização em causas políticas apresentam-se como uma dinâmica radicalmente pertinente e interessante em um mundo quase completamente conectado por redes cibernéticas e fluxos de informação. Trata-se de um ativismo político atuando no sistema nervoso central do aparato de controle e tráfego de dados.

Conforme discutido nesse trabalho, o potencial de resistência cibernética nasce da ambiguidade tecnológica e da tensão entre formas de organização horizontais e verticais. Em primeiro lugar, o determinismo tecnológico deve ser superado pela apropriação por parte de grupos ativistas ou minoritários dos aparatos, isto é, a tecnologia é o que os agentes humanos fazem com ela, seja para controlar populações e espionar governos, seja para organizar protestos, divulgar documentos secretos ou abrir novas frentes de debates para além das tradicionais. Em segundo lugar, a tensão vertical-horizontal se materializa na organização da rede, sua arquitetura e topologia, e suas potencialidades de desenvolvimento distribuído e anárquico. Por fim, enquanto espaço de disputa estratégica e militar, o ciberespaço é, por um lado, um local de conflito bélico potencial e constante, e, por outro, de organização, debate, consenso e dissenso, com papel fundamental para a democracia, liberdade de expressão e de oposição.

A partir disso, a atuação de grupos ativistas ocorre em três frentes: jurídica, ação direta e midiática. Juridicamente, os ativistas lutam por garantias legais e positivação de direitos como forma de defesa da liberdade e privacidade na internet. Conforme discutido no capítulo 2, diversos mecanismos legais, nacionais e internacionais, apontam nessa direção. No entanto, a ideia de exceção em nome da segurança e a política de vigilância preventiva das populações acabam por suspender esses direitos. Esse processo atua em de maneira ambígua: por um

lado, insere os conceitos e a defesa da privacidade e da liberdade no texto da lei; por outro lado, desrespeita esses direitos de maneira massiva. Partindo desse pressuposto, alguns grupos ativistas, entre eles os aqui chamados cypherpunks, orientam sua atuação para formas de ação direta. A crença nas "leis da física superando as leis dos homens" guia o ativismo criptográfico. Isto é, para além das garantias legais, facilmente ignoradas por Estados e corporações, a criptografia e a linguagem matemática devem proteger o indivíduo do aparato de controle.

Frente de disputa midiática é vital nesse processo. Ao utilizar as redes para abrir novos canais de comunicação e fontes alternativas de informação, os ativistas visam ganham visibilidade para sua causa, atrair seguidores e divulgar as ações de violação de direitos. Esse ponto é compartilhado por diversos grupos ativistas que usam a internet como plataforma principal de divulgação e organização. O que difere os ativistas da privacidade nesse caso é que a internet é o meio e o fim de ação, isto é, ao mesmo tempo plataforma de comunicação, organização e objeto final das ações. Portanto, medir seu impacto nas redes é essencial para entender o sucesso ou fracasso de suas demandas.

Essa diferenciação é fundamental para se compreender os caminhos adotados pela pesquisa. Em primeiro lugar, é preciso retomar a pergunta de pesquisa: "Qual o impacto do ativismo cypherpunks no Brasil?". Considerando as três frentes de atuação dos ativistas aqui elencadas, cada uma demandaria uma abordagem diferente. O impacto da luta por direitos positivados levaria a pesquisa, por exemplo, a uma análise da formulação e implementação de políticas públicas para a internet. Já a análise do impacto das ações diretas e o estudo do repertório de táticas dos ativistas enfrentam dificuldades de adentrar em um universo fechado de grupos ativistas, quase sempre em uma posição legal ambígua. Uma pesquisa desse tipo poderia demandar uma etnografia ou entrevistas em profundidade com grupos e indivíduos extremamente comprometidos com sua privacidade e anonimato, fato que poderia comprometer ou inviabilizar os resultados. Por essas razões, optou-se por medir o impacto do ativismo no debate público sobre o tema. De forma que, tanto as pressões por garantias legais quanto o debate subsequente a ações diretas sejam contemplados.

Dessa forma, a opção pela combinação entre big data e cartografia parece adequada para abarcar o debate em larga escala e indicar os principais atores envolvidos e seus respectivos pesos na rede. Por meio da captura de dados de redes sociais, foram obtidos

robustos banco de dados sobre o debate nos tópicos específicos. Já a ideia de cartografia permitiu visualizar as redes e seus atores.

A primeira observação é justamente a ausência nas cartografias de alguns atores citados no capítulo 2 como possíveis autoridades do debate. Grupos como “Actantes” e “Saravá” não estão presentes nos debates capturados no Twitter e nem nos ecossistemas de páginas observados no Facebook. Esse fato, porém, não invalida suas posições como uns dos principais grupos ativistas no Brasil. Com isso, a hipótese que surge é que esses grupos se retiram voluntariamente do debate nas redes sociais citadas, uma vez que eles discordam de sua política de privacidade. Essa conclusão aponta para a necessidade de se observar tais movimentos por meio de outras metodologias. Por outro lado, sua ausência em um debate mais amplo travado nas redes sociais pode indicar sua permanência em uma comunidade ativista mais fechada e restrita.

Pesquisas sobre termos mais genéricos, como “anonimato” e “privacidade”, resultaram em uma visão geral do debate, apontando apenas em alguns casos atores relevantes quase sempre ligados ao Wikileaks. Já pesquisas por termos como “criptografia” revelou uma dinâmica interessante, na qual perfis da mídia tradicional, ligadas aos grandes grupos de comunicação, aparecem como autoridades. Ou seja, é possível afirmar que o debate sobre criptografia é pautado pelas postagens desses veículos, porém com a metodologia empregada na pesquisa não é possível medir a valência dos comentários, positivos ou negativos, a partir das matérias. Por outro lado, as buscas pelo termo “neutralidade” foram bem sucedidas em apontar os principais atores do debate sobre a neutralidade da rede e liberdade na internet.

As pesquisas por “Anonymous”, “Antivigilância”, “Cryptoparty”, “Cryptorave”, “Cypherpunks” e “Partido Pirata” revelaram as comunidades em torno desses temas. A partir de seus principais atores e autoridades foi possível observar o alcance e a dimensão de suas redes de debate. No entanto, a principal conclusão que se pode chegar observando tais grupos é a formação de comunidades que falam muito entre si, sem interagir em um debate mais aberto com outros grupos dissonantes. A pesquisa do termo “Anonymous” revelou uma grande rede global de apoiadores, porém em grande medida formada por diversas páginas intituladas “Anonymous” que reproduzem o conteúdo das páginas centrais. O Boletim Antigivilância, apesar de se constituir em uma das principais iniciativas brasileiras na divulgação do debate sobre privacidade e liberdade na internet, possui um alcance restrito e dialoga, em geral, com os próprios ativistas, não alcançando um público mais amplo. O

mesmo acontece com as iniciativas “Cryptoparty” e “Cryptorave” e com o termo “Cypherpunks”, todas impactam dentro da própria comunidade ativista.

O “Partido Pirata” constitui um caso à parte. Devido a sua opção pela via eleitoral, um debate mais amplo e uma maior comunicação se faz necessário para seus objetivos. Por essa razão, em sua rede surgem tanto perfis ligados ao partido quanto perfis de revistas ligadas a grupos de comunicação. De maneira geral, pode-se afirmar que o Partido Pirata é obrigado a buscar o diálogo e o debate para além de sua comunidade de seguidores, ativistas e simpatizantes.

As buscas pelos termos ligados às personalidades ativistas de maior relevância, “Assange” e “Snowden”, assim como a organização “Wikileaks”, demonstraram uma rede global de apoiadores, veículos de mídia e jornalistas independentes. Essa rede global se demonstrou extremamente importante no debate, inclusive confrontando a mídia tradicional, e na construção de narrativas alternativas para os fatos ligados aos ativistas e a organização. Por exemplo, o papel do jornalista Glenn Greenwald foi crucial para o vazamento dos documentos de Edward Snowden, assim como a rede formada em torno dele operou em apoio ao ativista durante o exílio forçado.

Já a pesquisa dos principais ciberativistas adotou uma metodologia diferente ao cruzar os dados capturados diretamente dos principais perfis e medir suas relações entre si. Dessa forma, pode-se observar a relação dos ativistas brasileiros com os principais expoentes da defesa dos direitos da internet. O cluster brasileiro apresenta relevância na rede e está em sintonia com o ativismo global. Porém, conseguem adaptar fatos para a realidade local e levar para o debate internacional temas como o Marco Civil da Internet.

De maneira geral, conclui-se que o debate gerado nas redes sobre as controvérsias envolvendo a internet teve um impacto maior em temas envolvendo a trajetória pessoal dos ativistas como os casos de Julian Assange e Edward Snowden, juntamente com o Wikileaks. Isso é observado tanto nas cartografias quanto nas campanhas de defesa e apoio. Outras cartografias apontam que, em geral, os ativistas tendem a conversar e debater mais entre si, com alcance restrito a um grupo de indivíduos e organizações já engajados.

Por fim, a pesquisa pode observar os ecossistemas ativistas de algumas páginas no Facebook. Essa observação permitiu concluir em que contexto as páginas se inserem e sua importância na rede. Apesar de ter sido realizada na etapa final do trabalho, esse

procedimento parece mais adequado para as etapas iniciais e exploratórias da pesquisa, permitindo uma visão mais macroscópica dos ecossistemas ativistas, para posteriormente uma análise mais aprofundada e com uma escolha de amostras mais apurada.

A metodologia cartográfica, combinada com o uso de mineração de dados na internet, apresenta resultados interessantes e reveladores das interações online. Do ponto de vista das ciências sociais, a expansão e diversificação do uso de tais técnicas e métodos poderão abrir novas perspectivas e oportunidades de interpretação da realidade. Do ponto de vista específico da Ciência Política, a cartografia pode ser útil em diversas áreas. Por exemplo, o uso em estudos sobre eleições, medindo o debate travado nas redes em torno de candidatos e/ou programas de governo; estudos sobre políticas públicas, ao mapear na internet pontos de rejeição e aceitação da política; estudos sobre movimentos sociais e ativismo antirregime, uma vez que, conforme discutido neste trabalho, a internet tem sido a forma primordial de organização de protestos e dissidentes.

Nesse sentido, a metodologia apresenta, assim como qualquer outra, vantagens e desvantagens. Por um lado, é possível captar declarações e posições políticas em sua forma bruta, isto é, declarações espontâneas que poderiam ficar ocultas em métodos mais tradicionais como entrevistas e grupos focais. Por outro lado, o volume de dado e sua dificuldade de obtenção podem afetar a realização de pesquisas mais abrangentes. Abordagens com metodologias combinadas continuam sendo essenciais para garantir maior validade e profundidade dos resultados alcançados. Pesquisas realizadas com manifestantes durante protesto e comparadas à cartografia das controvérsias debatidas nas redes sociais, por exemplo, é um caminho a ser seguido nas agendas de pesquisa.

Ressalta-se também a necessidade da expansão de estudos multidisciplinares, assim como a adequação das grades curriculares na formação de pesquisadores. Por se tratar de uma área de fronteira, a pesquisa sobre internet necessidade de habilidades e ferramentas específicas dos pesquisadores. Teoria Social, linguagens de programação, estatística, matemática e comunicação convergem em estudos do tipo. O domínio dessa interface constitui o limite do conhecimento na área e, por essa razão, deve ser superado.

6 REFERÊNCIAS BIBLIOGRÁFICAS

ACTANTES. Manifesto Actantes. Disponível em: actantes.org.br/manifesto-actantes. Acesso em: 10/12/2013.

AGAMBEN, Giorgio. Homo sacer – o poder soberano e a vida nua I. Belo Horizonte: Ed. UFMG, 2002.

_____. Estado de Exceção. São Paulo: Boitempo, 2004.

ALBUQUERQUE JUNIOR; VEIGA-NETO & SOUZA FILHO. (Orgs.).Cartografias de Foucault. Belo horizonte: Autêntica, 2008

ANTOUN, Henrique. Democracia, Multidão e Guerra no Ciberespaço. In: PARENTE, André (Org.). Tramas da Rede. Porto Alegre: Sulina, 2013.

APPLEBAUM, Jacob. Internet e Política. ASSANGE, Julian et al. Cypherpunks: liberdade e o futuro da internet. São Paulo: Boitempo, 2013.

ARAÚJO, William Fernandes. Ciberativismo: levantamento do estado da arte na pesquisa no Brasil. In: ABCIBER, Simpósio Nacional da, V, Florianópolis, 2011. Anais. Florianópolis, SC. 1:1-14.

ARQUILLA, John; RONFELDT, David. In Athena's Camp: preparing for conflict in the information age. Santa Monica: RAND, 1997.

ASSANGE, Julian. Cypherpunks: liberdade e o futuro da internet. São Paulo: Boitempo, 2013.

ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS. Declaração Universal dos Direitos do Homem. São Francisco, 1948.

_____. Pacto Internacional sobre Direitos Civis e Políticos. Nova York, 1966.

_____. Direito à privacidade na era digital. Nova York, 2013.

BRASIL. Constituição Federal, de 05 de outubro de 1988. Constituição da República Federativa do Brasil, Brasília, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm (Acesso em 25/09/2014).

BENKLER, Yochai. The wealth of networks: how social production transforms markets and freedom. New Haven: Yale University Press, 2006.

BRUNS, Axel; BURGESS, Jean E. New methodologies for researching news discussion on Twitter. In: The Future of Journalism 2011, September 2011, Cardiff University, Cardiff, UK.

BRUNS, Axel; LIANG, Yuxian Eugene. Tools and methods for capturing Twitter data during natural disasters. In: First Monday, 2012. Disponível em: http://journals.uic.edu/ojs/index.php/fm/article/view/3937/3193%3E (acesso em: 15/02/2015).

CASTELLS, Manuel. A sociedade em rede. São Paulo: Paz e Terra, 2002.

_____. O Poder da Identidade. São Paulo: Paz e Terra, 1999.

_____. A Galáxia da Internet: Reflexões sobre a Internet, os Negócios e a Sociedade. Rio de Janeiro: Jorge Zahar, 2003.

COLEMAN, Gabriella. Anonymous in Context: The Politics and Power behind the Mask. Internet Governance Papers, Ontario, n. 3, Set. 2013.

CONGRESSO DOS ESTADOS UNIDOS DA AMÉRICA. Digital Millennium Copyright Act. Disponível em: http://www.copyright.gov/legislation/dmca.pdf (Acesso em 25/01/2014).

_____. Stop Online Piracy Act. Disponível em: https://www.govtrack.us/congress/bills/112/hr3261 (Acesso em 25/01/2014).

_____. Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011. Disponível em: https://www.govtrack.us/congress/bills/112/s968 (Acesso em 25/01/2014).

CULT OF DEAD COW. A declaração do Hackativismo. Online, 2001. Disponível em: http://www.hacktivismo.com/public/declarations/pt.php. Acesso 13/1/2014.

DELEUZE, Gilles. Conversações. Rio de Janeiro: Editora 34, 1992.

DELEUZE, Gilles; GUATTARRI, Félix. Mil Platôs: capitalismo e esquizofrenia. São Paulo: Ed. 34, 1996.

FEOFILOFF, P.; KOHAYAKAWA, Y.; WAKABAYASHI, Y. Teoria dos Grafos: uma introdução sucinta. São Paulo: IME-USP, 2011. Disponível em:

http://www.ime.usp.br/~pf/teoriadosgrafos/texto/TeoriaDosGrafos.pdf (acesso em 10/01/2015)

FRAGOSO, Suely; RECUERO, Raquel; AMARAL, Adriana. Métodos de pesquisa para internet. Porto Alegre: Editora Sulina, 2013.

FREITAG, Barbara. ROUANET, Sérgio Paulo (Org.). Habermas. São Paulo: Editora Ática. 1993.

FONSECA, T. M. G. & KIRST, P.G. Cartografia e devires: a construção do presente. Porto alegre: UFRGS, 2003

FOUCAULT, Michel. Vigiar e Punir: a história da violencia nas prisões. Petrópolis: Vozes, 1977.

_____. Microfísica do Poder. Rio de Janeiro: Paz e Terra, 2014.

GALLOWAY, A. Protocol. How control exists after decentralization. Boston: MIT, 2004.

GREENWALD, Glenn. Sem lugar para se esconder. Rio de Janeiro: Sextante, 2014.

HARDING, Luke. Arquivos Snowden: a história secreta do homem mais procurado do mundo. São Paulo: Leya, 2014.

HABERMAS, Jürgen. Mudança Estrutural da Esfera Pública. Rio de Janeiro: Tempo Brasileiro. 1984.

HARDT, Michael; NEGRI, Antonio. A Produção da Biopolítica. In: PARENTE, André (Org.). Tramas da Rede. Porto Alegre: Sulina, 2013.

HARDING, Luke. Arquivos Snowden: a história secreta do homem mais procurado do mundo. São Paulo: Leya, 2014.

HARVEY, D.; TELES, E.; SADER, E.; et al. Ocuppy: movimentos de protesto que tomaram as ruas. São Paulo: Boitempo Editorial, 2012.

HIMANEN, Pekka. The Hacker Ethic and the spirit of information age. Nova York: Random House, 2001.

KELLNER, Douglas. New technologies, technocities and the prospects of democratization. In: DOWNEY, John; MCGUIGAN (orgs.). Technocities. Londres: Routledge, 1999.

KRAMER, Adam; GUILLORY, Jamie; HANCOCK, Jeffrey. Experimental evidence of massive-scale emotional contagion through social networks. Proceedings of the National Academy of Sciences, vol 111, n. 24, 2013.

KREPINEVICH, Andrew. CYBER WARFARE: A "NUCLEAR OPTION"? Washington: CBSA, 2012.

KROKER, Arthur; WEINSTEIN, Michael. Data Trash. Nova York: St Martin's, 1994.

LEIGH, David; HARDING, Luke. Wikileaks: a guerra de Julian Assange contra os segredos de Estado. Campinas, Verus: 2011

LÉVY, Pierre. Cibercultura. Rio de Janeiro: Editora 34 Letras, 1999.

_____. As tecnologias da inteligência. Editora 34 Letras, 1995.

LEVY, Steven. Hackers: Heroes of the Computer Revolution. New York: Penguin Books, 2001.

LIMA, Venício. Mídia, rebeldia urbana e crise de representação. In: Cidades Rebeldes: Passe Livre e as manifestações que tomaram as ruas do Brasil. São Paulo: Boitempo, 2013.

MACHADO, Murilo Bansi. . A ação política dos Anonymous Brasil. In: 37º Encontro Anual da Anpocs, 2013, Águas de Lindóia. Anais do 37º Encontro Anual da Anpocs, 2013.

MILL, J. S. A liberdade / Utilitarismo. São Paulo: Martins Fontes, 2000.

NOMAN, Helmi. The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army. Infowar Monitor, 2011. Dispovível em: http://www.infowar-monitor.net/2011/05/7349/. Acesso: 13/1/2014.

NYE, Joseph. O Futuro do Poder. São Paulo: Benvirá, 2012.

_____. Cyberpower. Cambridge: Harvard Universtiy Press, 2010.

OLSON, Parmy. Nós somos Anonymous: por dentro do mundo dos hackers. Barueri: Novo Século Editora, 2014.

PASSOS, E. KASTRUP, V. & ESCÓSSIA, L. (Orgs.). Pistas do método da cartografia. Porto Alegre: Sulina, 2009.

PRADO FILHO, Kléber; TETI, Marcela. A Cartografia como método para ciências humanas e sociais. Revista Barbarói, Santa Cruz do Sul, n.38, p. 45-59, jan/jun, 2013.

RICHARDS, Jason. Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security. In: International Affairs Review, Volume XVIII, No. 1: 2009.

ROLNIK, Suely. Cartografia sentimental: transformações contemporâneas do desejo. São Paulo: Estação Liberdade, 1989.

RÜDIGER, Francisco. As teorias da cibercultura: perspectivas, questões e autores. Porto Alegre: Sulina, 2003.

SAFATLE, Vladimir. A esquerda que não teme dizer seu nome. São Paulo: Três estrelas, 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.

SEOANE, José; TADDEI, Emilio (orgs.). Resistências Mundiais: de Seattle a Porto Alegre. Petrópolis: Vozes, 2001.

SECCO, Lincoln. As jornadas de Junho. In: Cidades Rebeldes: Passe Livre e as manifestações que tomaram as ruas do Brasil. São Paulo: Boitempo, 2013.

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

_____. Arquiteturas em disputa: ativistas P2P e a indústria da intermediação. In: Revista de Economía Política de las Tecnologías de la Información y Comunicación, vol. XI, n. 1, enero – abril, 2009a.

_____. Redes cibernéticas e tecnologias do anonimato. Comunicação & Sociedade, Ano 30, n. 51, p. 113-134, jan./jun. 2009b.

_____. Cartografia de Espaços Híbridos. Interagentes, 2013. Disponível em: http://interagentes.net/?p=62 (acesso 11/10/2014).

TORET, Javier. Democracia Distribuida Miradas de la Universidad Nómada al 15M. Madrid: Universidad Nómada, 2013.

UNITED STATES OF AMERICA. The United States Constitution. 1791. Disponível em: http://www.usconstitution.net/const.html. (Acesso 25/09/2014).

VENTURINI, T. Diving in Magma: how to explore controversies with actor-network theory. Public Understanding of Science, n. 19, p. 258-273, 2010

_____. Building on Faults: how to represent controversies with digital methods. Public Understanding of Science, n. 21, p. 796-812, 2012.

WALLERSTEIN, Immanuel. O declínio do poder americano: os Estados Unidos em um mundo caótico. Rio de Janeiro: Contraponto, 2004.

_____. O que significa hoje ser um movimento anti-sistêmico. In: LEHER, Roberto; SETÚBAL, Mariana (Org.). Pensamento crítico e movimentos sociais. São Paulo: Cortez, 2005.

WRAY, Stefan. Electronic Civil Disobedience and the World Wide Web of Hacktivism. Disponível em: http://switch.sjsu.edu/web/v4n2/stefan. Acesso: 10/1/2014.

ZIMMERMANN, Jerémie. Internet e Política. In: ASSANGE, Julian et al. Cypherpunks: liberdade e o futuro da internet. São Paulo: Boitempo, 201 3.

Sites consultados:

15-M: http://datanalysis15m.wordpress.com/

Actantes: http://actantes.org.br/

Anonymous Brasil: http://www.anonymousbrasil.com/

Banco Mundial: http://data.worldbank.org/indicator/IT.NET.USER.P2

Cryptorave: https://cryptorave.org/

Escola de Ativismo: https://ativismo.org.br/

GEPHI: http://gephi.github.io/

IBM: http://www.ibm.com/midmarket/br/pt/infografico_bigdata.html

International Telecommunication Union: http://www.itu.int/en/ITU-D/Statistics

Oficina Antivigilância: https://antivigilancia.org/

LABIC- UFES: https://github.com/ufeslabic/

MACOSPOL: http://www.mappingcontroversies.net/

MediaLab UFRJ: https://github.com/medialabufrj

Partido Pirata: http://partidopirata.org/

Partido Pirata Internacional: http://www.pp-international.net/

Saravá: https://www.sarava.org/

Páginas do Facebook

Agência Pública: https://www.facebook.com/agenciapublica

Anonymous Brasil: https://www.facebook.com/AnonymousBr4sil

Cryptoparty: https://www.facebook.com/Cryptoparty

Direito à privacidade: https://www.facebook.com/direitoaprivacidade

Electronic Frontier Foudation: https://www.facebook.com/eff

Garoa Hacker Club: https://www.facebook.com/GaroaHC

Observatório do Marco Civil: https://www.facebook.com/omcibr

Partido Pirata: https://www.facebook.com/PartidoPirata.BR

Wikileaks: https://www.facebook.com/wikileaks

Dados utilizados na pesquisa:

https://mega.co.nz/#F!OxBknTRL!gHO8qbJWH24h7o_mG1zIPg