ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/325694844

Uma proposta de extensão inspirada na Pesquisa-Ação para atuar no combate à Vigilância Digital do Rio de Janeiro

Thesis · April 2018

DOI: 10.13140/RG.2.2.26537.08807

CITATIONS
0

READS
518

1 author:

Pedro Henrique da Costa Braga
Federal University of Rio de Janeiro

7 PUBLICATIONS **5** CITATIONS

SEE PROFILE

All content following this page was uploaded by Pedro Henrique da Costa Braga on 11 June 2018.

The user has requested enhancement of the downloaded file.

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

PEDRO HENRIQUE DA COSTA BRAGA

UMA PROPOSTA DE EXTENSÃO INSPIRADA NA PESQUISA-AÇÃO PARA ATUAR NO COMBATE À VIGILÂNCIA DIGITAL NO RIO DE JANEIRO

RIO DE JANEIRO

2018

PEDRO HENRIQUE DA COSTA BRAGA

UMA PROPOSTA DE EXTENSÃO INSPIRADA NA PESQUISA-AÇÃO PARA ATUAR NO COMBATE À VIGILÂNCIA DIGITAL NO RIO DE JANEIRO

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em História das Ciências e das Técnicas e Epistemologia, Universidade Federal do Rio de Janeiro, como requisito parcial à obtenção do título de Mestre em História das Ciências e das Técnicas e Epistemologia.

Orientador: Henrique Luiz Cukierman

RIO DE JANEIRO

2018

M379 Braga, Pedro Henrique da Costa.
Uma Proposta de Extensão Inspirada na Pesquisa-Ação para Atuar no Combate à Vigilância Digital no Rio de Janeiro / Pedro Henrique da Costa Braga. – 2018.
100 f.: il., 30 cm.

Dissertação (Mestrado em História das Ciências e das Técnicas e Epistemologia) – Universidade Federal do Rio de Janeiro, Centro de Ciências Matemáticas e da Natureza, Programa de Pós-Graduação em História das Ciências e das Técnicas e Epistemologia, 2018.
Orientador: Prof. Dr. Henrique Luiz Cukierman.

1. Vigilância Digital. 2. Segurança da Informação. 3. Tecnologias da Informação e Comunicação I. Usando a Pesquisa-Ação Participante para intervir na vigilância digital no Rio de Janeiro.

CDD 615.53

PEDRO HENRIQUE DA COSTA BRAGA

UMA PROPOSTA DE EXTENSÃO INSPIRADA NA PESQUISA-AÇÃO PARA ATUAR NO COMBATE À VIGILÂNCIA DIGITAL NO RIO DE JANEIRO

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em História das Ciências e das Técnicas e Epistemologia, Universidade Federal do Rio de Janeiro, como requisito parcial à obtenção do título de Mestre em História das Ciências e das Técnicas e Epistemologia.

Aprovada em 27/04/2018

_____
Henrique Luiz Cukierman, Dr., HCTE/UFRJ

_____
Isabel Leite Cafezeiro, Dr., HCTE/UFRJ

_____
Celso Alexandre Souza de Alvear, Dr., NIDES/UFRJ

_____
Antônio Cláudio Gómez de Sousa, Dr., NIDES/UFRJ

RESUMO

BRAGA, Pedro Henrique da Costa. Usando a Pesquisa-Ação participante para a construção de um mapa das redes sociotécnicas de vigilância digital no Rio de Janeiro. Rio de Janeiro, 2017. Dissertação (Mestrado em História das Ciências e das Técnicas e Epistemologia) - Programa em História das Ciências e das Técnicas e Epistemologia, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2017.

Em junho de 2013, a cidade do Rio de Janeiro, tal como outras metrópoles brasileiras, foi envolta em uma série de protestos, em sua maioria marcados pela forte violência policial. Esses protestos surgiram da demanda inicial de barrar o aumento da tarifa de ônibus, mas que se tornaram o vetor pelo qual as massas populares conseguiram expressar seu descontentamento com o governo e seus gastos abusivos com grandes eventos como a Copa do Mundo de 2014 e as Olimpíadas de 2016.

Nos anos seguintes às grandes manifestações, observou-se um aumento na repressão aos movimentos sociais e populares por parte do estado. Um marco nesse aumento foi o chamado "Caso dos 23", onde vinte e três manifestantes presentes em 2013 foram investigados pela Delegacia de Repressão à Crimes de Informática da Polícia Civil do Rio de Janeiro (DRCI) e acusados de formação de quadrilha armada. Nesse processo, o uso das redes sociais, tanto pelos investigados quanto pelos investigadores, é parte central da narrativa que levou à acusação. Dessa forma, observa-se que tanto a vigilância policial quanto a atividade política dos movimentos sociais passam a ter o ciberespaço como um importante palco de atuação.

A presente dissertação de mestrado tem como objetivo mapear as redes de vigilância que surgem nesse ciberespaço e como essas o reconfiguram. Para alcançar esse objetivo uso a metodologia da Pesquisa-Ação, que nesse caso específico tem como ação central a construção, em conjunto com membros de movimentos populares, de uma oficina de segurança da informação para movimentos sociais.

PALAVRAS-CHAVE: Vigilância Digital; Pesquisa-ação; Estudos Ciência, Tecnologia e Sociedade.

ABSTRACT

BRAGA, Pedro Henrique da Costa. Usando a Pesquisa-Ação participante para a construção de um mapa das redes sociotécnicas de vigilância digital no Rio de Janeiro. Rio de Janeiro, 2017. Dissertação (Mestrado em História das Ciências e das Técnicas e Epistemologia) - Programa em História das Ciências e das Técnicas e Epistemologia, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2017.

In June 2013, the city of Rio de Janeiro, just like several other Brazilian metropolises, was taken by a series of protests, most of which became remembered by the strong police violence. These protests were spawned by the initial necessity to halt the rise in the bus fare, but afterwards became the vector by which the popular masses could express their discontent against the government and its abusive spending with big events like the 2014 World Cup and the 2016 Olympics.

In the following years to the big demonstrations, one could observe a raise in the state repression directed towards the social movements. A landmark in this raise was the so called "Case of the 23", where twenty-three protesters from 2013 where investigated by the Rio the Janeiro Civil Police Cybercrime Repression Office (DRCI) and later charged with formation of armed gang. In this process, the use of social networks, both by the investigated and by the investigators, has a central spot on the narrative that led to the charges. In this way, one can observe that the police surveillance, as well as the political activity of the social movements, now have the cyberspace as an important stage.

The present mastery dissertation has as its objective to map the surveillance networks that come to be in these cyberspace as well as how they are responsible for its reconfiguration. To reach this objective I use the Action-Research methodology, that in this specific case has as central action the construction, alongside members of popular movements, of an workshop of information security for social movements.

KEY-WORDS: Digital Surveillance; Action-Research; Science, Technology and Society Studies.

DEDICATÓRIA

Dedico esse trabalho a todos os companheiros que lutam por um mundo melhor, mais justo, solidário e humano. Em especial, dedico aos meus camaradas de militância, que, junto a mim, embarcam no nosso frustrante, árduo e difícil, porém belo projeto de vida, de construir a semente da utopia na dura realidade do hoje.

Aos meus camaradas! Àqueles que me fizeram indestrutível pois contigo não termino em mim mesmo.

AGRADECIMENTOS

Agradeço ao meu orientador, Henrique Cukierman, por sempre me motivar e ajudar a tornar desse o trabalho o melhor que eu poderia fazer. Além disso também tenho que agradecê-lo por todos os conselhos, aulas, conversas e até mesmos puxões de orelha que me foram dados ao longo da minha trajetória no mestrado. Foram essenciais para que eu amadurecesse academicamente e como pessoa.

Também agradeço a Celso Alvear, cujo papel ao longo da pesquisa foi fundamental para que o trabalho tomasse forma, me orientando dentro do campo e me ensinando a fazer extensão universitária. Se não fosse por ele, certamente não seria capaz de ter feito o que fiz.

Agradeço aos coordenadores e bolsistas do Núcleo de Solidariedade Técnica, por constituírem, dentro da universidade, um ambiente de trabalho coletivo, discussão e troca de experiência fora do qual o presente trabalho não seria, nem de longe, tão rico. Destaco especialmente, minha querida equipe do TIFS: Arthur Castro, Arthur Guilherme e Mariana Rio. Eles foram protagonistas da história relatada aqui. Também incluo, ainda que tardiamente, nessa lista o Pedro Graça, que trabalhou conosco em 2017, depois da oficina relatada nesse texto.

Agradeço também os meus colegas de mestrado, com quem aprendi muito nas aulas, nos intervalos e nas reuniões de segunda na casa do Henrique. Em especial, destaco André Sobral, Alberto de Lima e Fernando Severo, cuja ajuda durante o processo de escrita foi essencial para que essa dissertação ficasse pronta.

Agradeço aos meus amigos, que me forneceram importantes momentos de descontração ao longo dessa escrita. E em especial, tenho que agradecer Vicente Melo, com quem completei 21 anos de amizade em 2017, e Matheus Lessa, grande amigo e colega de profissão.

Também devo agradecer aos meus familiares que me deram suporte afetivo nesse período e, por fim, à minha companheira Jéssica, que aguentou muitas das minhas inseguranças, medos e conflitos nesses últimos anos.

SUMÁRIO

1. INTRODUÇÃO.....12
1.1 CONTEXTO HISTÓRICO: DOS 20 CENTAVOS AOS 23 PRESOS.....12
1.1.1 A revolta dos 20 centavos: o levante de massas do Brasil em 2013.....12
1.1.2 A CEIV, a DRCI e o processo dos 23 presos políticos de 2013.....14
1.2 IDENTIFICAÇÃO DO PROBLEMA E MOTIVAÇÃO.....20
1.3 ORGANIZAÇÃO DO TEXTO.....22
1.4 OBJETIVOS.....23
1.4.1 Objetivos gerais.....23
1.4.2 objetivos específicos.....23
2. FUNDAMENTOS TEÓRICOS – ENTENDENDO A CONSTRUÇÃO DE UMA REDE DE VIGILÂNCIA.....24
2.1 CONCEITUANDO A VIGILÂNCIA: DE 1984 AO "CORPO, ALMA E CARTÃO DE CRÉDITO".....24
2.2 AS TICS E A VIGILÂNCIA DIGITAL NO RIO DE JANEIRO CONTEMPORÂNEO: A CONSTRUÇÃO DE UMA REDE DE MONITORAMENTO PREPARADA PARA OS MEGAEVENTOS.....34
3 METODOLOGIA: O USO DA PESQUISA-AÇÃO AO LONGO DA PESQUISA.....39
3.1 SOBRE A PESQUISA-AÇÃO.....39
3.2 TEMAS DA PESQUISA-AÇÃO.....40
3.3 A PESQUISA-AÇÃO NO PLANEJAMENTO E CONSTRUÇÃO DE AÇÕES DE EXTENSÃO PARA COMBATER A VIGILÂNCIA DIGITAL.....45
4. RESULTADOS COLETADOS E DISCUSSÃO.....51
4.1 A I OFICINA DE SEGURANÇA DIGITAL PARA ATIVISTAS.....51
4.2 RESULTADOS COLETADOS.....52
4.3 DISCUSSÃO DOS RESULTADOS.....58
5. CONCEITOS NORTEADORES DO PROBLEMA DA VIGILÂNCIA DIGITAL.....62
5.1 SOFTWARE LIVRE E SOFTWARE PROPRIETÁRIO.....62

5.1.1 *Backdoors* em softwares proprietários.....63
5.2 LEGISLAÇÃO, PRIVACIDADE E ANONIMATO.....64
5.3 CRIPTOGRAFIA E A ESTRUTURA DA INTERNET.....66
6. CONCLUSÃO.....70
6.1 É POSSÍVEL SER ATIVISTA SEM SER VIGIADO?.....70
6.2 CONTINUIDADE DA PESQUISA E TRABALHOS FUTUROS.....71
REFERÊNCIAS.....73
ANEXOS.....77
ANEXO 1: QUESTIONÁRIO DE REAÇÕES DA OFICINA-PILOTO.....77
ANEXO 2: QUESTIONÁRIO DISTRIBUÍDO DE MANEIRA IMPRESSA NO 21º CURSO ANUAL DO NPC (2015) E DISPONIBILIZADO ON-LINE POSTERIORMENTE.....83
ANEXO 3: SLIDES APRESENTADOS NA OFICINA-PILOTO.....89

PEDRO HENRIQUE DA COSTA BRAGA

UMA PROPOSTA DE EXTENSÃO INSPIRADA NA PESQUISA-AÇÃO PARA ATUAR NO COMBATE À VIGILÂNCIA DIGITAL NO RIO DE JANEIRO

HCTE-UFRJ
2018

1. INTRODUÇÃO

Em junho de 2013, aconteceu na cidade do Rio de Janeiro, assim como em diversas outras cidades do país, um aumento nas tarifas dos ônibus, que subiram, no caso do Rio, de R$ 2,75 para R$ 2,95. Contestando esse ajuste tarifário, pequenos protestos tomaram as ruas da cidade, sendo largamente ignorados pela grande mídia. Apesar desse bloqueio midiático, notícias das manifestações chegaram à população em geral através da Internet e das mídias alternativas que estavam cobrindo as passeatas.

Foram essas mesmas lentes da mídia alternativa que foram responsáveis por noticiar a brutal repressão policial aos manifestantes. Imagens da violência do estado viralizaram nas redes sociais e impulsionaram o movimento, transformando as manifestações em uma imensa revolta de massas. Agências bancárias, estátuas, e outros símbolos da ordem foram depredados pelos manifestantes e violentos confrontos com a polícia tomaram as ruas do país[1].

Um ano depois, às vésperas da Copa do Mundo, 23 ativistas foram presos e indiciados, primeiro por quebra de direitos autorais de software e depois por formação de quadrilha armada. Um protagonista dessa repressão foi a Delegacia de Crimes de Informática da Polícia Civil do Rio de Janeiro (DRCI), de onde veio grande parte das informações presentes no inquérito e responsável pela execução do mandato de busca e apreensão que ocorreu um dia antes da abertura da Copa (SOBRAL, 2016).

Se as Tecnologias de Informação e Comunicação (TICs) tiveram um papel importante na organização e convocação dessas manifestações através do midiativismo, também foram usadas para vigiar e reprimir o levante popular. As TICs portanto tiveram um papel dual nesses processos. Se por um lado auxiliaram a organização de massas, por outro auxiliaram a repressão.

1.1 CONTEXTO HISTÓRICO: DOS 20 CENTAVOS AOS 23 PRESOS

1.1.1 A revolta dos 20 centavos: o levante de massas do Brasil em 2013

Em junho de 2013, em diversas cidades ocorreram aumentos nas tarifas de ônibus. Ao mesmo tempo o Brasil se preparava para sediar a Copa do Mundo de 2014 e cifras bilionárias

1Àqueles que desejam se aprofundar nos protestos ocorridos em 2013, sugiro como fonte de pesquisa a dissertação de André Sobral (2016), “Ações coletivas em redes: um estudo de caso sobre o Anonymous Rio”, incluída como referência no presente texto.

estavam sendo gastas nesse evento, enquanto serviços básicos para a população eram deixados de lado:

> Ainda que difusas ideologicamente e extremamente débeis em seus âmbitos organizativo e político-diretivo, as multitudinárias manifestações tiveram como alvo central o alto custo e/ou a obscena precariedade dos serviços públicos básicos, dos quais depende a maioria esmagadora da população brasileira. Tal fato pôde ser verificado nos inúmeros cartazes que clamavam por "mais Saúde", "mais Educação" e pela "redução da tarifa" (ou "passe livre") nos transportes coletivos. Em comparação ao descaso estatal nessas áreas fundamentais, muitos manifestantes questionavam também o alto investimento de recursos públicos nos estádios que receberiam jogos da Copa do Mundo da FIFA (DEMIER, 2015).

Nessa conjuntura, logo assim que o aumento foi anunciado, ocorreram protestos, inicialmente pequenos. Nesse primeiro momento, a estratégia da mídia foi ignorar os protestos de rua, porém midiativistas, através do uso da Internet e das redes sociais, foram capazes de cobrir as manifestações de rua e chamar a atenção do público para aquilo que os meios tradicionais de comunicação buscavam ignorar (DEMIER, 2015). Em resposta, a grande mídia passou a atacar duramente as manifestações, como fez a Folha de São Paulo no seu editorial de 13 de Junho de 2013, intitulado "Retomar a Paulista":

> Oito policiais militares e um número desconhecido de manifestantes feridos, 87 ônibus danificados, R$ 100 mil de prejuízos em estações de metrô e milhões de paulistanos reféns do trânsito. Eis o saldo do terceiro protesto do Movimento Passe Livre (MPL), que se vangloria de parar São Paulo – e chega perto demais de consegui-lo. Sua reivindicação de reverter o aumento da tarifa de ônibus e metrô de R$ 3 para R$ 3,20 – abaixo da inflação, é útil assinalar – não passa de pretexto, e dos mais vis. São jovens predispostos à violência por uma ideologia pseudorrevolucionária, que buscam tirar proveito da compreensível irritação geral com o preço pago para viajar em ônibus e trens superlotados.

Esse editorial terminou com um pedido aberto para que a Polícia Militar reprimisse as manifestações, literalmente: "[é] hora de pôr um ponto final nisso. Prefeitura e Polícia Militar precisam fazer valer as restrições já existentes para protestos na avenida Paulista, em cujas imediações estão sete grandes hospitais". Rômulo Mattos, em seu artigo de 2013, intitulado "Grande imprensa e a repressão policial nas Jornadas de Junho", trata da importância histórica desse editorial:

> Esse editorial da *Folha de São Paulo* é um documento histórico da maior validade. Ele mostra como a brutalidade policial foi abertamente apoiada e mesmo incentivada pela

> grande imprensa nas primeiras manifestações brasileiras. Os profissionais de tal instituição trataram os manifestantes como vândalos e os colocaram como responsáveis pelos congestionamentos no trânsito da capital paulistana. Nesse sentido, as passeatas sangrariam a democracia de um país por impedir a prática do direito individual de ir e vir. Não obstante, vale reforçar que a criminalização dos movimentos sociais foi a tônica de seu conteúdo.
>
> A questão é que a barbárie protagonizada pelos policiais, a estigmatização dos manifestantes promovida pelos jornalistas e, é claro, a organização e a justeza da luta empreendida pelos movimentos sociais, que vinha crescendo nos últimos anos, levaram a uma alteração na correlação de forças. No dia 20 de junho de 2013, o instituto de pesquisas Datafolha revelou que 65% dos paulistanos eram favor de que a Avenida Paulista fizesse parte da rota de manifestações na cidade de São Paulo (ou seja, dois em cada três moradores da capital paulistana). Esse apoio ficava muito acima da média entre os jovens (81% apoiavam manifestações na Paulista) e entre aqueles que têm nível superior (77%) (MATTOS, 2013)

A violência policial tomou as mídias sociais e se viralizou, aumentando o contingente das manifestações em todo o país e a insatisfação popular com os governos federal e estaduais e municipais. Pressionados, os governantes em diversas capitais voltaram atrás no aumento tarifário (G1, 2013).

1.1.2 A CEIV, a DRCI e o processo dos 23 presos políticos de 2013

No dia 19 de julho de 2013, através do decreto 44.302, o governo do estado do Rio de Janeiro criou a Comissão Especial de Investigação de Atos de Vandalismo em Manifestações Públicas – CEIV. Segundo o texto do decreto, a comissão foi criada com o propósito de investigar grupos que causavam danos a patrimônio público e privado durante manifestações:

> [c]onsiderando os recentes e reiterados acontecimentos envolvendo atos de vandalismo perpetrados por grupos organizados, causadores de danos à incolumidade física de pessoas e destruição do patrimônio público e privado; e a necessidade de as instituições públicas incumbidas da defesa do Estado Democrático de Direito se organizarem para promover uma maior eficiência na investigação e na tomada de providência para a prevenção da ocorrência de novos atos de vandalismo e punição das práticas criminais já perpetradas (RIO DE JANEIRO, 2013)

A CEIV era composta por membros do Ministério Público do Estado do Rio de Janeiro, Secretaria de Segurança do Estado do Rio de Janeiro e das polícias Civil e Militar. O decreto também atribuía à comissão os poderes de “tomar todas as providências necessárias à realização da

investigação da prática de atos de vandalismo, podendo requisitar informações, realizar diligências e praticar quaisquer atos necessários à instrução de procedimentos criminais com a finalidade de punição de atos ilícitos praticados no âmbito de manifestações públicas", cabendo às operadoras de telefonia e aos provedores de internet o dever de atender os pedidos de informações da CEIV dentro de um prazo máximo de 24 horas (RIO DE JANEIRO, 2013).

O decreto foi criticado por juristas, que apontavam a atribuição à Polícia Militar do poder de investigação como ilegal, poder que todavia só caberia à Polícia Civil. Em entrevista ao G1, concedida no dia 23 de julho, Ivar Hartman, professor do Centro de Justiça e Sociedade da Fundação Getúlio Vargas, afirmou que "há uma série de problemas que tornariam esse decreto inconstitucional. A PM não exerce função de investigação, e sim, policiamento ostensivo. A PM não investiga crime, isso cabe à Polícia Civil" (HARTMAN, 2013 apud SOUZA et al, 2013). No dia 24 de julho, o decreto sofreu um adendo: "Observar-se-á a reserva de jurisdição exigida para os casos que envolvam quebra de sigilo." A CEIV portanto precisaria de ordem judicial para solicitar a quebra de sigilo de ligações telefônicas e de Internet. Além disso o novo texto trocou o prazo de 24 horas para as empresas de telecomunicação liberarem os dados solicitados pela comissão pela "prioridade para o atendimento dos pedidos de informações formulados pela CEIV ou decorrentes de ordem judicial nos casos de sigilo previstos na legislação" (RIO DE JANEIRO, 2013).

Segundo Larissa Azevedo[2], em entrevista pessoal concedida ao autor em janeiro de 2016, a CEIV passou a realizar o que chamaram "rondas virtuais" em redes sociais, com destaque para o Facebook. Essas rondas não tinham como alvo os ativistas que foram de fato processados. O foco inicial da Polícia Civil foi o "pessoal que estava sempre sem máscara, sempre na frente dos atos e sempre brigando muito na Internet […] um pessoal que um mês antes, na [manifestação] de um milhão, estava pintado de verde-e-amarelo[3]". A entrevistada ainda ressalta o papel da mídia em "criar personagens que não existiam", citando o caso de Elisa Quadros, conhecida como Sininho:

2 Advogada no caso dos 23 presos políticos das manifestações de 2013. Segundo a entrevistada, os ativistas foram representados por uma equipe de cerca de 10 advogados da qual ela faz parte.

3 A manifestação referida aconteceu no dia 20 de junho de 2013 e ocupou a Avenida Presidente Vargas no Rio de Janeiro. A manifestação foi marcada pela falta de unidade dos manifestantes em torno de um programa político, com indivíduos e grupos de todos os lados do espectro político, desde comunistas e anarquistas até integralistas e monarquistas, ocupando a rua. Por "ir de verde-e-amarelo", a entrevistada se refere a manifestantes sem experiência política e clareza ideológica, que foram para o ato movido apenas pela insatisfação com o governo e com a situação do país no momento. Muitos desses manifestantes foram à manifestação vestindo a camisa da seleção brasileira de futebol, daí o termo empregado.

> Ela [Elisa Quadros] é uma pessoa que nunca teve poder de decisão no movimento, [apesar de] que foi colocada como uma grande líder do movimento. Como se fosse possível que ela liderasse anarquistas, maoistas, o pessoal do PSOL e mais de não sei onde que eles queriam juntar como sendo um movimento coeso. Qualquer um que estuda história sabe que não é possível juntar marxistas e anarquistas, que tem diferenças que vão desde antes da Revolução Russa, em torno de uma única liderança, de uma única pessoa. Era claro que ela não era nada (AZEVEDO, 2016).

Em entrevista concedida à Agência Pública, periódico online de jornalismo investigativo, em 13 de Abril de 2017, a própria Elisa Quadros também afirmou que não era líder de movimento algum e que a "Sininho" era uma construção da mídia:

> A "Sininho" é uma construção midiática. Eu estou começando a entender um pouco melhor e a parar para pensar sobre tudo o que aconteceu. É assim que eles funcionam: a mídia, o Estado, eles precisam de uma liderança. Mas não teve liderança. Tinha pessoas que têm facilidade de assumir mais coisas, mas isso não significa uma liderança. Eu sou produtora, então sou muito rápida. Eu não tenho paciência, sou muito brava. Eu avalio hoje que, das pessoas que estavam mais ativas, eu fui escolhida para ser o bode expiatório.
>
> E aí você faz uma avaliação de critérios morais. Nesse país machista em que a gente vive, destruir mulher é fácil. Branca, hétero, classe média. Usaram muito o argumento de "rebelde sem causa". E o moralismo do machismo. Moralismo religioso: cara de vagabunda, destruidora de lares, "ela usa sedução para conseguir as coisas"… Virei "líder de Black Blocs". Gente, pelo amor de deus, eles não têm líder, eles usam uma tática, começa por aí. Eu nunca usei a tática, sou de outras táticas, por isso que eu nunca tampei o rosto. Gente, é uma tática política de ataque ao capital! (QUADROS, 2017 apud SIMÕES et al, 2017)

Segundo Azevedo, em virtude do pouco conhecimento das organizações de esquerda por parte dos agentes de repressão do estado, algumas ligações que não condiziam com a realidade foram incluídas nos inquéritos do que viria a ser o processo dos 23 presos políticos, como, por

exemplo, ligar a FIP[4] ao PSOL. Larissa conta como a CEIV partiu desse público para os ativistas que foram presos:

> Depois de milhões de depoimentos, onde eles foram atrás dessa galera mais perdida, eles foram atrás da Gerusa[5], e a partir de um *post* dela no Facebook eles acharam o nome de dois militantes do Anonymous[6]. […] Isso levou à prisão [das primeiras pessoas] […] Quando apareceu na TV que existia um mandado de busca e apreensão para eles, um ex-namorado de uma das acusadas foi na delegacia e entregou os demais. Aí que eles pegam o resto dos 23 (AZEVEDO, 2016).

A entrevistada diz que, depois dessa etapa, a polícia passou a grampear os 23 então suspeitos e a vigiá-los, citando o caso de uma reunião da Organização Anarquista Terra e Liberdade – OATL, cujos participantes foram fotografados na entrada e na saída. Larissa ainda aponta que "uma parte da galera não conhecia outra parte da galera, ninguém conhecia o Tiago [Rocha][7] por exemplo. Alguns não conheciam-se nem em ato, só se conheceram em Bangu[8]" (AZEVEDO, 2016).

Com o decreto Nº 44409, de 26/09/2013, a CEIV foi extinta e as investigações foram assumidas pela Delegacia de Repressão a Crimes de Informática da Polícia Civil do Estado do Rio de Janeiro (DRCI). Segundo Larissa, "a DRCI tomou o caso como sendo o grande caso deles. Tinham que prender de qualquer maneira". A entrevistada fala que em seus contatos com os agentes

---

4 Frente Independente Popular, uma frente de organizações anarquistas como a Organização Anarquista Terra e Liberdade (OATL), União Popular Anarquista (UNIPA) e maoistas como o Movimento Estudantil Popular Revolucionário (MEPR) e a Unidade Vermelha (UV). Dentre os principais elementos agregadores da frente figurava a denúncia do que chamam de "farsa eleitoral", isto é a falta de democracia do processo eleitoral do estado democrático burguês, e a defesa do voto nulo como parte da estratégia revolucionária. Outro importante ponto de unidade era a defesa da ação direta organizada como forma de derrotar o capital.

5 Gerusa Lopes, militante do movimento Dia do Basta, organização que luta pelo combate à corrupção na política parlamentar. Esse movimento foi defensor da criação da Lei Complementar n° 135/2010 (Lei da Ficha Limpa) e hoje luta pela aplicação dessa lei nas eleições.

6 Organização midiativista nascida da Internet. Para mais informações sobre essa organização, ler a dissertação de mestrado de André Sobral (2016).

7 Midiativista e réu no caso dos 23 presos políticos.

8 Presídio de Gericinó, onde ficaram os 23 ativistas presos.

da DRCI, ela pode presenciar esses policiais discutindo detalhes pessoais dos seus vigiados, numa relação que chamou de "inimigos íntimos" (AZEVEDO, 2016).

Thiago Rocha conta que a DRCI obteve todas as informações para montar o processo sem usar de muitos conhecimentos técnicos: "o que mais recheia o processo são *prints* de conversas públicas no Facebook" (ROCHA, 2016). Para o entrevistado "A capacidade de repressão do estado brasileiro é muito primária.[9] O que tem nos processos são escutas telefônicas, postagens públicas e o que eles receberam por intimação do Google e do Facebook e outras empresas. Não tem nenhuma quebra de criptografia no processo. […] Em nível estadual, eu não acredito que eles têm qualidade técnica para isso [para quebra de criptografia]. Em nível federal eu não sei, talvez sim. Teve um vazamento de e-mails trocados entre o pessoal da DRCI e a *Hacking Team*[10], então existe interesse de terceirizar essa vigilância" (ROCHA, 2016).

De fato, ao observar os inquéritos, a imensa maioria das informações obtidas nas chamadas rondas virtuais foram obtidas a partir de capturas de telas de postagens públicas no Facebook dos investigados. Na ronda virtual do dia 01 de março de 2014, a DRCI chegou a admitir que só conseguiu informações do grupo fechado do Facebook "Anonymous Rio" devido ao fato de outro membro ter vazado informações dessa comunidade ao restante da rede social:

> Ocorre que a sucessão de diálogos capturados em *print screens* da tela (sic) só foi possível de ser coletada em razão de uma cisão entre os próprios membros da Comunidade Anonymous Rio, que foi "'hackeada'" por um de seus frequentadores, expondo dados sobres os administradores da página, suas vinculações políticas e objetivos pessoais (RIO DE JANEIRO, 2013, p.3).

---

9 A afirmação do entrevistado, apesar de adequada para a capacidade de repressão empregado no caso dos 23, protagonizado pela Polícia Civil do estado do Rio de Janeiro, é problemática se usada para analisar a capacidade de vigilância do estado brasileiro como um todo. Tratarei mais dessa questão no capítulo 2.

10 Empresa italiana especializada em fornecer serviços de vigilância digital para estados interessados em monitorar as atividades de seus cidadãos na Internet. Em e-mail vazados no WikiLeaks, a empresa afirma ter realizado demonstrações de produtos para a ABIN, a Procuradoria-Geral da União, o Exército Brasileiro, a Polícia Federal e a departamentos de Polícia Civil. As mensagens vazadas estão disponíveis em https://www.wikileaks.org/hackingteam/emails/emailid/7226. Esta empresa será revista no capítulo 2.

Em caráter anedótico, Larissa relatou fragmentos do inquérito onde a DRCI mostrou-se incapaz de quebrar a criptografia empregada pelos ativistas:

> Tem uma parte muito interessante [do inquérito], onde eles [a DRCI] estavam monitorando o CMI[11], e ficaram frustrados[12] por que o CMI usava o TOR[13] para acessar a plataforma deles […] Eles falam essa hora do TOR, e falam também do Telegram[14], se referem a ele como sendo "irrastreável", eles usam essa palavra (AZEVEDO, 2016).

Além de buscar informações públicas, a DRCI também dispôs de técnicas de coerção a fim de levar alguns investigados a fornecerem senhas de redes sociais. A polícia também conseguiu infiltrar um policial em um grupo do Telegram usando um perfil falso e obteve algumas informações a partir de mandados judiciais de quebra de sigilo: "O Facebook forneceu dados de pesquisa que [os investigados] tinha[m] feito. Era isso, [policiais] pesquisando páginas, grupos, *profiles* [dos investigados]" (AZEVEDO, 2016).

No dia 11 de junho de 2014, véspera da abertura da Copa do Mundo, a Polícia Civil executou um mandado de busca e apreensão contra os ativistas que vinham sendo monitorados nas rondas virtuais. Tiago Rocha relata o evento, em entrevista concedida em 2015 à André Sobral:

> Foram lá com um mandado de busca e apreensão de objetos eletrônicos, mídias digitais e bomba. Eu pedi para ler e estava lá "quebra de direito autoral de software". Quando ele [o agente da DRCI] chegou, pegou o telefone da minha mão e começou a tirar foto. Eu tinha começado a avisar o povo sobre o que estava acontecendo, nessa semana o nome do grupo tinha sido mudado para "O Badernista RJ", e tive que explicar a eles que mudar o nome do chat não me fazia parte do Badernista ou da Polícia Civil se o título fosse esse. Questionei que ele não podia fazer aquilo e ele acabou desistindo e apagando as imagens e devolvendo meu celular, aí guardei em casa para ninguém tomar de mim de novo. Vasculharam tudo em minha casa, pegaram coisas de minha mãe, de meu irmão, que tinha só doze anos, reviraram meu armário e jogaram tudo no chão. Naquele momento só senti muita raiva. Tentei argumentar com eles que não podia, mas não tinha diálogo. Foram pegar a minha máscara de V de Vingança, tentei discutir que eles não podiam pegar, mandei eles lerem o mandado, que não

11 Centro de Midia Independente, um coletivo midiativista.

12 A entrevistada usou a palavra de baixo calão p*****.

13 The Onion Router, ferramenta de criptografia usada para mascarar o tráfego de rede e o IP da máquina. Para mais informações acesse: https://www.torproject.org/.

14 A afirmação da Polícia Civil é problemática. No mesmo ano das investigações (2013) fora descoberta uma falha na criptografia implementada pelo Telegram. Para mais informações acesse: http://www.cryptofails.com/post/70546720222/telegrams-cryptanalysis-contest

> dizia nada de máscara. Eles responderam que tinha que levar qualquer coisa que pudesse ser usada para praticar atos violentos. Perguntei se eles iam levar meu travesseiro que podia sufocar alguém, se iam levar minha caneta que podia matar alguém. São três homens armados que, em tese, são autoridades de alguma coisa. Levaram teclado, bateria externa, bombinha de São João de meu irmão pequeno, quase levaram uma camisa do Homem de Ferro por que tinha uma bateria embutida que acendia luzes na camisa. Me falaram que eu tinha que ir para a delegacia naquele momento. Eu não sabia se estava sendo preso, era minha primeira experiência, queriam até que eu fosse sozinho no carro deles. Meu irmão ficou muito assustado, não ficava mais sozinho em casa por que disseram que iam arrombar se ninguém atendesse a porta. Ele não gosta mais que falem de política porque as pessoas que fazem isso vão presas. Minha avó que estava lá em casa ficou chorando enquanto me levavam (ROCHA, 2015 apud SOBRAL, 2016).

Para Tiago, o objetivo da sua prisão e de outros midiativistas foi silenciar a mídia alternativa para possíveis manifestações de ruas que ocorressem durante a Copa do Mundo:

> Como eu avalio essa busca e apreensão: Ela foi realizada um dia antes da abertura da Copa. Nós éramos de um coletivo de mídia, e todos os nossos equipamentos eletrônicos foram apreendidos, nos deixando incomunicáveis. A gente não seria capaz de fazer a cobertura, isso era uma censura (ROCHA, 2016).

1.2 IDENTIFICAÇÃO DO PROBLEMA E MOTIVAÇÃO

Meu primeiro contato com a segurança da informação se deu em 2010, enquanto cursava o segundo ano da graduação em Ciência da Computação. Foi quando entrei para o GRIS (Grupo de Resposta a Incidentes de Segurança), laboratório e projeto de extensão do DCC[15]. Esse projeto era um espaço extremamente privilegiado e horizontal, onde os alunos de Computação se reuniam para aprender juntos sobre segurança, dar cursos sobre temas relacionados e resolver incidentes que ocorressem em laboratórios da UFRJ, caso fossem solicitados e autorizados pelos responsáveis pelo laboratório em questão. O GRIS é orientado por dois professores do DCC, mas na época em que fui membro do projeto, esses docentes tinham um papel mais próximo de guias pela burocracia da UFRJ, em especial os editais internos da pró-reitoria de extensão, e de provedores de espaço e equipamentos, do que um papel de formadores ativos dos estudantes membros do projeto. O ensino e o aprendizado ficavam por conta dos próprios alunos que trocavam conhecimento e experiências de forma simétrica e horizontal entre si. Permaneci no GRIS de 2010 até o final de 2012.

15 Departamento de Ciência da Computação da UFRJ

Nesse mesmo ano, comecei a participar do movimento estudantil da UFRJ e, assim como muitos outros de minha geração, fui às ruas nos protestos de junho de 2013. A Segurança da Informação não era uma preocupação do movimento; atos foram marcados e organizados por Facebook, perfis pessoais eram usados de forma indiscriminada pelos militantes sem nenhuma preocupação com vigilância digital. No ano seguinte, porém, o caso dos 23 presos políticos e o aumento da repressão policial aos movimentos sociais devido ao contexto de megaeventos em que vivia a cidade do Rio de Janeiro, colocaram na ordem do dia a necessidade dos grupos contra-hegemônicos[16] se preocuparem com a vigilância digital. Proponho com este estudo a investigação da relação desses coletivos com as TICs e a sua percepção da vigilância digital. Para isso, utilizei como ferramenta um experimento pedagógico que consistiu na realização de um circuito de seminários de segurança da informação e contra-vigilância digital para grupos contra-hegemônicos.

Essa escolha metodológica, inspirada pela Pesquisa-Ação, da qual tratarei no capítulo 3, foi consequência do meu contato com o SOLTEC-UFRJ (Núcleo de Solidariedade Técnica da UFRJ) e com experiências prévias do uso da metodologia da Pesquisa-Ação por esse laboratório. O SOLTEC é um programa de extensão do Centro de Tecnologia da UFRJ, de caráter interdisciplinar, que desenvolve projetos em rede com abordagem territorial e participativa, atuando nos campos da tecnologia social e da autogestão, com o objetivo de promover a equidade social e o equilíbrio ambiental. Uma das linhas de ação do SOLTEC se chama TIFS (Tecnologias da Informação para Fins Sociais), que teve como última ação a construção de um portal comunitário da Cidade de Deus[17], comunidade periférica localizada na Zona Oeste do Rio de Janeiro. Esse projeto foi iniciado

16 O conceito de hegemonia e contra-hegemonia por si só já mereceria um estudo próprio. Dessa forma, considera-se, para fins práticos nesse estudo, como sendo grupos contra-hegemônicos aqueles que contestam, respeitando as particularidades político-ideológicas, a ordem vigente do estado contemporâneo e do capitalismo globalizado. Dentro dessa categoria encontram-se partidos políticos, coletivos e movimentos sociais, populares e sindicais que tenham como objetivo a transformação da sociedade em uma mais justa e humana. Esses grupos também variam no espectro político entre a extrema-esquerda ostensivamente revolucionária até a centro-esquerda social-democrata, passando por uma miríade de ideologias políticas. Também variam em local de militância e formas de atuação e organização. Não pretendo com esse trabalho colocar em uma "escala de contra-hegemonia" os diferentes tipos de movimento e suas relações com o estado estabelecido, ou seja, aqui procurei analisar os diferentes grupos pelos mesmos termos.

17 Para mais informações sobre a construção do Portal Comunitário da Cidade de Deus, ler a tese de Alvear (2014), "Tecnologia E Participação: Sistemas de Informação e a Construção de Propostas

em 2008 e tinha como objetivo final a produção de um site na Internet onde os diversos atores locais da Cidade de Deus pudessem divulgar suas atividades, fortalecendo as instituições desse território. Para a construção participativa do portal com os atores locais, foi necessário uma série de entrevistas e reuniões para envolver a comunidade com a construção do projeto. Se o produto final, o Portal Comunitário, só foi obtido a partir da participação da comunidade e das visões dos diferentes atores sobre qual deveria ser o papel daquele artefato, acredito que um mapeamento das percepções da vigilância digital pelos diferentes grupos contra-hegemônicos também precisa ser obtido como fruto de um processo participativo que envolva esses grupos.

1.3 ORGANIZAÇÃO DO TEXTO

O segundo capítulo, por sua vez, está dividido em duas seções. A primeira apresenta um resumo da bibliografia empregada no texto, desenvolvendo-se ao longo dos eixos da vigilância e dos estudos de Ciência, Tecnologia e Sociedade (CTS), em especial os trabalhos de Latour (2000), Cukierman et al (2007), Marques (2005) e Law(1992). Também são utilizados como referências os conceitos de Sociedade de Controle (FOUCAULT, 1975) e de Sociedade de Vigilância (LYON, 1994) e a ontologia do Rizoma (DELEUZE e GUATTARI, 1995). Na segunda seção, parto de fontes jornalísticas para narrar a história de como se deu a construção de uma rede de vigilância preparada para receber os megaeventos que aconteceriam no Rio de Janeiro.

No capítulo 3, foco na metodologia empregada para a construção do trabalho de campo, a Pesquisa-Ação tal como apresentada nos trabalhos de Fals Borda (1991), Alvear (2014), Thiollent (1986), Addor (2005) e Lianza (2005). Tal como o capítulo anterior, também divido esse em duas seções, a primeira explicando a metodologia segundo os autores previamente mencionados e a segunda explicando como empreguei a metodologia ao longo do mestrado.

No quarto, relato a principal ação da Pesquisa-Ação realizada até a finalização desse texto e discorro sobre os dados levantados em campo, articulando-os com a bibliografia.

No quinto capítulo explico brevemente os conceitos discutidos com os participantes da oficina piloto.

O sexto e último capítulo contem as considerações finais.

Coletivas para Movimentos Sociais e Processos de Desenvolvimento Local", incluída como referência no presente texto. Recomendo também a leitura da dissertação de mestrado de Luiz Arthur (2010) "Softwares Livres, Economia Solidária e O Fortalecimento de Práticas Democráticas: Três Casos Brasileiros" disponível em: http://www.cos.ufrj.br/uploadfile/1287490984.pdf (acessado em 10/01/2018)

1.4 OBJETIVOS

1.4.1 Objetivos gerais

Essa dissertação de mestrado tem como objetivo estudar a relação dos militantes organizados em grupos contra-hegemônicos que atuam na Região Metropolitana do Rio de Janeiro com as Tecnologias da Informação e Comunicação (TICs) e como o risco de vigilância digital configura e é configurado por essas relações. Além disso, esse estudo se propõe a experimentar uma intervenção da Universidade nessa temática, e a partir dessa experiência planejar futuras ações extensionistas.

1.4.2 objetivos específicos

- Acompanhar e descrever a construção participativa, com movimentos contra-hegemônicos, de uma série de oficinas orientadas aos temas de vigilância digital e segurança da informação e voltadas para esses mesmos grupos.
- Extrair, dessas oficinas, informações relativas à visão que os movimentos sociais possuem da vigilância digital sofrida por eles e como ela afeta sua relação com as TICs.
- Construir a partir dessas informações um mapa das redes de vigilância existentes no Rio de Janeiro.
- Propor futuras ações que possam ser realizadas pela Universidade, em parceria com os movimentos sociais, para atuar na questão da vigilância digital.

2. FUNDAMENTOS TEÓRICOS – ENTENDENDO A CONSTRUÇÃO DE UMA REDE DE VIGILÂNCIA

2.1 CONCEITUANDO A VIGILÂNCIA: DE 1984 AO "CORPO, ALMA E CARTÃO DE CRÉDITO"

O que é vigilância? Podemos começar essa discussão por uma definição de dicionário: segundo a coletânea *The Encyclopedia of Privacy,* organizada por William G. Staples (2007), a vigilância não deve ser caracterizada como o oposto de privacidade, ainda que essa manifeste-se em muitos casos como "os meios usados para cruzar as barreiras que protegem a privacidade"[18] (MARX 2007, p. 535). Segundo essa enciclopédia, essa definição, que como veremos adiante, não é a única, está fortemente associada com a coleta, através de meios eletrônicos, químicos e estatísticos, de informação pessoal capaz de identificar um indivíduo (MARX, 2007, p. 535).

Ao se deparar com essa definição de vigilância, o leitor pode lembrar de inúmeras distopias produzidas pela literatura de ficção científica. Um caso especial é o do livro *1984*, de George Orwell. Nele o protagonista, Winston Smith, tal como os demais personagens do livro, é constantemente monitorado por um governo totalitário. Um artefato icônico utilizado no livro para vigiar os cidadãos é a teletela: um híbrido de televisão e câmera de segurança, obrigatoriamente presente em todas as residências e na maioria dos espaços públicos. Através desse dispositivo, que não podia ser desligado, o regime era capaz de, ao mesmo tempo, monitorar seus cidadãos e transmitir a propaganda governamental, 24 horas por dia.

Segundo David Lyon, ainda que a distopia orwelliana já esteja tecnologicamente datada, alguns de seus aspectos se mantêm relevantes para ilustrar o que chama de sociedade de vigilância (LYON, 1994, p. 58). Lyon usa o conceito de sociedade de vigilância para ilustrar o contexto atual nos quais sistemas computacionais, tanto de entes estatais quanto privados, possuem uma série de informações pessoais de uma parcela considerável da população:

> Organizações de diversos tipos nos conhecem apenas como sequências de números e letras. Antigamente isso era guardado em pedaços de papel ordenados em pastas e guardados em armários, porém atualmente essas mesmas tarefas – e muitas outras, inimagináveis para um escriturário dos tempos vitorianos – são realizadas por computadores. Detalhes precisos das nossas vidas pessoais são coletados, armazenados, consultados e processados todo dia em vastos bancos de dados computacionais pertencentes a grandes corporações e repartições públicas. Isso é a 'sociedade de vigilância' (LYON, 1994, p.3)[19].

18 *"Surveillance may be the means of crossing borders that protect privacy."* (tradução do autor)

No romance 1984, Winston afirma que não sabe se todas as teletelas estão sendo monitoradas a todo instante, isto é, se de fato todos os cidadãos são vigiados 24 horas por dia, 7 dias por semana, porém o sentimento para a população da Oceania, um dos estados-nações da obra de Orwell, é de monitoramento constante. De maneira análoga ao romance, no mundo contemporâneo não se sabe o escopo da vigilância, não temos a dimensão real da vigilância:

> Ninguém está nos espionando, exatamente, porém para muitas pessoas esse é o sentimento que fica se e quando elas descobrem o quão detalhado é o retrato de nós que está disponível. 'Eles' sabem coisas sobre nós. Porém, geralmente, nós não sabemos o que eles sabem, o porquê deles saberem o que sabem, ou com quem eles podem compartilhar esse conhecimento. (LYON, 1994, p.4)[20].

Ainda segundo o autor, ninguém está sendo vigiado diretamente, no sentido de que não existe um espião nos observando através da janela. Porém experimentamos essa sensação de invasão quando nos damos conta da vigilância decorrente do uso de sistemas computacionais que coletam dados indiscriminadamente dos seus usuários. Esse sentimento, segundo o autor, é potencializado pelo fato de não sabermos, em detalhes, quais informações estão sendo coletadas de nós, com qual propósito elas estão sendo coletadas e com quem estão sendo compartilhadas.

Voltando novamente ao mundo de 1984, na distopia de Orwell é sabido que grande parte da população não é vigiada, visto que a vigilância limita-se apenas aos membros do partido dirigente da sociedade. Isto é: vigia-se apenas aqueles que importam, e para ascender socialmente é necessário submeter-se à vigilância. No nosso cenário atual, não existe um partido dirigente que vigie seus membros, mas paralelos podem ser traçados: a vigilância se torna o "pedágio" que pagamos para consumir através dos nossos cartões de crédito, e/ou acessar os aplicativos dos nossos *smartphones* que requisitam dados de geolocalização para funcionar, e/ou ainda interagir através

---

19 Essa citação, tal como as demais provenientes desse livro foram traduzidas por mim. Texto original: "*organizations of many kinds know us only as coded sequences of numbers and letters. This was once worked out on pieces of paper collated in folders and kept in filling cabinets, but now the same tasks – and many others, unimaginable to a Victorian clerk – are performed by computer. Precise details of our personal lives are collected, stored, retrieved and processed every day within huge computer databases belonging to big corporations and government departments. This is the 'surveillance society'*".

20 Texto original: *"No one is spying on us, exactly, although for many people that is what it feels like if and when they find out just how detailed a picture of us is available. 'They' know things about us, but we often don't know what they know, why they know, or with whom else they might share their knowledge."*

das redes sociais. Para participar desta sociedade de maneira plena é necessário submeter-se à vigilância. Lyon, ainda em 1994 quando essas tecnologias ou não existiam ou ainda estavam em sua infância, já utilizava a metáfora do passaporte para problematizar para a vigilância.

> Passaportes nos permitem atravessar fronteiras, nas quais nossas carteiras de motoristas são levadas mais seriamente do que nossa palavra na hora de provar quem nós somos. Em grande parte da vida moderna, lidamos com estranhos relativos e para demonstrar nossa identidade e confiança devemos ser capazes de apresentar prova documental. De fato o provérbio russo apresentado acima[21] deveria ser atualizado para indicar que nós seres humanos somos identificados de forma mais precisa como compostos por 'corpo, alma e cartão de crédito'. (LYON, 1994, p.3)[22]

Uma diferença marcante entre a vigilância de 1984 e a presente em nossas sociedades informacionais do século XXI (CASTELLS, 1996) se dá em relação ao agente central da vigilância. No romance de Orwell, o único responsável pela vigilância é o governo totalitário da Oceania. No cenário contemporâneo, além do estado a vigilância é praticada por entes privados.

Um cenário onde a vigilância ocorre de maneira intensa é o interior das fábricas, na linha de produção do capitalismo moderno. Segundo Lyon, enquanto modos de produção anteriores necessitavam da violência, ou da ameaça de violência, para coordenar grandes números de trabalhadores, no capitalismo isso não ocorre, uma vez que nele os trabalhadores são, no sentido jurídico, livres. Então, se fez necessária uma nova forma de controle dos trabalhadores, de forma que esses mantenham-se produzindo o máximo possível pelo menor custo (LYON, 1994). Em outras palavras,

> [o] que nós hoje conhecemos como 'gestão' foi desenvolvido para monitorar os trabalhadores e para garantir sua obediência enquanto força de trabalho disciplinada. A ideia de trazer todos os trabalhadores para baixo de um mesmo teto, em fábricas e oficinas, foi vista como uma forma de maximizar a eficiência técnica, fazendo uso completo do maquinário, etc. Porém, pode-se igualmente argumentar que o uso de fábricas para garantir a

---

21 Lyon abre esse capítulo com o seguinte provérbio russo: "Um indivíduo na Rússia é composto de três partes; um corpo, uma alma e um passaporte".

22 Texto original: *"Passports get us across borders, who drivers' licences are taken more seriously than our own word for proving who we are. In much of modern life we deal with relative strangers, and to demonstrate our identity or reliability we must produce documentary evidence. Indeed, the Russian*

proverb above should really be updated to indicate that human beings would now be defined more accurately as 'body, soul and credit card'."

> disciplina de trabalho através do monitoramento dos trabalhadores foi tão importante quanto, senão mais (LYON, 1994, p.25)[23].

Podemos relacionar esse aspecto da vigilância com o que Foucault define como o surgimento da sociedade disciplinar ao longo do século XIX. Para, o autor, as sociedades anteriores, protagonizadas pelo suplício, isto é, pela punição violenta dos transgressores, davam espaço para uma nova ordem social, protagonizada pelo poder disciplinar (FOUCAULT, 1975). Esse poder, segundo Foucault, era comedido, discreto, racional e sempre presente, buscando a todo tempo adestrar as grandes multidões de forma a controlá-las e garantir sua produtividade (FOUCAULT 1975). Segundo Ferreira, "a eficiência do poder disciplinar se deve à associação íntima ao poder de vigilância, parte integrante de suas engrenagens e que se dissemina por meio de uma rede de relações ramificadas em todas as direções" (FERREIRA, 2014, p. 113). Isto é, para controlar os as massas e mantê-las produtivas e obedientes, os estados modernos têm a vigilância como necessidade.

Um outro aspecto da vigilância moderna é o monitoramento crescente de consumidores em potencial por parte de grandes empresas. Essa prática se tornou uma parte crucial do modelo de negócio dessas corporações, influenciando em decisões de marketing e de negócios, que vão desde quais serviços uma empresa decide fornecer, em quais localidades ela decide operar, quais investimentos são feitos com quais consumidores, e mais ainda [24:]

> A vigilância dos consumidores, e por extensão do seu consumo, contribui e depende da 'economia da informação pessoal' - um contexto em que o uso de dados pessoais identificáveis tornou-se um recurso primário sobre o qual são construídas muitas economias de mercado. A economia da informação pessoal depende da coleta de dados através de sistemas de vigilância e depois da análise destes dados em comparação com padrões e categorias consideradas 'de valor', reavaliando continuamente as práticas e produtos corporativos com base nessas análises. Este processo cíclico destina-se a obter a máxima rentabilidade, tanto atual quanto potencial, a partir de diferentes conjuntos de consumidores (PRIDMORE, 2012, p. 321)[25].

---

23 Texto original: *"Hence what we now know as 'management' was developed to monitor workers and to ensure their compliance as a disciplined force. The idea of bringing workers together under one roof, in factories and workshops, has often been seen as a way of maximizing technical efficiency, making full use of machinery, and so on. But it can equally well be argued that the use of factories to ensure labour discipline through the oversight of workers' activities was at least as important, if not more so."*

24 Essa citação, tal como as demais provenientes desse livro, foram traduzidas pelo autor.

Um ator protagonista nesse aspecto da vigilância são as aplicações da Web 2.0, como o Facebook, o Twitter ou o Instagram. Essas aplicações coletam um volume brutal de informações dos seus usuários. Esses dados são armazenados, comparados, avaliados e vendidos de forma sistematizada, oferecendo um panorama do comportamento digital dos usuários. Esse panorama pode ser comparado com os demais utilizadores do sistema, com a finalidade de estipular perfis e direcionar a propaganda e o consumo (ESTEVÃO, 2014). É importante notar que essa vigilância tem como requisito que o usuário aceite ser vigiado, tanto no momento que em que esse aceita um termo de uso que permite a coleta de informações, quanto quando alimenta a rede com fotos, *check-ins*, vídeos, textos, etc.

As redes sociais também são parte fundamental de outro aspecto da vigilância, a vigilância lateral ou *peer-to-peer* (ESTEVÃO, 2014). Trata-se da vigilância que os usuários das redes sociais ao mesmo tempo sofrem e executam ao usarem essas redes. Um exemplo: ao usar o Facebook, um usuário comum pode compartilhar uma foto, dessa forma se submete à vigilância dos seus contatos nessa rede, ao mesmo tempo que é capaz de vigiar seus conhecidos a partir das informações que esses publicam nas redes sociais. Esse tipo de vigilância também pode ser estimulada pelo estado, como ocorreu em 2013 no 4chan[26] após o atentado de Boston:

> A introdução das redes sociais no processo da procura dos suspeitos dos atentados da Maratona de Boston foi amplamente difundida pelas autoridades norte-americanas, mobilizando a comunidade civil a agir em prol da segurança nacional. É de evidenciar neste processo o papel de comunidades

25 Texto original: *"The surveillance of both consumers and their associated consumption contributes to and is reliant upon the 'personal information economy'— a context in which the use of personally identifiable data has become a primary resource and upon which many market economies are built. The personal information economy depends upon the gathering of data through surveillance systems and then analyses this data for patterns and associations deemed to be 'of value,' continually re-evaluating corporate practices and products based on these analyses. This circular process is directed towards obtaining the maximum current and potential profitability from differing sets of consumers"*

26 Lançado em 1 de outubro de 2003, o 4chan é um fórum onde os usuários podem publicar imagens e textos anonimamente, com as postagens mais recentes aparecendo acima das mais antigas. É dividido em vários subfóruns com cada um tendo seu próprio conteúdo específico e regras da comunidade. Os usuários não se cadastram para publicar no site, salvo os administradores dos fóruns. Os primeiros sub-fóruns do 4chan surgiram em torno de animes, mangás e cultura pop japonesa, mas a plataforma rapidamente se expandiu para incluir diversos outros assuntos como *videogames*, música, política, filmes, séries de televisão, esportes, etc.

online como o 4Chan que recolheram e divulgaram dezenas de fotografias dos dois suspeitos (ESTEVÃO, 2014, p. 162).

A metáfora de 1984 também mostra-se insuficiente para descrever a vigilância por parte do estado moderno. Enquanto a distopia orwelliana mostra a vigilância exclusivamente como uma forma de encontrar e combater ameaças ao regime, os estados modernos usam-na de forma muito mais mundana:

> Foi a partir da industrialização que os estados começaram a coletar informação dos seus cidadãos com alguma regularidade, quando métodos ficaram mais organizados, estruturados, racionais e centralizados e evoluíram para se tornar o que nós hoje reconhecemos como o sistema moderno de vigilância da burocracia[…]. Métodos de coleta centralizada de informação e vigilância governamental se desenvolveram a partir da necessidade e dos requisitos. Desde o fim do século XVIII, a industrialização ocidental teve um enorme impacto na necessidade da coleta de informação centralizada, mais significativamente na Grã-Bretanha, nos Estados Unidos e na Europa Continental. Migração para novas áreas urbanas, revoluções na comunicação e nos transportes, crescimento do eleitorado, e uma força de trabalho cada vez mais condensada, todos esses fatores levaram a sociedades que demandam maior capacidade de resposta e prestação de contas por parte de seus governos (WELLER, 2012, p. 57)[27].

Isto é, mais do que apenas tiranos querendo controlar seus cidadãos, os estados modernos necessitam da vigilância para manter suas burocracias e serviços públicos funcionando. Segundo Weller, a "supervisão social, pode também ser comparada com o gerenciamento da informação sobre os cidadãos de forma a providenciar o bem-estar e a proteção destes. Em outras palavras, em vez de uma sinistra e orwelliana forma de observação e monitoramento, a vigilância estatal é justificada como sendo um meio através do qual o cidadão se beneficia da aplicação do bem-estar social" (WELLER, 2012, p. 59)[28].

---

27 Texto original: *"It was not until industrialization that states began to collect information on their citizens with any regularity, when methods became more organized, structured, rational and centralized and evolved into what we recognize as the modern bureaucratic surveillance system […]. Methods of more centralized information collection and state surveillance developed out of necessity and requirement. Since the late eighteenth century, Western industrialization had a huge impact on the need for centralized information collection, most significantly in Britain, the United States and Continental Europe. Migration into new urban areas, communication and transportation revolutions, growth in the electoral franchise, and an increasingly condensed workforce, all led to societies which demanded greater response and accountability from their governments."*

Note-se que, até agora, vimos vários tipos, faces e aspectos da vigilância. Pode-se dizer que alguns desses podem ser positivos, como quando falamos da vigilância que um estado moderno exerce para planejar seu sistema de saúde ou sua previdência social. Também existe a face orwelliana da vigilância, onde o estado policial controla seus cidadãos. Existe a vigilância exercida pelas grandes empresas sobre seus consumidores e sobre seus empregados, na qual o estado não é protagonista. Tampouco vemos a figura do estado quando falamos da vigilância *peer-to-peer*. Então retomo a pergunta inicial: o que é a vigilância? Todas essas definições, tomadas de forma isolada, tal como a definição do dicionário apresentada no início desse capítulo, explicam parte da vigilância, mas, ao mesmo tempo, se mostram incapazes de explicar uma suposta totalidade. Tal como o rizoma de Deleuze e Guattari (1995, pp. 10-36)[29], a vigilância não deve ser encarada como uma singularidade e sim pelo reconhecimento da sua multiplicidade.

Tendo este aspecto rizomático em vista, deixo claro que fiz uma escolha de qual faceta da vigilância escolhi tratar no meu estudo, uma vez que independente de tempo ou recursos, não seria possível, tampouco desejável, tratá-la enquanto unidade. Dessa forma, nesta dissertação busquei estudar a vigilância perpetrada pelo estado contra organizações políticas que questionam a ordem social e política hegemônica, representada aqui pelo capitalismo neoliberal e pelos limites da democracia representativa burguesa. Fiz, ainda, um segundo recorte, no tempo e no espaço: escolhi estudar os casos de repressão a dissidentes políticos ocorridos na Cidade do Rio de Janeiro no período de 2013 a 2016, ou seja, depois das chamadas Jornadas de Junho de 2013, e no período ao longo do qual a cidade recebeu os chamados "Megaeventos"[30].

---

28 Ainda a respeito desse aspecto da vigilância, recomendo a leitura da dissertação de mestrado de Paulo Feitosa (2010), intitulada "O Cidadão Codificado: A Digitalização da Cidadania em Bancos de Dados de Interesse Público". Disponível em: http://objdig.ufrj.br/60/teses/coppe_m/PauloHenriqueFidelisFeitosa.pdf (Acessado em 07 de dezembro de 2017)

29 A palavra rizoma na botânica é atribuída a algumas plantas cujos brotos podem ramificar-se em qualquer ponto, e dessa forma, funcionar tanto como raiz, ramo ou talo, independente de sua localização física no corpo do vegetal. Assim, a metáfora de Deleuze e Guattari ilustra um modo de conhecimento onde não há proposições ou afirmações mais fundamentais do que outras, isto é, não existe uma raiz e um caminho a ser traçado a partir dela. Ao contrário, existem múltiplos pontos de entrada e múltiplos destinos finais.

30 Por megaeventos, refiro-me à Copa do Mundo de 2014, à Jornada Mundial da Juventude de 2013 e aos Jogos Olímpicos de 2016. Todos esses grandes eventos tiveram como palco o Rio de Janeiro e foram catalisadores de profundas mudanças no cenário urbano e político da cidade.

Uma opção para contar essa história seria levar em contra tanto os fatores sociais - o estado, o capital, a cultura carioca, a cultura política dos manifestantes, etc,- quanto os fatores maquínicos - as câmeras, grampos, celulares, a Internet, entre outros. A partir desta opção, como, a tecnologia e a sociedade se relacionam na vigilância? Segundo Lyon, aspectos da sociedade de vigilância surgiram antes das tecnologias computacionais, porém essas novas tecnologias têm uma relação de simbiose, de configuração e reconfiguração com a sociedade:

> Apesar das novas tecnologias de fato possuírem um tipo de capacidade de autodesenvolvimento […] isso não as tornas imunes do escrutínio por parte da sociedade. Esse processo, através das quais elas se desenvolvem é geralmente uma 'caixa-preta'. Nós devemos abrir essa caixa e analisar seu conteúdo; ao fazer isso nós poderemos descobrir os fatores sociais que moldam essas tecnologias. Ao mesmo tempo, não desejo subestimar a dimensão na qual as novas tecnologias podem contribuir com os processos de controle social. Porém essa história é uma sutil, que não pode ser reduzida para categorias cruas que assumem que a vigilância nasce de um conluio maligno de poderes econômicos e políticos (LYON, 1994, p.11)[31].

Note que a fala de Lyon na citação acima carrega consigo uma aparente contradição: se por um lado afirma que a sociedade molda os artefatos usados na vigilância, por outro a sociedade é moldada em parte pela tecnologia. Ou seja, tal como a metáfora do ovo e da galinha, uma é o produto e produtor da outra, numa relação extremamente imbricada. Para entendermos esse processo contínuo de (re)configuração entre a sociedade de vigilância e as Tecnologias de Informação e Comunicação (TICs) utilizadas para esse controle social, tal como as translações, traduções e transbordamentos oriundos dessa relação, usarei o referencial teórico dos estudos de Ciência, Tecnologia e Sociedade (CTS), dentre eles, a Teoria Ator-Rede. Vamos então adentrar nesse campo para entender como ele fornece ferramentas para entender a construção das redes de vigilância digital no Rio de Janeiro.

Os Estudos CTS são um campo interdisciplinar e dinâmico, que rapidamente se estabeleceu na Europa e na América do Norte. Como campo, é o resultado das interseções entre os trabalhos de

31 Texto original: "while new technologies do indeed have a kind of self-augmenting capacity […] this does not make them immune from sociological scrutiny. The process by which they are augmented is all-too-often a ''black box''. We should open the box and analyse the contents; we may well discover some deeply social factors shaping the technologies. At the same time, I do not wish to underestimate the extent to which new technologies may contribute to the processes of social control. But the story is a subtle one, and cannot be reduced to any crude categories that assume that surveillance is born of a malign collusion of economic and political power"

biólogos, sociólogos, historiadores, filósofos, antropólogos e outros estudiosos dos processos e resultados da ciência, incluindo a ciência médica e a tecnologia. (SISMONDO, 2012).

Um bom ponto de partida para se compreender os estudos CTS é a imbricação, indissociabilidade e indeterminação do social e do técnico. Cukierman et al (2007, p. 203) por exemplo, chamam o desafio de encarar essa complexidade de "olhar sociotécnico". Segundo a perspectiva sociotécnica, a sociedade produz, desenha e configura a ciência, ao mesmo tempo que é (re)produzida, (re)desenhada e (re)configurada pela ciência. Portanto, o social e o técnico não se dividem, mas, ao contrário, um é o produto e o produtor do outro. O olhar sociotécnico rompe as barreiras impostas pela disciplinaridade, uma vez que ao mesmo tempo que encara-se a mútua escrita da sociedade e da técnica, pode-se "igualmente fazer pensar em uma escrita que é ao mesmo tempo a das ciências exatas e a das ciências humanas e sociais. Uma escrita interdisciplinar (ou mesmo transdiciplinar) por excelência" (CUKIERMAN et al, 2007, p. 203).

O olhar sociotécnico e os estudos CTS vão na contramão da visão hegemônica da ciência pura e neutra. Para os defensores da neutralidade e universalidade da ciência:

> [o] conhecimento científico independe de quem o produziu. Não interessa se o cientista é branco ou negro, mestiço, rico ou pobre, gay, homem, mulher, judeu, muçulmano ou católico, em que século ou região vive ou sob que regime político trabalha, pois a verdade ou o fato científico transcende as contingências locais e sociais e paira acima delas. A Sociedade nada teria a dizer sobre o fato científico, que teria unicamente a Natureza como árbitro (MARQUES, 2005, p. 2).

Segundo Marques, para a visão da ciência sem valores é necessário estabelecer uma distinção entre a "ciência pura" e a "ciência aplicada". Enquanto a primeira usufrui da total imparcialidade oriunda de ter somente a Natureza como árbitro, a segunda está contaminada pelos males da Sociedade, perdendo seu caráter universal. Distingue-se então a ciência (neutra) de suas aplicações, que podem ser tão benévolas ou maliciosas quanto a sociedade: "a Física faz a bomba e faz a usina nuclear" (MARQUES, 2005, p. 2).

Os estudos CTS portanto quebram a divisão entre ciência, tecnologia e sociedade e estudam as três como indissociáveis. Para entender então essas configurações e reconfigurações sociotécnicas, um caminho a seguir é o da Teoria Ator-Rede (TAR). Segundo essa teoria, a tecnociência é explicada como um efeito das relações em rede de atores, onde cada ator também é uma rede, sem existir divisão entre os agentes e a estrutura da rede, conforme explica John Law:

> [a]utores da Teoria Ator-Rede começaram seus estudos na sociologia da ciência e da tecnologia. Como outros da sociologia da ciência, eles argumentaram que o conhecimento é um produto social, em vez de algo gerado pela operação de um método científico

> privilegiado. E, em particular, eles argumentavam que o "conhecimento" (que eles generalizam como podendo variar entre conhecimento e agentes, instituições sociais, máquinas e organizações) pode ser visto como um produto ou um efeito de uma rede de materiais heterogêneos. (LAW, 1992, p. 381)[32]

Law escreve "conhecimento" entre aspas para indicar que ele sempre está materializado de alguma forma, seja em um artigo, uma apresentação em congresso, uma patente. Também pode vir materializado enquanto habilidades incorporadas em cientistas e técnicos. Segundo o autor, a Teoria Ator-Rede se utiliza do reconhecimento dessa característica material do conhecimento para explicar a sua origem. Segundo a TAR, o conhecimento é o produto final do trabalho conjunto de vários atores heterogêneos agindo em conjunto. (LAW, 1992, p. 381)

É importante notar que, assim a TAR não diferencia, na rede, os atores humanos dos não-humanos. Os não-humanos, por sua vez, não se restringem às máquinas: uma organização, como uma empresa ou um governo, é um não humano; um elemento da natureza, como o clima, bactérias, a gravidade, também é. Em vez de organizar esses elementos em diferentes categorias, a TAR escolhe tratá-los em pé de igualdade e observar suas interações nas redes que compõem, ao mesmo tempo que reconhecem que todos esses atores também são construídos por redes heterogêneas.

Uma pergunta surge: o que faz com que uma rede heterogênea aja em uníssono para um objetivo comum? Para responder essa pergunta, a Teoria Ator-Rede usa um conceito de difícil tradução para língua portuguesa: o conceito de tradução/translação, vindo do inglês *translation*, que apresenta dois significados. Segundo Law, tradução/translação pode significar tanto possibilidade de equivalência (tradução) quanto de transformação (translação) (LAW, 1992, p. 386). Tradução/translação portanto indica a possibilidade de que uma entidade (humana ou não-humana) possa se aliar (voluntariamente ou de maneira forçada) a outra(s) para trabalhar rumo a um interesse tornado comum através da "interpretação dada pelos construtores de fatos aos seus interesses e aos das pessoas que eles alistam" (LATOUR, 2000, p. 178). Segundo Latour, a ato de traduzir/trasladar possui duas funcionalidades na construção de uma rede de atores heterogêneos: alistar outros atores para que estes participem da construção de fatos e artefatos e controlar o comportamento desses atores para que suas ações tornem-se previsíveis (LATOUR, 2000, p. 178). Para efeitos de

32 Traduzido do original em inglês: *"Actor-network authors started out in the sociology of science and technology. With others in the sociology of science, they argued that knowledge is a social product rather than something generated by through the operation of a privileged scientific method. And, in particular, they argued that "knowledge" (but they generalise from knowledge to agents, social institutions, machines and organizations) may be seen as a product or an effect of a network of heterogeneous materials."*

simplificação, usarei no texto a partir desse momento, alternadamente os vocábulos tradução e translação. Usarei em cada momento a palavra que julgar mais adequada para representar o significado pretendido.

Agora voltemos à vigilância. Como os estudos CTS e, em particular, a TAR, podem ser usados para compreendê-la? Segundo Rosa Pedro, a vigilância deve ser entendida enquanto um dispositivo sociotécnico:

> a análise que buscamos empreender recusa qualquer tipo de determinismo em relação à tecnologia, filiando-se aos estudos que considera a sociedade – e a subjetividade – como um coletivo híbrido tecido a partir da interação complexa de humanos e não-humanos. Assim, é preciso compreender os novos dispositivos tecnológicos de vigilância colocando em evidência sua hibridação sociotécnica (PEDRO, 2005, p.3).

Por hibridação sociotécnica, a autora se refere à indissociabilidade entre o técnico e o social. Defende, portanto, que a compreensão da vigilância se dá pensando-a enquanto um dispositivo extremamente complexo, que articula-se com a (e é produzido a partir da), articulação de diversos outros dispositivos. Dessa forma, pensar na vigilância aponta para a articulação de uma rede que produz "tanto objetos como sujeitos" (PEDRO, 2010, p. 41).

Voltamos então ao recorte feito anteriormente: queremos falar aqui da rede de vigilância que foi construída na conjuntura dos megaeventos na cidade do Rio de Janeiro. Para usar o olhar sociotécnico dos estudos CTS visando descrever a construção dessa rede temos que tomar um ponto de partida e seguir os atores dessa rede através das suas interações. Porém, tal como o rizoma, essa rede possui vários pontos de entrada e várias possíveis narrativas. Na sessão a seguir adentro em uma das histórias, que começa com a descoberta de que a Presidenta da República era vigiada, iniciando um processo de construção e capacitação do aparato brasileiro de segurança cibernética.

2.2 AS TICS E A VIGILÂNCIA DIGITAL NO RIO DE JANEIRO CONTEMPORÂNEO: A CONSTRUÇÃO DE UMA REDE DE MONITORAMENTO PREPARADA PARA OS MEGAEVENTOS

Na introdução desta dissertação, contei a história de como foi montado o aparato de vigilância usado na prisão dos 23 ativistas das manifestações de 2013. Aquela foi uma história que tinha como atores os manifestantes, a CEIV, o Ministério Público, a DRCI, a Copa do Mundo, entre outros. As TICs também figuraram naquela história através de atores como os celulares, o Google e o Facebook. Agora, darei mais destaque a essas tecnologias, narrando a história de mudanças em políticas do estado brasileiro relativas à governança da Internet que tiveram como consequência o aumento da vigilância digital.

Esta história começou em 2013, também no mês de junho, porém bem longe do Rio de Janeiro, mais precisamente, no Reino Unido, quando Glen Greenwald, jornalista do periódico The Guardian, publicou pela primeira vez um artigo descrevendo os documentos vazados por Edward Snowden, ex-funcionário da CIA, agência de inteligência estado-unidense. De acordo com as informações vazadas, um esquema de vigilância, encabeçado pelo governo dos Estados Unidos, mas envolvendo também agências de segurança do Reino Unido, Canadá, Austrália e Nova Zelândia, permitia armazenar de forma não-autorizada os dados de pessoas físicas, entes estatais e empresas privadas. Através do software chamado Prism, a NSA (National Security Agency) tinha acesso a diversos tipos de dados, como "histórico de pesquisas, conteúdo de e-mails, transferências de arquivos, vídeos, fotos, chamadas de voz e vídeo, detalhes de redes sociais, logins e quaisquer outros dados em poder das empresas de Internet" (ARTIGO 19, 2016, p. 6).

Segundo as denúncias de Snowden, o Prism teria rastrado 2,3 bilhões de telefonemas e mensagens e todas as informações hospedadas nos diversos serviços das principais empresas atuantes na Internet, como Google, Microsoft, Facebook, Apple, AOL e Yahoo eram passíveis de monitoramento pela NSA. (ARTIGO 19, 2016, p. 6)

Entre os vigiados encontravam-se diversos governos da Europa e da América Latina, e, no meio deles, figurava o Brasil:

> O denunciante demonstrou através de documentos vazados que o governo dos EUA, mais especificamente a NSA, estava inclusive fazendo o monitoramento de conversas de e-mail da presidenta Dilma Rousseff. De acordo com os vazamentos de Snowden, o Brasil ficou atrás apenas dos Estados Unidos em volume de monitoramentos e interceptações. Alguns dos arquivos fazem parte de uma apresentação interna da NSA, denominada 'filtragem inteligente de dados: estudo de caso México e Brasil' e foram divulgados por Greenwald. Eles demonstram que a presidente Dilma Rousseff e seus principais assessores foram alvos específicos e diretos de espionagem da agência (ARTIGO 19, 2016, p. 6).

A ameaça de espionagem repercutiu de forma intensa em Brasília. Em uma primeira investigação realizada pelas Forças Armadas e pelo Ministério da Defesa, não foi detectada invasão nos sistemas de informação estratégicos do governo, conforme noticiado pelo jornalista Thiago Herdy, para o jornal O Globo, no dia 14 de julho de 2013. Nessa entrevista, o então Ministro da Defesa, Celso Amorim, admitiu que, apesar de não ter sido detectada quebra na segurança, os sistemas de criptografia nacionais tinham como vulnerabilidade a dependência de tecnologia estrangeira, e indicou que os Ministérios da Defesa e da Ciência e Tecnologia buscariam "soluções nacionais inovadoras" para resolver o problema, destacando a necessidade da produção de algoritmos criptográficos próprios (HERDY, 2013).

O caso repercutiu no Congresso Nacional a tal ponto que, em 10 de agosto de 2013, através do Requerimento nº 811/2013 do Senado Federal, foi instaurada uma CPI – Comissão Parlamentar de Inquérito, batizada de CPI da Espionagem, para investigar "a denúncia de existência de um sistema de espionagem, estruturado pelo governo dos Estados Unidos, com o objetivo de monitorar e-mails, ligações telefônicas, dados digitais, além de outras formas de captar informações privilegiadas ou protegidas pela Constituição Federal" (BRASIL, 2014, p. 5).

O estudo realizado pela Organização Não-Governamental Artigo 19 sobre políticas de vigilância no Brasil descreve a CPI da Espionagem:

> Durou sete meses e teve participação de 13 senadores entre titulares e suplentes. Segundo as conclusões da CPI, não foi possível determinar quais informações teriam sido violadas ou se efetivamente houve espionagem nos moldes das revelações feitas por Snowden, mas a CPI destacou que os indícios coletados apontavam nesta direção. A conclusão mais importante – e que legitimou a adoção de medidas práticas para o desenvolvimento de políticas no setor – foi a constatação de que há fragilidades na segurança digital brasileira e há necessidade de mais transparência e controle sobre as requisições de dados feitas no Brasil (ARTIGO 19, 2016, p. 7).

Segundo esse estudo, a CPI, cujas recomendações finais incluíam o desenvolvimento de tecnologia nacional de segurança, maiores investimentos em inteligência e contrainteligência e a capacitação de profissionais para atuação na área de segurança digital (BRASIL, 2014), teve como resultado a "constituição de um amplo aparato estatal de vigilância da Internet no Brasil" (ARTIGO 19, 2016, p. 7).

A rede estatal brasileira de contra-vigilância começava a tomar forma, reunindo o gabinete da Presidência da República, as Forças Armadas, o Parlamento, os Ministérios da Defesa e de Ciência e Tecnologia. Todos trabalhavam para que o Brasil se tornasse capaz de monitorar o seu ciberespaço de forma a se defender dos espiões cibernéticos da NSA. Seus interesses específicos eram traduzidos nesse objetivo comum.

Porém translação também é traição, e apareceram novos atores que chegaram para bagunçar essa rede e captar seus atores para suas agendas. Esses novos atores eram os megaeventos, e, com eles, o medo de que as manifestações que ocorreram em 2013 se repetissem em 2014, durante a Copa do Mundo. A entrada dos megaeventos nessa rede mudou o inimigo contra o qual todo o aparato de vigilância cibernética seria utilizado. A rede não olhava mais para fora, para Washington, para a NSA: olhava agora para dentro, para o Rio de Janeiro, para aqueles que poderiam tomar as ruas novamente e colocar a Copa e as Olimpíadas a perder. Isto é: olhava para o próprio povo brasileiro.

Sérgio Amadeu acusou essa mudança de paradigma em entrevista ao Jornal Brasil de Fato, em 04 de agosto de 2016:

> Na verdade, há algum tempo o Brasil vem procurando seguir a doutrina de vigilância em massa que foi lançada pelos Estados Unidos. Ela chegou antes, o próprio Snowden mostrou isso em 2013. É que a gente não sentia isso. Uma das grandes justificativas para essa observação massiva da vida das pessoas são os grandes eventos – Copa do Mundo, agora as Olimpíadas. O Brasil criou um centro de cibersegurança organizado pelo Exército que, há algum tempo, persegue aquilo que é considerado "perigoso", aquilo que é considerado, a qualquer momento, um inimigo do Estado. […] O problema é que, para a doutrina de segurança norte-americana, você tem uma série de agentes que são indistintamente vigiados como se fossem de alta periculosidade, como se fossem efetivamente terroristas. Incluem-se aí: ativistas ambientais, defensores de comunidades tradicionais e indígenas, movimentos sociais – tradicionais e novos ativistas –, defensores da liberdade na internet, estudantes que protestam contra políticas educacionais e que entendem que, muitas vezes, é preciso ocupar sua própria escola para evitar seu fechamento. Tudo isso passa a ser alvo (AMADEU, 2016 apud TATEMOTO, 2016).

Com essa mudança de paradigma, surgiu no Brasil, e especialmente no Rio de Janeiro durante a preparação para os megaeventos, uma oportunidade de grandes negócios para venda de equipamentos de vigilância, como mostram Natália Viana e Gabriele Rosa em estudo realizado para a ONG Agência Pública:

> Os gastos foram de fato extraordinários. Apenas a Secretaria Especial para Grandes Eventos (Sesge), do Ministério da Justiça, gastou em cinco anos (2011 a 2016) cerca de R$ 1,17 bilhão, isso sem contar os gastos feitos pelas Forças Armadas, governos estaduais e municipais. Desse total, mais da metade (R$ 637 milhões) foram para os Centros de Comando e Controle (CICCs), unidades de segurança pública que reúnem diversas forças policiais no mesmo prédio, depois doados para as secretarias de Segurança de cada estado (VIANA e ROSA, 2017).

As portas da rede estavam abertas para a entrada de uma nova leva de não-humanos, isto é, de diversas soluções de segurança, produzidas por diferentes empresas. Podemos citar como exemplo. a gaúcha Aeromot, que forneceu "para o monitoramento aéreo da Copa do Mundo, […] 35 aeronaves com um sistema que gera imagens, inclusive infravermelhas, que são enviadas para equipes em terra. A empresa chama esse sistema de 'guardiãs silenciosas'". A mineira Polsec, dentre outros produtos, equipou a Secretaria Nacional de Grandes Eventos (SESGE) com vans passíveis de serem transformadas "em viaturas secretas, camufladas e equipadas com sistemas de monitoramento e sistema de radiotransmissão". Não só empresas nacionais participaram desse

negócio: por exemplo, as câmeras dos 12 CICCs das cidades-sede da Copa do Mundo de 2014 receberam software da alemã Helmut Mauell (VIANA e ROSA, 2017). Além da Mauell, e-mails vazados pelo portal WikiLeaks[33] expuseram a comunicação entre a Polícia Federal e a Hacking Team (HT), empresa italiana especializada na venda de softwares de espionagem para governos ao redor do mundo:

> Basicamente, o produto principal da HT é uma suíte de invasão desenvolvida a partir de vulnerabilidades não divulgadas publicamente nos sistemas operacionais. Através da engenharia social, isto é, da ação do alvo clicar e executar o programa malicioso, é possível [contaminar o sistema operacional do vigiado], extrair os dados, interceptar áudios e vídeos de conversas, acionar a câmera de vídeo, infectar outros computadores, descobrir sua localização e inclusive ser removido sem deixar rastros no dispositivo da vítima. […] Sob o codinome Brenda, a Polícia Federal estabeleceu um contrato com a HT para a implementação de um projeto-piloto no início de 2015 (ARTIGO 19, 2016, p. 38).

Ao seguirmos os atores dessa rede de vigilância montada para a segurança dos megaeventos, nos deparamos com uma sofisticação técnica que contrasta com os métodos tradicionais empregados no caso dos 23 presos. Deve-se ressaltar que a construção do processo dos 23 e a capacitação do aparato repressor do Estado Brasileiro, no âmbito da segurança digital, ocorreram e ocorrem em paralelo. Apesar de os grandes eventos, os grandes catalisadores para a construção dessa rede, já terem acabado, não se pode dar por encerrada nenhuma das histórias que contei até aqui. Tanto técnicas tradicionais, ou menos sofisticadas, como as Rondas Virtuais, ou o emprego de "soluções inovadoras", como aquelas materializadas nos CICCs, ainda podem ser usadas para reprimir um ascenso das massas como ocorrido em 2013.

Este quadro impõe uma questão urgente para os objetivos desta dissertação: podem os movimentos contra-hegemônicos responder a essa vigilância do estado? Novamente precisamos responder usando um olhar sociotécnico, levando em conta o aparato de vigilância do estado brasileiro e as especificidades dos diversos movimentos sociais que atuam na cidade do Rio de Janeiro. Para entrarmos nessa rede temos que entender o problema da vigilância pela ótica dos movimentos sociais. Logo, a resposta para esse problema parte inicialmente dos próprios movimentos sociais, a quem eu preciso convencer a construir comigo uma resposta. Seguindo a lógica da TAR, preciso, portanto, traduzir os interesses desses movimentos para os meus e os meus para os interesses deles, de forma que trabalhemos em conjunto nessa resposta. Farei isso usando a Metodologia da Pesquisa-Ação, apresentada no capítulo a seguir.

33 Os e-mails foram vazados no dia 08 de julho de 2015 e encontram-se disponíveis para consulta no link https://wikileaks.org/hackingteam/emails/ (acessado em 18 de janeiro de 2017)

3 METODOLOGIA: O USO DA PESQUISA-AÇÃO AO LONGO DA PESQUISA

3.1 SOBRE A PESQUISA-AÇÃO

A Pesquisa-Ação, chamada na academia anglófona de Participatory Action Research (PAR), consiste em uma metodologia de pesquisa baseada na cooperação entre o pesquisador e os atores pesquisados tendo como objetivo a realização de uma ação, que é planejada e construída de forma participativa e colaborativa entre o pesquisador e os pesquisados. Essa colaboração é fruto de um processo de "reflexão coletiva, que servirá para embasar e avaliar essa ação e que gera conhecimento em diálogo com a prática" (ALVEAR, 2014, p. 157).

Segundo Thiollent, a Pesquisa-Ação não é adequada para o estudo de casos individuais ou de grupos muito pequenos, devido ao fato de ter como principal foco os aspectos sociopolíticos, em detrimento dos aspectos psicológicos das relações interpessoais e da psicologia individual. Tampouco é adequada ao enfoque macrossocial, isto é de nações inteiras, ou da sociedade como um todo. A Pesquisa-Ação é portanto "apenas um instrumento de trabalho e de investigação com grupos, instituições, coletividades de pequeno ou médio porte" (THIOLLENT, 1986, pp. 8-9).

Para Alvear, a Pesquisa-Ação tem seu foco na análise de problemas e planejamento de ações. Porém, deve-se levar em consideração os aspectos estruturais de uma determinada realidade, devido à sua influência na ação a ser realizada, e nas relações sociais existentes entre os atores estudados.[34] Dessa forma:

> poderíamos dizer que não faria muito sentido fazer uma Pesquisa-Ação sobre o Movimento Sem-Terra, sobre a favela Santa Marta ou mesmo sobre uma determinada ONG, mesmo que pequena. Porém, poderíamos fazer uma Pesquisa-Ação sobre um mutirão realizado pelo MST em uma determinada localidade, ou sobre a realização de um curso de educação para jovens e adultos no Santa Marta, ou sobre um projeto de fortalecimento da pesca realizado por uma ONG (ALVEAR, 2014, p. 159).

Segundo Fals Borda, a orientação da metodologia para a resolução de problemas práticos em conjunto com atores externos à universidade pode contribuir para a construção de conhecimento confiável a serviço dos pobres[35], grupos e classes sociais oprimidas e exploradas, levando ao

34 Aqui temos um ponto de tensão entre a Teoria Ator-Rede e a Pesquisa-Ação: uma vez que a TAR busca desconsiderar as estruturas previamente definidas, torna-se dissonante falar em aspectos estruturais da realidade. Mais pontos de tensão como esse aparecerão ao longo da dissertação:tentarei expô-los ao leitor, bem como os pontos de convergência entre elas.

35 Gostaria de destacar aqui o uso da palavra "pode" na afirmação acima. Isto é, este é apenas um dos caminhos possíveis para o uso da Pesquisa-Ação. Ao mesmo tempo que a metodologia pode ser

fortalecimento de um poder contra-hegemônico. Segundo o autor, para isso é necessário um comprometimento autêntico do pesquisador com os grupos pesquisados, que devem se unir com o propósito único de concretizar a ação transformadora proposta. Para isso é necessário que, de forma voluntária e movida pela experiência prática de todos os envolvidos, rompam-se os papéis tradicionais de pesquisador/pesquisado de forma a dar lugar à relação simétrica sujeito/sujeito. Para o autor, a busca coletiva desses ideais de simetria e participação coloca todos os envolvidos na Pesquisa-Ação no papel de intelectuais orgânicos da classe trabalhadora, ao mesmo que tempo que evita o surgimento de novas hierarquias permanentes dentro dos grupos estudados (FALS BORDA, 1991, pp. 3-5).

Fals Borda também afirma que a Pesquisa-Ação parte do princípio de que a ciência não é neutra e universal, sendo somente uma forma de conhecimento válida e útil para um determinado contexto e baseada em determinadas verdades relativas àquele contexto. Toda ciência é um produto cultural formulado para um determinado propósito e portanto carrega consigo ideologias e valores associado à sua formulação.[36] Dessa forma a ciência é enviesada no sentido de favorecer aqueles indivíduos e grupos que a produzem e a controlam. Portanto, em um cenário ideal, a Pesquisa-Ação deve buscar envolver os grupos estudados em todas as etapas do processo de pesquisa, desde o momento em que se decide o tema da pesquisa[37] até a publicação dos resultados (FALS BORDA, 1991, pp. 7-8).

3.2 TEMAS DA PESQUISA-AÇÃO

Thiollent afirma que desde o incio da Pesquisa-Ação é necessário definir com precisão qual será a ação realizada, quais os agentes estudados, seus objetivos, e quais os obstáculos que podem vir a surgir no decorrer do desenvolvimento da ação. O autor afirma ainda que o objeto de estudo da Pesquisa-Ação não é constituído pelas pessoas e sim pela situação social e pelos problemas estudados, isto é os aspectos estruturais da realidade estudada[38]. O objetivo da Pesquisa-Ação ação empregada para fortalecer um movimento social, ela também pode ser empregada em uma grande empresa capitalista para solução de um problema prático. Essa versatilidade da Pesquisa-Ação se relaciona diretamente à necessidade de comprometimento do pesquisador com a comunidade pesquisada, conforme apontado por Fals Borda.

36 Aqui observa-se um ponto de convergência entre a Pesquisa-Ação e a Teoria Ator-Rede.

37 Falarei mais sobre a escolha do tema da Pesquisa-Ação relatada nessa dissertação nas sessões a seguir.

38 Observa-se novamente o conflito entre a TAR e a Pesquisa-Ação em relação às questões estruturais da realidade estudada.

por sua vez deve ser a resolução ou, pelo menos, o entendimento do problema estudado. Thiollent adverte porém que a Pesquisa-Ação não deve se limitar ao ativismo: a produção de conhecimento tanto pelos pesquisadores quanto pelos pesquisados deve ser um dos nortes de todo o processo investigativo (THIOLLENT, 1986, pp. 16).

Doze temas constituem o processo da Pesquisa-Ação. É necessário ressalvar que esses temas não devem ser tratados como etapas a serem seguidas linearmente, uma vez que muitos deles, em especial os temas intermediários, podem ocorrer paralelamente ou desrespeitando a ordem apresentada (THIOLLENT, 1986, pp. 47-72). Os temas e suas descrições são:

1. A Fase Exploratória;
2. O Tema da Pesquisa;
3. A Colocação dos Problemas;
4. O Lugar da Teoria;
5. Hipóteses;
6. Seminário;
7. Campo de observação, Amostragem e Representatividade Qualitativa;
8. Coleta de dados;
9. Aprendizagem;
10. Saber formal / Saber informal;
11. Plano de Ação;
12. Divulgação externa.

A **Fase Exploratória** é o ponto de partida da Pesquisa-Ação. Ela consiste na identificação dos atores interessados na ação, suas expectativas e demandas, o contexto social da situação estudada e os possíveis entraves e obstáculos que deverão ser superados no decorrer da Pesquisa-Ação. Também são resolvidos os problemas práticos relacionados à constituição da equipe de pesquisa e dos recursos financeiros, materiais e institucionais necessários para a realização do projeto. É nesse momento inicial que busca se estabelecer uma relação de confiança entre o pesquisador e os atores externos à academia, ao passo que é ponderada a viabilidade do projeto de Pesquisa-Ação proposto. Segundo Thiollent, é necessário medir bem os fatores apresentados acima no estudo de viabilidade de forma que os pesquisadores possam iniciar o projeto sem criar falsas expectativas nos atores externos (THIOLLENT, 1986, pp. 48-50).

O **Tema da Pesquisa** é a "designação do problema prático e da área de conhecimento a serem abordados" (THIOLLENT, 1986, p. 50). Deve ter associação direta à ação que será desenvolvida ao longo da Pesquisa-Ação. Por exemplo, uma pesquisa sobre acidentes de trabalho em uma empresa tem como ação relacionada providenciar a diminuição desses acidentes. Para Thiollent, o tema deve interessar tanto ao pesquisador quanto à população estudada, visto que "um tema que não interessar à população não poderá ser tratado de modo participativo. Um tema que não interessar aos pesquisadores não será levado a sério e eles não desempenharão um papel eficiente" (THIOLLENT, 1986, p. 52). O tema é normalmente definido durante a Fase Exploratória, mas algumas vezes o tema é definido de antemão, devido à natureza da situação ou à urgência do problema (THIOLLENT, 1986, pp. 50-53), como é o caso da Pesquisa-Ação relatada nesta pesquisa de mestrado, a saber, a conjuntura relacionada aos chamados Megaeventos que ocorreram na cidade do Rio de Janeiro no período de 2014-2016 (Copa do Mundo e Olimpíadas) e à prisão dos 23 presos Políticos de 2014. Foi essa conjuntura que serviu de motivação para a realização dessa pesquisa, levando à escolha prévia do tema.

A **Colocação dos Problemas** trata de definir uma problemática que confira sentido ao tema escolhido. Segundo Thiollent, um mesmo tema pode ser enquadrado em problemáticas diferentes: problemas de saúde podem ser colocados em uma problemática conectada à medicina ou a questões político/sociais (THIOLLENT, 1986, p. 53), ou então problemas relacionados às Tecnologias de Informação e Comunicação podem ser encarados pelo viés da informática ou da comunicação. A **Colocação dos Problemas** consiste em: análise e delimitação da situação atual; delineamento da situação final; identificação dos problemas a serem resolvidos de forma a passar da situação atual para a final; planejamento das ações correspondentes; e, por fim; execução e avaliação das ações. Para Thiollent, é na **Colocação dos Problemas** que se deve discutir a relevância científica e prática do que se está estudando, de forma a redirecionar ou mesmo cancelar, se necessário, o processo de investigação e ação (THIOLLENT, 1986, pp. 53-54).

O **Lugar da Teoria** "consiste em gerar ideias, hipóteses ou diretrizes para orientar a pesquisa e as interpretações" (THIOLLENT, 1986, pp. 55). É a teoria que permite ao pesquisador ir além do empirismo do senso comum, além de permitir um diálogo mais produtivo com o saber popular dos participantes. A informação extraída do processo participativo deve ser interpretada à luz de uma teoria, de forma a ser traduzida em conhecimento científico (THIOLLENT, 1986, pp. 54-55).

As **Hipóteses na Pesquisa-Ação** não diferem muito de suas contrapartes na pesquisa tradicional: em ambos os casos consistem em uma "suposição formulada pelo pesquisador a respeito de possíveis soluções a um problema colocado na pesquisa, principalmente ao nível

observacional" (THIOLLENT, 1986, p. 56). A diferença do papel das hipóteses nas formas tradicionais de pesquisa para a Pesquisa-Ação reside no fato de que, nesta última, não se busca mostrar uma relação causal entre dois fatos e sim criar diretrizes para serem usadas no plano normativo que orienta a ação realizada. Isto é, em vez de buscar provar, por exemplo, que a vigilância digital sofrida pelos grupos políticos atuantes no Rio de Janeiro é causada por uma determinada conjuntura, procuramos investigar se essa vigilância pode ser resolvida ou combatida com sucesso (ainda que parcial) através de um conjunto determinado de ações[39] (THIOLLENT, 1986, pp. 56-58).

O **Seminário** é um tema extremamente importante na Pesquisa-Ação. Segundo Thiollent, o seminário se configura como a principal técnica, ao redor da qual as outras gravitam, para organizar a construção participativa das ações. Ele deve ter início a partir do momento em que os pesquisadores e os interessados na pesquisa estão de acordo sobre os objetivos e os problemas a serem investigados e reúne em um mesmo espaço os principais membros da equipe de pesquisadores e membros significativos dos grupos afetados pelo problema estudado. A função do seminário consiste em examinar, discutir e tomar decisões acerca do desenvolvimento da Pesquisa-Ação. Caso o seminário seja organizado em um meio heterogêneo, as questões da representação dos diversos segmentos ganham importância. Segundo Thiollent, essas questões devem ser resolvidas por meio de negociações e requerem muita transparência por parte dos pesquisadores. Os dados coletados ao longo da pesquisa devem ser levados de volta ao seminário para debate e sistematização. Nesse ponto entram em contato os conhecimentos formais dos pesquisadores com o conhecimento informal dos participantes. Esses dois saberes devem dialogar e buscar áreas de contato e traduções devem ser feitas entre os interesses dos pesquisadores e dos participantes. (THIOLLENT, 1986, pp. 58-60)

Em casos onde o campo delimitado é demasiadamente amplo, coloca-se a questão da amostragem além da já mencionada representatividade. Segundo Thiollent, a representatividade qualitativa é dada por uma avaliação da relevância política dos grupos e visões que existem dentro do campo estudado. Trata-se portanto de uma representação politicamente fundamentada da realidade estudada. Distorções nessa representação devem ser controladas e retificadas pelo seminário ao longo da Pesquisa-Ação (THIOLLENT, 1986, pp. 60-63).

Como já dito anteriormente, a **Coleta de Dados** é efetuada em constante diálogo e controle do seminário. Na Pesquisa-Ação, as principais técnicas utilizadas são a entrevista individual

39 É importante notar que a compreensão da conjuntura vai ser necessária para definir, planejar e realizar as ações. Porém o norte da Pesquisa-Ação é a ação prática e, portanto, as hipóteses, e seu papel na metodologia, refletem essa opção.

aplicada de modo aprofundado e as entrevistas coletivas por locais de moradia e trabalho. Técnicas tradicionais de entrevistas, como questionários, podem ser utilizadas, porém essas não podem ser suficientes em si mesmas, devendo todas as informações coletadas serem discutidas e aprofundadas nos seminários. Desta forma, não basta o processo estatístico das respostas coletadas nas entrevistas: é preciso acompanhar esses dados quantitativos com um processamento qualitativo da informação, realizado por meio do retorno ao campo e aos atores interessados (THIOLLENT, 1986, pp. 64-66).

Na Pesquisa-Ação, a **Aprendizagem** anda de mãos dadas com o processo investigativo. O papel dos pesquisadores deve ser o de facilitar a aprendizagem dos atores[40], o que inclui também os próprios pesquisadores. Isso ocorre de várias maneiras vistas anteriormente, tais como a discussão no seminário, as negociações necessárias entre os atores para a construção da ação, e o retorno das informações coletadas aos participantes envolvidos, etc. Em suma, toda o processo de discussão necessário para a construção da ação é um experimento não apenas científico, isto é, de produção de conhecimento, como também pedagógico tanto para os participantes quanto para os pesquisadores (THIOLLENT, 1986, pp. 66-67).

Na Pesquisa-Ação, a relação entre os saberes formais e informais busca estabelecer a troca de conhecimento entre o universo dos pesquisadores e o dos atores. Segundo Thiollent, a Pesquisa-Ação é incompatível com a noção tradicional da academia de que os grupos pesquisados, em especial aqueles das classes populares, não tem conhecimentos que possam contribuir com a produção de conhecimento científico. Segundo o autor, o participante conhece, de forma mais intensa que o pesquisador, o universo que está sendo estudado e seus problemas relacionados. O saber desses participantes é rico e bem-adaptado ao contexto local, porém é permeado por costumes, tradições e crenças que o tornam insuficiente para produzir transformações rápidas. De forma análoga, o saber dos especialistas também é incompleto e não universal[41]. Dessa forma é necessário estabelecer uma linguagem comum[42] a fim de permitir que ambos completem-se

40 O uso da palavra ator dentro da Pesquisa-Ação é novamente um ponto de tensão entre a TAR e a Pesquisa-Ação. Para a Teoria Ator-Rede, estão incluídos nos atores os não-humanos, que para a Pesquisa-Ação ficam de fora do processo de participação, aprendizado e construção coletiva do conhecimento.

41 Diria inclusive que o próprio saber científico também possui seus próprios costumes e crenças que permeiam a produção tecnocientífica, uma vez que a produção científica é indissociável da sociedade e de seus valores, conforme discutido no capítulo anterior.

42 Note que aqui a Pesquisa-Ação se aproxima da Teoria Ator-Rede, visto que a busca de uma linguagem comum poderia equivaler ao na TAR é conceituado como uma tradução.

mutuamente. Essa troca se inicia com os participantes colocando suas visões sobre a situação vivenciada, alternando entre a busca de explicações e a de possíveis soluções. Os especialistas atuam sobre essa visão com as suas problemáticas e temas. Essas duas linguagens são comparadas e traduzidas, buscando zonas de compatibilidade e incompatibilidade. Deve-se ressalvar que o uso dessa técnica de comparação não soluciona todos os problemas da relação entre o saber formal e o informal, sendo apenas um ponto de partida para iniciar o mapeamento dos dois universos com fim de estabelecer uma linguagem comum (THIOLLENT, 1986, pp. 67-69).

A elaboração do **Plano de Ação** consiste em definir com precisão os atores que serão impactados pela ação, como se relacionam esses atores entre si e com a situação em questão, quem dentro dos grupos pesquisados é responsável pela tomada de decisões referentes à Pesquisa-Ação, quais os objetivos e metas da ação planejada, como dar continuidade à ação em caso de dificuldades, como assegurar a participação dos atores[43] e incorporar suas decisões na pesquisa, e, por fim, como controlar o conjunto do processo e avaliar os resultados. Thiollent atenta que o Plano de Ação deve ser feito de forma realista a fim de não criar falsas esperanças entre os participantes. (THIOLLENT, 1986, pp. 69-71).

O último tema é referente à **Divulgação Externa.** Na Pesquisa-Ação, além do retorno do conhecimento produzido ao longo do processo investigativo aos grupos implicados na pesquisa por intermédio do Seminário, deve-se buscar a publicação conjunta dos trabalhos resultantes da pesquisa. Os canais dessas publicações podem tanto ser acadêmicos – congressos, seminários, revistas científicas, etc – quanto populares, ou seja, aqueles diretamente ligados à realidade estudada. Os canais de divulgação da pesquisa, sobretudo os informais, fortalecem o processo de difusão do conhecimento produzido em conjunto daquela população e portanto as possibilidades de apropriação desse conhecimento por ela mesma, não se limitando aos participantes efetivos (THIOLLENT, 1986, pp. 71-72).

Tratados os 12 temas da Pesquisa-Ação, apresentarei na seção a seguir como esta metodologia foi empregada durante o projeto de pesquisa desta dissertação de mestrado.

3.3 A PESQUISA-AÇÃO NO PLANEJAMENTO E CONSTRUÇÃO DE AÇÕES DE EXTENSÃO PARA COMBATER A VIGILÂNCIA DIGITAL

Como já exposto anteriormente, a escolha do tema desta Pesquisa-Ação, anterior à *Fase Exploratória,* partiu de minha iniciativa enquanto pesquisador motivado por uma tríade de fatores: meu envolvimento com o movimento estudantil em 2013, meu interesse na graduação por

43 Mais uma vez, observamos aqui a tensão entre a TAR e a Pesquisa-Ação provocada pelo conceito divergente de ator.

Segurança da Informação e meu desejo por produzir algo útil aos movimentos sociais e aos meus companheiros de militância. Como também já formulado anteriormente, a Pesquisa-Ação não é uma metodologia adequada para estudar a vigilância digital propriamente dita, uma vez que o tema da pesquisa deve estar associado a ações que venham a ser realizadas. Desta forma foi escolhido como *Tema da Pesquisa* o combate à vigilância, o qual enseja a proposição e a realização de projetos de extensão que podem ser realizados pela universidade conjuntamente com grupos políticos que são alvo da vigilância no Estado do Rio de Janeiro. A *Colocação do Problema* também teria de se dar dentro do escopo das Tecnologias de Informação e Comunicação (TICs) e da Informática e Sociedade, devido à minha formação em Ciência da Computação e vinculação à linha de pesquisa em Ciência, Tecnologia e Sociedade do HCTE/UFRJ. Para transformar este meu desejo em um plano para uma Pesquisa-Ação, foi necessário, primeiramente, buscar aliados dentro da UFRJ que pudessem compartilhar comigo essa aventura, o que deu início à Fase Exploratória.

Meu primeiro ponto de parada foi, logicamente, o local onde decidi cursar meu mestrado, o Programa de Pós-Graduação em História das Ciências e das Técnicas e Epistemologia (HCTE). Esta primeira aliança forneceu, além, é claro, da formação teórica necessária para produzir uma dissertação de mestrado, as credenciais acadêmicas necessárias para minha Pesquisa-Ação. Um segundo aliado foi o Núcleo de Solidariedade Técnica (SOLTEC), localizado no Centro de Tecnologia, um laboratório com anos de experiência na realização da Pesquisa-Ação e no contato com os movimentos sociais. Um das ações do Núcleo é o projeto Tecnologias da Informação para Fins Sociais (TIFS) que "trabalha principalmente a partir de uma ótica de um desenvolvimento participativo de tecnologias voltadas para ampliar a participação e a democracia em movimentos sociais e processos de desenvolvimento local"[44]. Esta segunda aliança propiciou uma nova credencial acadêmica: além de aluno de mestrado, passei a ser também membro de um programa de extensão, que forneceu como maior recurso a parceria com dois bolsistas de graduação, Arthur Castro e Arthur Guilherme, que, ao meu lado, compuseram a equipe de pesquisa responsável pelo projeto relatado nesta dissertação de mestrado. Também participaram da equipe de pesquisa, em grau menor, devido ao envolvimento em outras atividades, Mariana Rio e Celso Alvear, pesquisadores-extensionistas do SOLTEC.

O passo seguinte, ainda dentro do escopo da *Fase Exploratória*, foi o primeiro contato com o campo. Buscamos o contato com sindicatos, partidos e movimentos sociais de forma a verificar o interesse por parte desses grupos em participar na/da pesquisa. O primeiro grupo que respondeu nosso contato foi o Movimento dos Trabalhadores Rurais Sem-Terra (MST). Em entrevista pessoal

44 http://nides.ufrj.br/index.php/projetos-soltec/tifs (Acessado em 25/11/2016)

realizada no dia 31 de agosto de 2015, Maria[45], militante do MST e integrante da diretoria de comunicação do movimento, relatou que o grupo possuía pouco domínio do uso das TICs e, portanto, optava muitas vezes por não usá-la em sua comunicação interna.

O grupo seguinte com o qual buscamos contato foi o Núcleo Piratininga de Comunicação (NPC). O NPC é uma ONG, formada em sua maioria por profissionais da área de comunicação, cuja atividade declarada é capacitar e promover a comunicação popular, em todo o território nacional, para grupos interessados em melhorar sua comunicação: do jornal impresso à Internet, da oratória ao uso do rádio e do vídeo.[46] Suas atividades incluem a promoção de cursos, palestras e debates ligados à área de comunicação para sindicatos e movimentos sociais. Em reunião realizada no dia 23 de setembro de 2015, conversamos com Cláudia Gianotti, comunicadora e principal liderança da ONG, que nos informou que o tema da Segurança da Informação era uma demanda antiga por parte dos militantes de sindicatos que frequentavam os cursos do NPC, porém a ONG não tinha conhecimentos suficientes nessa área para ministrar um curso. Cláudia então sugeriu que a nossa equipe iniciasse uma pesquisa, realizada através de um formulário impresso[47], no último dia do Curso Anual do NPC daquele ano[48].

Naquele momento, a equipe de pesquisa ainda estava muito incerta sobre o formato da Pesquisa-Ação, fazendo com que as perguntas do formulário fossem construídas com o intuito de mapear quais ferramentas eram usadas pelos militantes e se eles (e seus companheiros de militância) sentiam interesse pela temática da vigilância e da segurança da informação. Através dessa pesquisa inicial, obtivemos respostas de 17 sindicalistas, os quais, salvo um, indicaram preocupação com o tema[49]. Do ponto de vista da Pesquisa-Ação, este é um resultado positivo: como já comentado anteriormente, o tema da pesquisa deve ser interessante para os participantes e nós havíamos conseguido detetar o interesse por parte do pretendido público-alvo.

Para continuar na Pesquisa-Ação seguindo os 12 temas, o próximo passo seria a montagem de um *seminário*. A equipe de pesquisa decidiu então construir ao menos uma oficina de segurança digital com as finalidades de introduzir o tema da vigilância digital para os movimentos políticos,

45 Nome fictício. A militante não autorizou a divulgação do seu nome verdadeiro.

46 http://nucleopiratininga.org.br/o-que-fazemos/ (Acessado em 25/11/2016)

47 Formulário disponível como Anexo dessa dissertação.

48 O Curso Anual do NPC é oferecido todo ano para militantes do movimento sindical, sendo realizado sempre no último trimestre, na cidade do Rio de Janeiro. No ano de 2015, a 21ª edição do curso foi realizada entre os dias 18 e 22 de novembro.

49 Os resultados desse questionário serão novamente tratados nas considerações finais desta dissertação, junto com os demais resultados da pesquisa.

de buscar aliados interessados em construir a pesquisa conosco e de mapear quais outras ações poderiam ser realizadas além de oficinas pontuais (cursos mais longos, material didático, videoaulas, etc). O primeiro passo nessa direção foi passar o questionário usado no curso do NPC da forma impressa para uma versão online hospedada em um servidor seguro, isto é, um servidor no qual a equipe de pesquisa poderia garantir aos interessados na pesquisa , na medida do possível, que suas informações não vazariam. Isto é, não poderíamos usar um formulário hospedado na nuvem do Google, tínhamos que buscar uma alternativa que garantisse um certo grau de privacidade. Para solucionar esse problema, foi usado o portal da Rede de Engenharia Popular Oswaldo Sevá (REPOS)[50] no Milharal[51]. Perguntas relacionadas à disponibilidade dos interessados para participar de uma oficina foram adicionadas ao questionário para auxiliar na escolha do dia e horário.

Para a organização da oficina piloto, a equipe de pesquisa buscou a participação de grupos políticos com algum grau de envolvimento na problemática da segurança. Os grupos foram contatados graças à militância prévia por parte dos membros da equipe de pesquisa no movimento estudantil e na esquerda organizada, ou seja, já existia algum grau de contato, ainda que indireto com, pelo menos, algum membro da equipe de pesquisa. Realizamos então três reuniões, entre maio e julho de 2016, que contaram com a participação de militantes dos seguintes coletivos[52]:

- Rede de Informação Anarquista[53]
- Partido Pirata[54]

50 A REPOS é um movimento social organizado na forma de uma rede de engenheiras e engenheiros, com participação de profissionais de outras áreas de conhecimento, que tem como o objetivo trabalhar as demandas das tecnologias e das engenharias sob uma perspectiva popular e solidária. Para tal objetivo presta assessoria a movimentos sociais. Através do SOLTEC, conheci a REPOS e passei a participar dos espaços de articulação dessa rede. Por meio dessa participação, consegui o acesso ao portal da REPOS, onde hospedei o questionário. Para mais informações sobre a REPOS, acesse https://repos.milharal.org/. (Acessado dia 27/11/2016)

51 O Milharal é um projeto que hospeda diversas páginas na Internet de movimentos sociais e políticos. Para mais informações sobre o Milharal http://milharal.org/. (Acessado dia 27/11/2016)

52 Nem todos os coletivos estiveram presentes em todas as reuniões.

53 Coletivo midiativista de orientação política anarquista. http://redeinfoa.org/ (Acessado dai 29/11/2017)

54 Partido político, ainda em processo de legalização do registro eleitoral. Tem como bandeira a luta contra as atuais leis de propriedade intelectual e industrial. https://partidopirata.org/ (Acessado dia 29/11/2017)

- Coletivo Redes e Ruas[55]
- Anonymous Rio[56]
- Intervozes[57]

Essas reuniões se constituíram na prática como o embrião de um Seminário, nas quais foram definidas a grade, o local, o dia, o horário e o formato da oficina-piloto. Relatarei a oficina adiante, porém, vale adiantar que participantes dessas reuniões também dividiram com a equipe de pesquisa não somente a responsabilidade de ministrar a oficina mas também, ao final dela, o registro de suas impressões sobre a experiência.

Para garantir apoio institucional por parte da UFRJ, a equipe registrou dois cursos de extensão no Registro Único de Ações de Extensão (RUA), de 2016. Este registro tem como finalidade "cadastrar, por meio do Sistema de Informação e Gestão de Projetos (SIGProj), propostas de ações de extensão, na forma de projetos, cursos ou eventos, para fins de avaliação, registro, certificação e incorporação no processo de creditação da extensão universitária"[58]. Foram registrados dois cursos de extensão, um com duração de oito horas[59] e outro de vinte horas[60]. A primeira oficina foi creditada no registro do curso de menor duração[61]. A realização da oficina e os resultados da pesquisa serão relatados no próximo capítulo.

55 Coletivo midiativista, próximo ideologicamente do PSOL. Publica principalmente em sua página no Facebook https://www.facebook.com/redeseruasbr/ (Acessado dia 29/11/2017)

56 Coletivo midiativista, já apresentado anteriormente.

57 Movimento social "que trabalha pela efetivação do direito humano à comunicação no Brasil". http://intervozes.org.br/quem-somos/ (Acessado dia 29/11/2017)

58 http://sigproj1.mec.gov.br/edital_blank.php?id=1188 (Acessados dia 28/11/2016)

59 Mini-curso de Sensibilização de Contra-vigilância e Segurança da Informação para Movimentos Sociais http://sigproj1.mec.gov.br/apoiados.php?projeto_id=228179 (acessado em 28/11/2016)

60 Curso de Introdução à Ferramentas de Contra-vigilância e Segurança da Informação para Movimentos Sociais http://sigproj1.mec.gov.br/apoiados.php?projeto_id=242655 (acessado em 28/11/2016). Esse curso teve sua 1ª turma em Dezembro de 2017, quando o processo de escrita do presente texto já encontrava-se no final. Mais turmas estão sendo planejadas para 2018. Falarei mais do futuro dessa pesquisa nas conclusões.

61 Por questões de segurança, foi deixado claro aos participantes que nenhum deles, fosse palestrante ou ouvinte, seria obrigado a receber o certificado de participação, uma vez que esse era emitido pela universidade e o controle dessa informação era desconhecido pela equipe de pesquisa. Dessa forma, apenas 8 certificados foram solicitados (inclusos os certificados da equipe de pesquisa).

4. RESULTADOS COLETADOS E DISCUSSÃO

4.1 A I OFICINA DE SEGURANÇA DIGITAL PARA ATIVISTAS

No capítulo anterior relatei a construção do primeiro seminário de Pesquisa-Ação que construí como parte dessa dissertação. Conforme as discussões iam se desenvolvendo, mostrou-se necessário trazer novos atores para nossa rede e aumentar a troca de informações nesse espaço, ainda demasiadamente restrito para realizar nosso objetivo de produzir uma intervenção concreta no problema da vigilância digital. Foi decidido então realizarmos uma oficina-piloto para convidar mais pessoas para nossa rede. No dia 08 de outubro de 2017, na sede do sindicato dos engenheiros no Estado do Rio de Janeiro, localizada na Cinelândia, realizamos a I Oficina de Segurança Digital para Ativistas.

A oficina começou às 08 h e terminou às 18 h, com uma pausa para o almoço, abrindo com palestras de atores presentes no seminário anterior. Entre cada palestra foi realizada uma rodada do que chamamos de reações, onde os participantes respondiam perguntas preparadas pela equipe de investigação e, após um intervalo de escrita, voluntários expunham suas respostas e debatiam com o coletivo, em roda, suas impressões. O bloco de papel contendo as perguntas foi entregue aos participantes na entrada do evento; na primeira folha deveriam ser preenchidas informações necessárias para classificar a demografia dos participantes[62].

A primeira palestra foi de Thiago Rocha, um dos ativistas presos por sua participação nas manifestações de junho de 2013, e que já havia sido entrevistado por mim como parte da produção desta dissertação. Sua apresentação consistiu em contar a sua história do processo movido contra os 23 ativistas. Essa primeira palestra serviu para abrir o debate com um caso concreto de vigilância para chocar o público com esse relato. Ao final da exposição de Thiago, foi pedido aos participantes que enumerassem os três maiores interessados em vigiar a sua organização e, depois, que escolhessem o mais perigoso. O tempo dedicado à escrita das respostas foi de 5 minutos e, ao debate, de 30 minutos.

Após essa reação, dois palestrantes falaram um seguido do outro e, posteriormente, foi realizada uma nova rodada de reações, relativa a ambas as apresentações. O segundo palestrante foi André[63], militante do Partido Pirata, que fez uma exposição técnica sobre criptografia e o funcionamento da Internet e de redes de computadores em geral. O objetivo dessa exposição foi introduzir aos presentes o funcionamento de mecanismos de vigilância digital e como se proteger dela, o que dependia do uso crítico de ferramentas e da adoção de novos comportamentos. O

62 Anexo 1

63 Nome fictício, pois o palestrante não deu permissão para que seu nome verdadeiro fosse divulgado.

terceiro palestrante foi Marcos[64], também do Partido Pirata, que apresentou o Marco Civil da Internet e a lei de Acesso à Informação, focando na parte legal relativa à privacidade e ao anonimato[65] no Brasil. A reação realizada ao final dessas duas palestras consistia na seguinte pergunta: "Existe algum ''cara de TI'' na sua organização que já falou de algum tópico abordado aqui? Se sim, comente." Novamente, o tempo dedicado à escrita das respostas foi de 5 minutos e, ao debate, de 30 minutos.

A apresentação final ficou por conta da equipe de pesquisa. Para evitar que os participantes dessa oficina saíssem decepcionados, considerando a possibilidade dos participantes estarem na oficina mais interessados em um conhecimento aplicável do que em discussões teóricas, optamos por apresentar algumas ferramentas e dicas para comunicação segura[66].

Ao final dessa apresentação foi feita uma terceira rodada de reações, dessa vez com 20 min e 90 min reservados, respectivamente, para a escrita e para o debate. Os participantes responderam sete questões avaliando a oficina, e no debate expuseram quais novas ações poderiam ser realizadas no campo desta pesquisa. Aqueles que desejassem fazer parte de novos seminários desta Pesquisa-Ação também tiveram a opção de adicionar telefone e e-mail de contato. O relato da roda final e os dados coletados ao longo da pesquisa serão expostos na seção seguinte.

4.2 RESULTADOS COLETADOS

Nessa subseção irei expor os dados coletados nas reações da oficina-piloto e do questionário online[67]. A discussão dessa informação coletada em campo se dará na seção seguinte.

Entre os 25 participantes da primeira oficina, 16 se identificaram como do sexo masculino e 9 do feminino. Na pergunta relacionada ao espaço de militância, dentre os 25 participantes, 9 afirmaram participar de um partido político, 14 de um movimento social, 5 de um sindicato e 8 afirmaram atuar em outra esfera de militância.

Em relação a distribuição etária dos participantes, um era menor de 18 anos, 7 possuíam entre 18 e 24 anos, 7 entre 25 e 29 anos, 3 entre 30 e 34 anos, 4 entre 35 e 39 anos, um entre 40 e 44

64 Nome fictício, pois o palestrante não deu permissão para que seu nome verdadeiro fosse divulgado.

65 Falarei desses conceitos no próximo capítulo.

66 As ferramentas escolhidas para serem apresentadas foram decididas através das discussões no seminário, onde se buscou apresentar aquelas que pudessem auxiliar nas demandas mais genéricas (ou seja, comuns a diversos espaços de militância) apresentadas pelo seminário. Os slides com a lista de ferramentas constam como anexo da dissertação. Um panorama das ferramentas apresentadas também será exposto no próximo capítulo.

67 Vide capítulo anterior.

anos, e 2 com mais de 50 anos[68]. Quando questionados sobre a existência de um quadro de TI dentro da organização que já tivesse tocado em algum dos assuntos tratados no evento, 14 responderam que sim, 10 que não e um não respondeu.

Quando pedidos para enumerar seus três principais inimigos os participantes responderam:

- 15 citaram a Polícia (PM, Federal ou Civil), a repressão ou a Unidade de Polícia Pacificadora (UPP);
- 7 citaram a extrema-direita, reacionários ou fascistas;
- 7 citaram a burguesia ou o estado burguês;
- 5 citaram o governo, a justiça ou o Ministério Público Federal (MPF);
- 5 citaram o exército;
- 3 citaram a "patronal";
- 3 citaram os Estados Unidos da América (EUA) ou o imperialismo;
- 3 citaram grandes empresas ou a mídia;
- 2 citaram "pelegos" ou "canalhas do movimento";
- 2 citaram agências reguladoras;
- 1 citou a sociedade;
- 1 citou a milícia;
- 1 citou "homofóbicos, racistas e machistas";
- 1 citou a "direita liberal";
- 6 não souberam responder;

A seguir, quando indagados sobre qual desses três inimigos era o mais perigoso, os participantes responderam da seguinte maneira:

- 8 escolheram a Polícia (PM, Federal ou Civil), a repressão ou a Unidade de Polícia Pacificadora (UPP);
- 3 escolheram a extrema direita, reacionários ou fascistas;
- 3 escolheram a burguesia ou o estado burguês;
- 2 escolheram o governo, a justiça ou o Ministério Público Federal (MPF);
- 1 escolheram os Estados Unidos da América (EUA) ou o imperialismo;
- 1 escolheu os "canalhas do movimento";
- 7 não responderam ou não souberam escolher um inimigo mais perigoso dentre os 3 citados anteriormente;

68 Nenhum participante se encontrava na faixa entre 45 e 49 anos de idade.

Durante a roda final, falaram e responderam ao questionário 23 dos 25 participantes da oficina. A primeira pergunta dessa sessão final de reações foi se a oficina tinha sido útil; todos afirmaram, em fala e no papel, positivamente. As perguntas seguintes foram todas discursivas, isto é os participantes tinham um campo aberto para escrever suas respostas de forma livre e tempo de fala para explicar seus posicionamentos. Quando perguntados sobre o que foi positivo na oficina, os 4 pontos mais citados foram as ferramentas apresentadas (11 citações); o público composto por militantes e por pessoas que estavam fora do meio acadêmico e da Tecnologia da Informação (6 citações); a presença de palestrantes externos à universidade (6 citações); e as trocas de relatos e discussão coletiva de falhas de segurança, riscos e ameaças comuns à atividade dos militantes (6 citações). Na tabela abaixo seguem todas as respostas citadas:

Resposta	**Quantidade de citações**
Ferramentas apresentadas	11
Presença de militantes e pessoas fora do meio de TI	6
Trocas de relatos / análise de falhas e ameaças	6
Os palestrantes externos	6
Discussão sobre o Marco Civil	4
Tudo (foi perfeito)	4
Didática / Linguagem	4
Debate sobre o conceito de Software Livre	3
Preocupação da organização em oferecer comida	3

Tabela 1: Elementos presentes na resposta à pergunta "O que você diria que foi bom [sobre a oficina]?"

Quando perguntados sobre o que foi ruim na oficina, 9 participantes destacaram a falta de profundidade na abordagem, apontando como causa disso o tempo curto. Seis participantes destacaram em suas falas que a falta de exercícios foi um problema da oficina.

Resposta	**Quantidade de citações**
Superficialidade / Tempo curto	9
Falta de exercícios práticos	6
Nada	6
Repetição de temas ao longo da oficina	2
Falhas pontuais de organização	2
Duração muito longa para um único dia	1
Escolha do local	1
Linguajar técnico	1

Tabela 2: Elementos presentes na resposta à pergunta "O que você diria que foi ruim [sobre a oficina]?

Sobre o que acharam mais útil da oficina, as respostas se concentraram no uso de ferramentas, com 18 participantes apontando esse elemento em suas reações, o dobro do que o segundo elemento mais citado, a saber, a discussão sobre casos concretos.

Resposta	**Quantidade de citações**
Ferramentas apresentadas	18
Discussão sobre casos concretos	9
Relação entre o mundo analógico e o digital	6
Discussão sobre legislação	5
Tudo	1

Tabela 3: Elementos presentes na resposta à pergunta "Quais tópicos abordados nessa oficina você achou mais útil?"

Quando indagados sobre tópicos não abordados na oficina, 10 participantes citaram a ausência de alguma ferramenta, mais que o dobro da segunda resposta mais citada.

Resposta	Quantidade de citações
Alguma ferramenta específica	10
Relação entre a vigilância e a sociedade moderna	4
Abordagem específica para um determinado grupo	3
Não sentiu falta de nada	2
Discussão de gênero e racial	2
Como multiplicar o conhecimento abordado dentro dos grupos	2
Estatísticas relacionadas a vigilância	1
Mais foco em legislação	1
Elementos audiovisuais de apresentação	1

Tabela 4: Elementos presentes na resposta à pergunta "Existe algum tópico que você sentiu falta, e que deve ser abordado em ações futuras?"

Vinte e um dos vinte e três presentes na roda final afirmaram que mais membros da sua organização se interessariam pela oficina, 2 não se pronunciaram e nenhum participante afirmou um possível desinteresse. E, em concordância com as respostas anteriores, o conhecimento técnico foi aquilo que majoritariamente os participantes (15) afirmaram ser de interesse das suas organizações[69] [70].

Resposta	Quantidade de citações
Conhecimento técnico (em geral ou alguma ferramenta específica)	15
Cultura de segurança	5
Debates teóricos ou políticos sobre a vigilância	2
Legislação	2
Segurança para mulheres	1

Tabela 5: Tópicos que os participantes indicaram como os mais demandados pelos membros das suas organizações em uma eventual nova oficina

69 O uso da palavra técnico é parafraseada dos entrevistados. Apesar do uso dessa palavra ir na contramão do referencial teórico da TAR, escolhi mantê-la para dialogar com a visão difundida da separação do técnico e do social.

70 Alguns enunciaram em suas falas uma ou mais ferramentas específicas, outros apenas falaram de ferramentas de forma genérica, sem citar alguma em especial. Para fins de visualização, consolidei todas essas respostas em um único campo.

Na pesquisa online[71], foram coletadas 23 respostas entre 15 de novembro de 2015 e 26 de junho de 2016. Entre os entrevistados, 15 afirmaram ser militantes de sindicatos, 2 de partidos político e 6 de movimentos sociais ou outras categorias de organização política. Quando perguntados sobre o estado de atuação, 8 afirmaram atuar no Rio de Janeiro, 4 em São Paulo, 1 no Ceará, 1 no Distrito Federal, 1 no Espírito Santo, 1 em Goiás, 1 no Maranhão, 1 no Paraná, 1 no Rio Grande do Sul e 4 não responderam.

Meio de divulgação	**Quantidade de organizações que afirmaram usar**
Facebook	20
Site/Blogue	17
Meios impressos	14
Whatsapp	11
Twitter	10
Telefone	7
Telegram	4
YouTube	4
Newsletter/E-mail	4
Televisão	3
Rádio	2
Telegrama	1
SMS	1
Outdoor	1

Tabela 6: Meios de comunicação usados para divulgação externa das ações

No tocante à comunicação externa, isto é, como a organização comunica suas ideias e ações à sociedade, o Facebook dominou a pesquisa online, com 20 citações, seguido por blogues e sites web, com 17 citações, e meios impressos, com 14 citações.

71 Também realizada presencialmente no Curso Anual do NPC em 2015. Como as perguntas foram as mesmas, os resultados aqui são apresentados de forma consolidada. Dessa forma, sempre que me referir daqui em diante à pesquisa online me refiro também às respostas obtidas em papel na referida ocasião.

Meio de comunicação	Quantidade de organizações que afirmaram usar
E-mail	19
Telefone	18
Facebook	16
Whatsapp	15
Correio	5
GoogleDocs	4
Boletins impressos	3
Telegram	2
Signal	2
SMS	2
RiseUp	1
Trello	1

Tabela 7: Meios de comunicação usados para comunicação interna da organização

Em relação à comunicação interna da organização, o e-mail apareceu como o mais citado, com 19 citações, seguido pelo telefone com 18, pelo Facebook com 16 e pelo WhatsApp com 15.

Em relação à existência de um setor dedicado à TI na organização, 20 responderam positivamente, 2 negativamente e 1 não respondeu. Quando perguntados se sabiam dizer o que é Software Livre, 18 afirmaram positivamente, 3, negativamente e 2 não responderam. Apesar disso apenas um dos entrevistados afirmou usar ferramentas livres quando perguntado quais os programas usados pelas organizações[72].

Quando perguntados se acreditavam que alguém poderia vigiá-los e se sofreram algum tipo de perseguição, 19 afirmaram que acreditam estar passíveis de monitoramento por alguém, 2 afirmaram que não e 2 não responderam. Onze responderam já ter sofrido repressão ou perseguição, 10 responderam negativamente e dois nada responderam.

Quando perguntados quem seriam os interessados em vigiar a sua organização, os participantes da pesquisa online responderam da seguinte forma:

72 Falarei novamente sobre software livre no capítulo a seguir, porém adianto para o leitor que usarei o termo ferramentas livres para referir-me àquelas cujo código é aberto, ou seja, não é proprietário. É importante ressaltar que ferramentas proprietárias podem possuir *backdoors* colocados pelos desenvolvedores sem o conhecimento dos usuários. No capítulo seguinte falo dos *backdoors* e por que estes podem ser evitados através do uso de ferramentas livres.

Resposta	Quantidade de citações
Patronal, a gerência	6
Outras organizações políticas	6
O governo federal, governos estaduais ou municipais	5
Polícia (PM, Civil, PF), DRCI, ABIN, serviços de inteligência, Forças Armadas	4
Os EUA, imperialismo	4
Não respondeu, respondeu algo distinto do perguntado	4
Direita, reacionários	3
Oposição interna, outros membros do movimento	2
O estado burguês, a burguesia	2
Hackers	2

Tabela 8: Adversários que os participantes da pesquisa online acreditam poder vigiá-los

Entre aqueles que responderam ter sofrido repressão ou perseguição, 8 afirmaram que essa experiência provocou mudanças nos hábitos da organização e 3 afirmaram que não houve mudança significativa. Na tabela abaixo estão discriminadas as mudanças citadas.

Respostas	Quantidade de citações
Menor exposição / aumentou a cautela na atividade online	5
Muito pouco / Não mudou	3
Estudos internos para criação de procedimentos	2
Buscar chamar atenção do público para o ocorrido	1
Evitar uso de telefones / meios digitiais pare certos assuntos	1

Tabela 9: Mudanças provocadas pela repressão ou perseguição no funcionamento interno da organização

Por fim, 7 dos entrevistados afirmaram ter havido campanhas internas promovidas pela direção de sua organização para conscientização sobre o tema da vigilância, 8 afirmaram negativamente e 8 não responderam.

4.3 DISCUSSÃO DOS RESULTADOS

Na oficina-piloto, o principal inimigo que os participantes relataram temer foi a Polícia, com larga margem em relação aos demais inimigos. Um provável motivo para isso está presente na fala de um participante, reproduzida abaixo, onde fica claro que o poder coercitivo da polícia transcende o meio digital:

> Eu moro numa área de UPP. Se a Polícia quiser minha senha, ela vai pegar meu celular, me encher de porrada e vai fazer com que eu digite a senha, e vai ser isso (RELATORIA, 2016)

Outro fator que pode ter contribuído para essas respostas foi o fato dessa reação ter sido realizada imediatamente após a apresentação de Thiago, onde foi relatada sua investigação e prisão pela Polícia Civil do Rio de Janeiro, o que pode ter induzido alguns participantes a elencarem a Polícia entre seus inimigos. A composição da oficina, com maior presença de movimentos sociais e pequenos partidos políticos, ideologicamente localizados na esquerda, também é um fator a ser levado em conta. Ainda mais se considerarmos que no questionário online, onde a maioria das respostas veio de militantes de sindicatos, a Polícia não foi tida como principal inimigo, dando lugar para a "patronal" e para "outras organizações políticas".

Uma questão presente nas respostas do questionário, também trazida à tona na oficina, foi a dificuldade do uso do software livre pela militância. Se, no questionário, a maioria afirmou conhecer o software livre, sem, contudo, fazer uso deste tipo de software, na oficina um dos participantes afirmou:

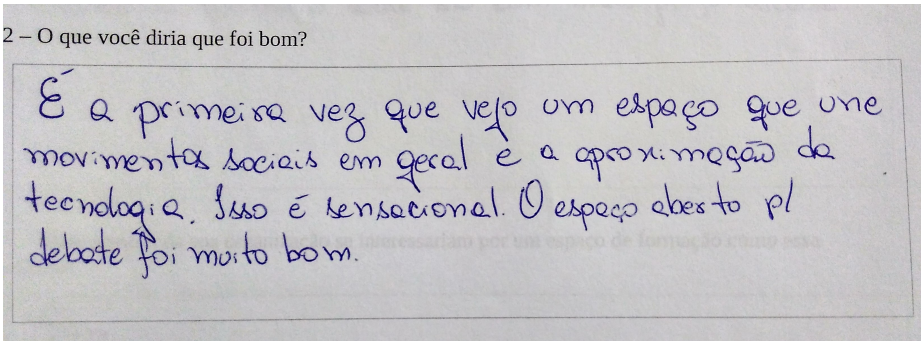
> Eu, o Renato e mais uns aqui imagino, somos *Adobe-dependentes*, porque eu sou fotógrafo e preciso do Lightroom, ele porque é designer e precisa do Illustrator; a gente que edita vídeo precisa de Premiére, e o Linux infelizmente ainda não oferece ferramentas suficientemente boas, à altura pra substituir essas. […] [O que existe de alternativa livre disponível] não chega aos pés. Infelizmente, […] porque [se] a gente precisa de produtos bons, tá nas mãos desses filhos da puta. É a vida. Então esse é o ponto final que eu quero colocar, não é como se livrar disso, mas como equilibrar isso […] tem que pensar nesse caminho, ou seja, de que forma, já que estamos de alguma maneira prisioneiros de Bill Gates, a gente pode pelo menos enxergar um pouco mais as barras e entortá-las um pouquinho mais pra botar o braço pra fora. (RELATORIA, 2016)

Ou seja, por mais que a oficina tenha se preocupado em apresentar os riscos relacionados ao uso de certas ferramentas proprietárias[73], as alternativas livres existentes não satisfazem todas as necessidades dos movimentos políticos.

Outro fator importante de ser destacado nas informações fornecidas pelos participantes é o grande peso dado nas reações ao aprendizado de novas ferramentas. Esse anseio dos participantes pela "técnica" deve ser levado em conta por parte da equipe de pesquisa em futuras ações, que por sua vez deve ressaltar e reforçar a necessidade de se encarar a tecnologia como um ator dentro de um conjunto de atores que compõe as redes sociotécnicas que desenvolvem a atividade militante e

73 Pela própria natureza do software proprietário, não se pode saber, ao certo, quais instruções estão sendo executadas na máquina durante a operação do programa. Não existe, portanto, garantia ao usuário de que o fabricante do programa não incluiu um b*ackdoor* no código. *Backdoors* são programas que permitem o acesso remoto a um dispositivo informacional por meio de serviços criados ou modificados para este fim. Falarei mais sobre esses programas no próximo capítulo.

não como algo apartado de outras ações, espaços e elementos da militância. Isso fica evidente quando lembramos do vazamento de informações do Anonymous RJ por um membro do coletivo, relatado no capítulo 1. Nesse caso, a DRCI foi capaz de obter a identidade dos administradores da página do coletivo no Facebook não através de procedimentos complexos da ciência da computação, como quebra de criptografia ou exploração de falhas de software, mas devido a um ato de traição pessoal de um militante em conflito com o restante da organização[74]. Esse caso ilustra bem a natureza sociotécnica da vigilância e das TICs, que implica que qualquer solução encontrada por parte dos movimentos sociais para se proteger do panóptico eletrônico do estado também deverá ser, a princípio, sociotécnica.


2 – O que você diria que foi bom?

É a primeira vez que vejo um espaço que une movimentos sociais em geral e a aproximação da tecnologia. Isso é sensacional. O espaço aberto p/ debate foi muito bom.

Figura 1: Extrato da reação escrita de um participante da oficina

É importante discutir a aplicação da Pesquisa-Ação no planejamento da oficina e discutir como isso se refletiu nos resultados apresentados em campo. De maneira análoga, esses resultados também podem ser usados como parte importante do planejamento de futuras ações de Pesquisa-Ação no tema da vigilância. O público participou de forma ativa da oficina e esta serviu a seu propósito inicial de ser um ponto de partida para a construção de novos projetos de Pesquisa-Ação na temática da vigilância, conforme foi observado pelo fato de 19 participantes terem fornecido suas informações de contato para a equipe de pesquisa, sob a promessa de auxiliar em futuras ações em seus territórios. Conforme ilustro na imagem abaixo, em suas reações os participantes registraram que sentiram a necessidade de espaços que promovam a aproximação dos movimentos sociais com a tecnologia. Porém, futuras ações também devem levar em consideração a linguagem apresentada e a adequação para o público determinado pelo espaço onde a Pesquisa-Ação vier a acontecer. Na ação relatada no presente texto, a diversidade do público dificultou essa

74 Segundo um olhar sociotécnico, tanto a quebra de criptografia quanto a traição pessoal possam ser vistas a partir do mesmo argumento, isto é, o do rompimento de uma tradução que mantinha a rede militante estável e coesa. Isso ilustra a natureza dinâmica das traduções que mudam para formar novos elos e transladar para novos aliados. Isto é, a nova tradução provoca novas alianças e a traição das alianças anteriores.

adequação da linguagem, o que resultou em reclamações por parte dos participantes, como ilustrado a seguir:

> Eu senti falta de um olhar mais atento a questão de gênero, de raça, etnia, e sobretudo geracional, porque a gente ta aqui num grupo majoritariamente jovem, mas a questão geracional pesa muito, claro que a preguiça é uma inerente ao ser humano, eu também sou preguiçosa, to com pressa eu vou no caminho que eu conheço, mas tem uma questão aí de geração que deve ser levado em conta, pra pensar nas metodologias de apropriação mesmo dessas ferramentas que vão nos deixar mais seguras e seguros. (RELATORIA, 2016)

Essa necessidade de adequação da linguagem ao público soma-se às reclamações da falta de exercícios práticos e do pouco tempo de duração da ação. Traduzo esses comentários como um indício da existência de interesse do público-alvo na construção de novas ações, com tempo maior para debate, prática e assimilação do conteúdo. Dessa forma, abre-se espaço para a intervenção da universidade não só em ações que tomem o formato de cursos, como também para outras formas de imersão e assessoria aos movimentos sociais em seus territórios e espaços de militância.

5. CONCEITOS NORTEADORES DO PROBLEMA DA VIGILÂNCIA DIGITAL

Nesse capítulo exponho os eixos teóricos norteadores da vigilância digital que, a partir da discussão coletiva nos seminários, foram apresentados aos participantes da oficina piloto. Parte desses conceitos já foram introduzidos de forma breve ou mencionados nos capítulos anteriores. Acredito que não caberia nesse texto apresentar ferramenta por ferramenta apresentada[75] mas mostrar os três eixos que nortearam a exposição. Esses eixos são:

1. Software livre e software proprietário;
2. Anonimato e privacidade, de acordo com a legislação brasileira;
3. Criptografia e a estrutura da Internet;

5.1 SOFTWARE LIVRE E SOFTWARE PROPRIETÁRIO

Softwares são formados por conjuntos de instruções (algoritmos) escritos pelo programador, usando linguagens de programação que buscam se aproximar da linguagem humana[76], chamadas de linguagens de alto nível[77]. Esse código é então compilado por um programa chamado compilador, para que seja convertido em código de máquina, isto é um programa executável por um computador. O código de máquina não é legível por seres humanos, mesmo aqueles versados em programação. Desta forma, para entender o que o está sendo executado pelo software, é necessário o acesso ao código fonte.

Como dito no capítulo anterior, o conceito de software livre está relacionado ao acesso ao código fonte de um programa de computador: enquanto no software proprietário a leitura do código fonte é vedada ao usuário, no software livre, segundo Richard Stallman, qualquer usuário pode exercer o que define como as Quatro Liberdades, que são:

1. Liberdade para executar o programa como quiser, para qualquer fim.
2. Liberdade de modificar o programa para atender às suas necessidades, como desejar.

75 Para os leitores que desejarem, os slides apresentados na oficina contam como anexo da dissertação.

76 Por questões econômicas e geopolíticas a imensa maioria das linguagens de programação usadas de forma ampla em projetos de software são feitas com comandos em inglês.

77 Exemplos de linguagens de alto nível são C, Java, C#, Perl, PHP, Ruby, Fortran, Cobol, Python, entre outros.

3. Liberdade de redistribuir cópias, tanto do programa quanto, se desejar, do código fonte, seja gratuitamente ou por uma taxa.
4. Liberdade de distribuir versões modificadas do programa, de modo que a comunidade possa se beneficiar de suas melhorias. (STALLMAN, 1998)

Existe na academia e na comunidade hacker[78] um debate entre o Software Livre e o Open Source, ainda que ambos se refiram a softwares de código aberto. Os defensores do primeiro encaram essa abertura como um movimento social, que encara a liberdade como um direito inerente ao usuário de um programa, o de saber e poder modificar o que está sendo executado em sua máquina. Por outro lado, os defensores do segundo encaram a abertura do código como uma metodologia mais eficiente de desenvolvimento de software. Foge ao escopo desta dissertação entrar neste debate. Desta forma, uso o termo ferramentas livres para referir-me àquelas cujo código é aberto, ou seja, que não é proprietário[79].

5.1.1 *Backdoors* em softwares proprietários

É importante ressaltar que ferramentas proprietárias podem possuir *backdoors* colocados pelos desenvolvedores sem o conhecimento dos usuários. Conforme mencionado no capítulo anterior, *backdoors* são pequenos programas, escondidos em sistemas maiores, que permitem o acesso remoto a um dispositivo informacional por meio de serviços criados ou modificados para este fim. Segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) "[h]á casos de *backdoors* incluídos propositalmente por fabricantes de programas, sob alegação de necessidades administrativas. Esses casos constituem uma séria ameaça à segurança de um computador que contenha um destes programas instalados pois, além de comprometerem a privacidade do usuário, também podem ser usados por invasores para acessarem remotamente o computador." (CERT.br, 2017)

---

78 Apesar de hacker ser popularmente conhecido como alguém que invade um sistema computacional, o significado original da palavra se refere aos amantes da programação e do desenvolvimento de soluções tecnológicas para problemas cotidianos.

79 Para um debate sobre essa questão, sugiro a leitura do artigo "Por que o Código Aberto não compartilha dos objetivos do Software Livre" de Richard Stalmann (2007) disponível em: https://www.gnu.org/philosophy/open-source-misses-the-point.html (Acessado em 10 de janeiro de 2018).

Um exemplo de *backdoor* inserido em um software proprietário é o caso do Android. A Google, principal responsável pelo desenvolvimento da plataforma em 2011, usou um *backdoor* nativo do sistema operacional para remover, sem consentimento, softwares maliciosos que tinham sido instalados nos celulares de 50.000 a 200.000 usuários (KEIZER, 2011). Em 2010, Rich Cannings, chefe da equipe de desenvolvimento responsável pela segurança do Android, escreveu no blogue de desenvolvimento do sistema que:

> Em casos em que usuários tenham instalado uma aplicação maliciosa que represente uma ameaça, nós desenvolvemos tecnologias e processos para remover remotamente um programa do dispositivo. Se uma aplicação for removida dessa maneira, o usuário recebe uma notificação em seu celular.[80] (CANNINGS, 2010)

Steve Jobs, falecido CEO da Apple, responsável pelo desenvolvimento do iPhone, admitiu em 2008 para o *Wall Street Journal* que os celulares de sua empresa também possuíam tal funcionalidade (WINGFIELD, 2008).

Ainda que as empresas afirmem que colocam esses dispositivos em seus sistemas por questões de segurança, a presença de *backdoors* traz dois problemas importantes para a questão da privacidade:

1. Coloca o controle da privacidade do usuário na mão de uma empresa, tirando-o do próprio usuário do sistema;
2. Se por algum motivo o funcionamento interno de um *backdoor* vazar para fora da empresa, ele se torna uma falha que pode ser explorada por qualquer terceiro malicioso. (CERT.br, 2017)

Conforme foi apresentado na oficina, o software livre resolve essas duas questões uma vez que um código-fonte público para ser lido por qualquer um versado em programação impossibilita que seja colocado um *backdoor* malicioso lá, uma vez que este seria visto e apagado rapidamente.

5.2 LEGISLAÇÃO, PRIVACIDADE E ANONIMATO

Segundo Kerr (2007, p. 17), o conceito de anonimato está relacionado a um estado onde a identidade de uma pessoa está escondida, podendo tanto ser aplicado para casos nos quais esta se anonimiza para tentar fugir da repressão do diálogo quanto nos casos em que busca-se a ocultação

80 "In cases where users may have installed a malicious application that poses a threat, we've also developed technologies and processes to remotely remove an installed application from devices. If an application is removed in this way, users will receive a notification on their phone." (tradução do autor)

de um crime. A privacidade por outro lado, está relacionada ao direito ao espaço íntimo e ao controle das informações pessoais, o que por sua vez está diretamente ligado ao isolamento de uma pessoa em relação aos sentidos e equipamentos de vigilância de terceiros. (ALLEN, 2007, p. 393)

Segundo a Constituição Federal de 1988, a privacidade é garantida a todos cidadãos, porém o anonimato é vedado constitucionalmente, conforme expresso no texto do Artigo 5º:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: […]
>
> IV – é livre a manifestação do pensamento, sendo vedado o anonimato; […]
> X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; (BRASIL, 1988)

Além da Constituição Federal, a Lei Nº 12.527, de 18 de novembro de 2011, que regulamenta o acesso à informação, também garante a privacidade das informações pessoais:

> Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.
>
> §1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:
>
> I – terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e
>
> II – poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem. […]
>
> § 3º O consentimento referido no inciso II do § 1o não será exigido quando as informações forem necessárias:
>
> I – à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;
>
> II – à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;
> III – ao cumprimento de ordem judicial;
>
> IV – à defesa de direitos humanos; ou
>
> V – à proteção do interesse público e geral preponderante. (BRASIL, 2011)

Isto é, salvo nos casos específicos citados acima, a privacidade, diferentemente do anonimato, é um direito do cidadão.

No dia 23 de abril de 2014, a Presidenta da República Dilma Rousseff sancionou a Lei nº 12.965, conhecida como Marco Civil da Internet, que "Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil". (BRASIL, 2014) Nela, tal como na Constituição, a privacidade é garantida:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
>
> I – garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
>
> II – proteção da privacidade;
>
> III – proteção dos dados pessoais, na forma da lei; (BRASIL, 2014)

O anonimato, por sua vez não é citado no texto legal, mas é importante ressaltar que o artigo citado acima reforça que a liberdade de expressão se dará no ambiente online dentro dos termos expressos na Constituição Federal, onde, como já vimos, o anonimato é expressamente vedado.

Dessa forma, o curso foi construído tendo o foco em buscar ferramentas que auxiliassem na garantia da privacidade, ao mesmo tempo em que tivemos o cuidado de explicar para os participantes a questão legal do anonimato.

5.3 CRIPTOGRAFIA E A ESTRUTURA DA INTERNET

O termo computação em nuvem entrou no vocabulário popular para se referir ao uso de serviços online. Porém esse termo também é extremamente confuso para o usuário, como na pesquisa realizada em 2012, e relatada por Bojanova et al (2013), junto a 1000 usuários estado-unidenses investigados, dos quais 51% afirmaram acreditar que tempo chuvoso interferia na computação em nuvem. 29% dos entrevistados também afirmaram que a chamada "nuvem" era de fato uma nuvem; e apenas 16% conseguiram explicar corretamente o que é a computação em nuvem. (BOJANOVA et al, 2013, p. 12)

Na realidade, apesar do conceito de nuvem passar a imagem de distribuição e de dispersão da informação na Internet, o que acontece é que essa informação está em armazenada em algum lugar, em algum servidor. Ao acessar essa informação, estamos acessando um servidor localizado fisicamente em algum lugar via Internet, ou melhor dizendo, por um dos cabos de fibra ótica submarinos que conectam as diversas redes do mundo entre si, formando o que chamamos de Internet, conforme ilustrado no mapa abaixo:

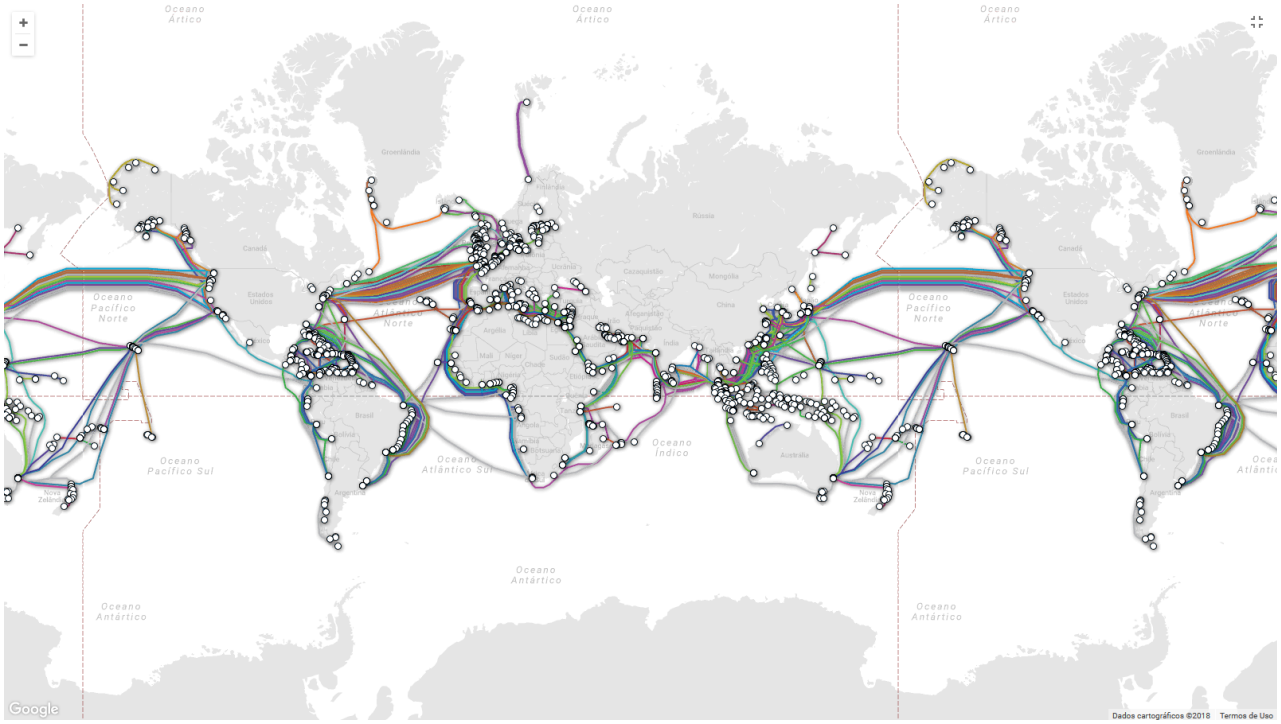


Figura 2: Mapa de cabos submarinos. Dados cartográficos de janeiro de 2018. Disponível em: https://www.submarinecablemap.com

E esses cabos possuem donos. Observa-se isso na imagem abaixo na qual tomo como exemplo o cabo destacado:

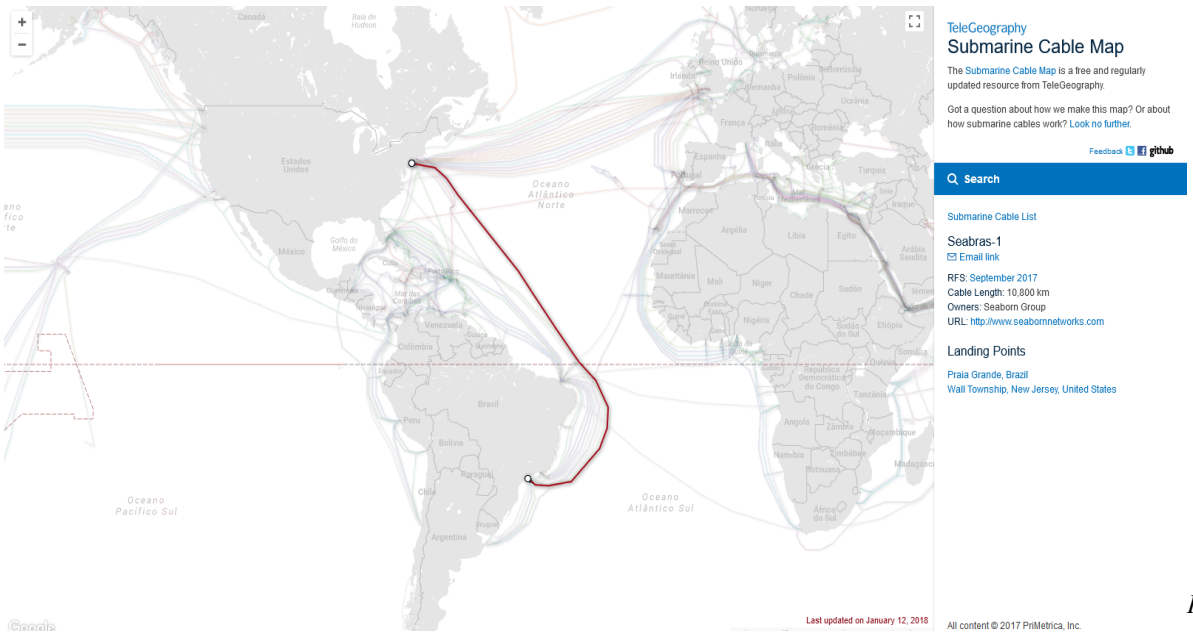


Figura 3: Cabo Seabras-1. Dados cartográfico de janeiro de 2018. Disponível em: https://www.submarinecablemap.com/#/submarine-cable/seabras-1

A proprietária do cabo do exemplo acima é a empresa *Seaborn Group*. O cabo liga a cidade de Praia Grande, na Baixada Santista, à cidade de Nova Jérsei, no nos Estados Unidos.

Dessa forma, ao colocarmos nossas informações em algum serviço web[81], existe a possibilidade de nossas informações serem lidas tanto pelos donos do serviço, quanto pelos donos das redes pelas quais nossa informação trafega até chegar no servidor. Assim sendo, para garantir nossa privacidade, temos como necessidade o uso da criptografia.

A (já mencionada) cartilha de segurança do CERT.br define a criptografia como sendo "a ciência e a arte de escrever mensagens em forma cifrada ou em código". Isto é, a criptografia é o estudo dos processos matemáticos que aplicados a uma mensagem garantem que essa seja possa lida por um destinatário autorizado, mas que pareça completamente ininteligível a terceiros que tentem interceptá-la. Ao pedaço de informação que controla o procedimento de um algoritmo de criptografia damos o nome de chave criptográfica.

Existem duas categorias de criptografia: a simétrica e a assimétrica. Na criptografia simétrica, o algoritmo e a chave são iguais. Dessa forma, o remetente usa a mesma chave para criptografar que o destinatário usa para descriptografar. Por sua vez, a criptografia assimétrica (que é a mais usada na Internet) utiliza um par de chaves matematicamente relacionados, uma para criptografar e outra para descriptografar. A chave usada para criptografar é chamada de chave pública, e pode ser compartilhada por um canal inseguro (como a Internet), enquanto a chave usada para descriptografar é chamada de privada e deve ser mantida em sigilo. Dessa forma se duas pessoas (ou programas de computador) querem conversar de forma segura, elas trocam suas chaves públicas, assim ambas podem criptografar uma mensagem que somente o outro poderá ler (usando a chave privada).[82]

Apesar da quantidade de matemática envolvida na criptografia, como explica a cartilha do CERT.br, os algorítimos criptográficos estão implementados nativamente (e de forma transparente para o usuário) em diversos programas usados cotidianamente na Internet. (CERT.br, 2017) Um exemplo de uso de criptografia no cotidiano é o protocolo HTTPS[83], implementado em diversos servidores web, que criptografa a comunicação entre o navegador e a página visualizada.

81 Como por exemplo um e-mail, uma rede social, um serviço de armazenamento de arquivos, entre outros.

82 Existem diversas implementações de criptografia assimétricas usadas na Internet, como RSA, DSA, El Gamal, entre outros. Para o leitor que deseja entender os meandros dos processos matemáticos envolvidos nesses algoritmos sugiro a leitura do livro "Números Inteiros e Criptografia RSA", de Severino Coullier Coutinho, publicado pelo Instituto de Matemática Pura e Aplicada (2ª ed, 2014, Rio de Janeiro).

83 Sigla para Hyper Text Transfer Protocol Secure.

Ao longo da oficina buscou-se exemplificar quais programas usam a criptografia nativamente[84] e para quais o uso da criptografia requereria alguma interação do usuário[85]. Note que esse eixo está intimamente ligado com a questão do software livre: ainda que programas como o WhatsApp afirmem possuir criptografia nas suas conexões, devido ao fato do software ser proprietário, o usuário não possui garantia de que não existe nenhum *backdoor* inserido para coletar suas informações pessoais. Tampouco seria possível que usuários capazes tecnicamente e motivados decidam de maneira voluntária auditar o código do programa para garantir e melhorar a segurança das comunicações.

84 Um exemplo de programa que usa a criptografia nativamente é o cliente de troca de mensagens Signal.

85 Um exemplo desse caso é a criptografia de e-mails usando o cliente de e-mails Thunderbird em conjunto com a extensão Engimail. Para celulares Android, uma alternativa é o cliente de e-mails K-9 e o aplicativo OpenKeyChain.

6. CONCLUSÃO

6.1 É POSSÍVEL SER ATIVISTA SEM SER VIGIADO?

Comecei este trabalho com o desejo de impactar de forma positiva a maneira pela qual o ativismo organizado utiliza as TICs. Dessa forma, não quis, e não quero, propagar a paranoia. O objetivo dessa dissertação não é descrever o ciberespaço como um lugar horrível onde o ativismo é vigiado incessantemente pelo estado e por agentes privados.

Essa narrativa pessimista não explica o papel dos midiativistas nas manifestações de 2013 e tampouco explica o papel de celulares, computadores e redes em diminuir as distâncias físicas que separam militantes de uma mesma organização. O fato de ativistas terem participado e se interessado por esta Pesquisa-Ação é um indicador de que existe, nesse meio, a preocupação com a vigilância digital, ao mesmo tempo que suas respostas nas reações indicam que não abrem mão do uso das TICs nas suas atividades.

Segundo Bruno (2012), "[c]omunicar é deixar rastro. A máxima pragmática 'não podemos não comunicar' pode ser reescrita: não podemos não deixar rastros". No ciberespaço, porém, esses rastros ganham uma nova dimensão: para além do que colocamos de forma voluntária nas redes sociais, outros rastros relacionados são produzidos; e, para além do receptor, localizado espacial e temporalmente, para quem a informação é destinada, nossos rastros ficam disponíveis para serem acessados por outros e arquivados para a posteridade. (BRUNO, 2012, p. 687)

Dessa forma, a perspectiva necessária para futuras ações a serem desenvolvidas no tema da vigilância digital sofrida por movimentos políticos deve focar na compreensão da Internet e das TICs enquanto sistemas sociotécnicos, formados por diversos atores que precisam ser mapeados e compreendidos na hora de escolher quais artefatos e tecnologias serão usados para a comunicação interna e externa dos coletivos. Isso é, ao encarar as TICs enquanto redes de não-humanos e humanos, ambos passíveis de traição, os ativistas se tornam capazes de avaliar essas tecnologias de forma crítica e fazer escolhas informadas sobre o risco que escolhem sofrer para atingir os seus objetivos. Consideraria, portanto, como um exemplo de caso de sucesso, um participante da oficina que continue usando serviços proprietários em sua militância, como o WhatsApp e o Gmail, por exemplo, mas fazendo isso reconhecendo os riscos associados com o uso dessas ferramentas, a capacidade dos seus vigilantes em explorar esses riscos e os benefícios trazidos pelo uso dessas ferramentas (em relação a possíveis alternativas) para a sua militância. Defino como um bom uso

das TICs aquele que pesa essas três variáveis de forma realista e toma uma decisão com base nesse julgamento. Não se trata portanto de fazer silêncio, mas da melhor maneira de fazer barulho.

6.2 CONTINUIDADE DA PESQUISA E TRABALHOS FUTUROS

O que relatei nessa dissertação foi o início de um projeto que ainda está em andamento. A construção dos seminários e a oficina-piloto de 2016 deram frutos que são colhidos ainda hoje em 2018, mas antes de falar do presente e do futuro, avaliarei o passado, isto é, o que foi relatado neste texto.

Começando pelo emprego da Pesquisa-Ação, o ciclo descrito por Thiollent com todos os 12 temas é grande demais para ser avaliado por completo em um ano. Posso afirmar que conseguimos, ao longo de 2016, concluir a Fase Exploratória e construir, a partir do campo, um seminário para continuarmos a pesquisa. Nesses espaços que construímos com os atores, constatamos que existe um interesse dos movimentos sociais no tema da vigilância, conforme foi constatado pelas avaliações da oficina-piloto e pelo questionário online. Também descobrimos que o formato de oficina foi bem-aceito pelos movimentos sociais, o que me leva a defender que a construção de novas ações semelhantes por parte da universidade pode provocar impactos positivos no combate à vigilância digital.

Porém também foi constatado que o projeto em seu primeiro ano não conseguiu abordar as questões de gênero, raça e geracional, conforme já anunciado na discussão dos dados coletados na oficina. Tratar essas questões será um grande desafio para a equipe de pesquisa, formada majoritariamente por homens e integralmente por jovens brancos. Assim sendo, o projeto deve ter como prioridade a inclusão de membros que fujam desse padrão na equipe de pesquisa e no seminário.

Sobre o presente e o futuro dessa pesquisa, vale destacar que, em 2017, a equipe dedicou-se a usar o contato com os movimentos sociais para a construção do curso de 20 horas relatado anteriormente. Após a conversa com os participantes da oficina-piloto, decidimos que o curso deveria priorizar a formação de multiplicadores responsáveis por reproduzir esse conhecimento nas suas organizações. Assim o curso seria constituído por 16 horas de aula e 4 horas de atividade de multiplicação. Fizemos a primeira turma em novembro de 2017, e temos as multiplicações marcadas para ocorrer no início de 2018. A partir dessas atividades de multiplicação, pretendemos construir novos seminários localizados em espaços de militância específicos. Isto é, planejaremos ações focalizadas em movimentos de favela, enquanto outras serão realizadas junto ao movimento de ocupações urbanas e ainda outras ao movimento feminista, por exemplo.

Esta dissertação é um recorte de um projeto que ainda vive, no qual, novas ações são possíveis e novas conclusões podem surgir. Por isso, gostaria de concluir esta dissertação com a constatação de que nada neste estudo e nas ações construídas foge do permitido em um estado democrático de direitos. Apesar disso, alguns participantes relataram que presenciaram em seu espaço de militância uma resistência para tratar do tema da segurança da informação, conforme exponho na citação abaixo:

> Há uma ideia do senso comum de que quando você faz uma atividade como essa de segurança […] é de que tem algo errado acontecendo, que [estamos nos] escondendo, e não é disso que se trata aqui. Nós não estamos falando de coisas erradas que precisam ser escondidas, estamos falando dos objetivos do ativismo, de mudança social. (RELATORIA, 2016)

Não podemos encarar como crime o estudo da segurança da informação junto aos movimentos sociais, e as futuras ações a serem realizadas devem enfatizar isso, tanto para evitar que o medo afaste a participação de ativistas, quanto para validar os produtos acadêmicos oriundos dessa pesquisa enquanto conhecimento científico a ser publicado e difundido.

Como já dito no capítulo anterior, a privacidade do usuário é uma garantia constitucional de todo cidadão, tal como é também a liberdade de expressão. É direito de todo ativista se colocar contra uma política do estado, é direito de todos falar e ser ouvido sem medo de repressão. É dever do estado garantir esse direito, e não atuar na repressão do mesmo. Se direitos estão sendo reprimidos por quem devia protegê-los, então trabalhos como este se fazem ainda mais necessários.

REFERÊNCIAS

ALLEN, A. L. In: STAPLES, W. G. Encyclopedia of Privacy. vol 1-2. Londres: Greenwood Press, pp. 393-403, 2007.

ALVEAR, C. Tecnologia E Participação: Sistemas de Informação e a Construção de Propostas Coletivas para Movimentos Sociais e Processos de Desenvolvimento Local. 286p. Tese (Doutorado) – Universidade Federal do Rio de Janeiro (UFRJ) – Rio de Janeiro, Março de 2014.

AZEVEDO, L; ROCHA, T. 28 de Janeiro de 2016. Entrevista concedida a Pedro Braga

ARTIGO 19. "Da Cibersegurança à Ciberguerra: O Desenvolvimento De Políticas de Vigilância No Brasil". Disponível em: https://www.article19.org/data/files/medialibrary/38291/Da-Ciberseguranc%CC%A7a-a%CC%80-Ciberguerra.pdf. Acessado em 03 de fevereiro de 2017

BRASIL. Diário do Senado Federal. Ano LXIX – Sup. "C" ao nº 51 – 17 de abril de 2014. Disponível em: http://www.senado.leg.br/atividade/rotinas/materia/getTexto.asp?t=149208&c=PDF&tp=1. Acessado em 17 de fevereiro de 2017

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/ConstituicaoCompilado.htm Acessado em 16 de janeiro de 2018

BRASIL. Lei Nº 12.965, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm Acessado em 16 de janeiro de 2018

BRASIL. Lei Nº 12.527, de 18 de novembro de 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm Acessado em 15 de março de 2018

CANNINGS R. Exercising Our Remote Application Removal Feature. 23 de junho de 2010. Disponível em: https://android-developers.googleblog.com/2010/06/exercising-our-remote-application.html Acessado em 11 de janeiro de 2018

CASTELLS, M. A Sociedade em Rede: Volume 1; Tradução de Roneide Venancio Majer, 8ªed. São Paulo: Paz e Terra. 574p. 1996.

CERT.br, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Cartilha de Segurança para Internet Disponível em https://cartilha.cert.br Acessado em 04 de setembro de 2017

CUKIERMAN, H., TEIXEIRA, C.A.N., PRIKLADNICKI, R., "Um Olhar Sociotécnico sobre a Engenharia de Software", In: RITA – Revista de Informática Teórica e Aplicada, vol 14, no. 2, pp. 199-219. 2007.

DELEUZE, G., GUATTARI, F., Mille plateaux – Capitalisme et schizophrénie, vol. 1. 2ªed. São Paulo: Editora 34, 1995. 94 p. (Coleção TRANS)

DEMIER, F. Nas ruas por direitos: uma análise das jornadas de junho de 2013. Disponível em: http://blogconvergencia.org/?p=2805 Acessado em 28 de fevereiro de 2016

ESTEVÃO, T. V. O Novo Paradigma da Vigilância na Sociedade Contemporânea: "Who Watches the Watchers". Observatório, Lisboa, vol.8, nº2, pp. 155-169, 2014.

FALS BORDA, O. Some basic ingredients. In: FALS BORDA, O.; RAHMAN, M. A. Action and knowledge: breaking the monopoly with participatory action research. Apex Press, 1991

FERREIRA, R. S. F. A sociedade da informação como sociedade de disciplina, vigilância e controle. Información, cultura y sociedad, Buenos Aires, vol. 31, pp. 109-120, dezembro de 2014.

FOLHA DE SÃO PAULO. Retomar a Paulista. São Paulo: Folha de São Paulo. 13 de junho de 2013. Disponível em: http://www1.folha.uol.com.br/opiniao/2013/06/1294185-editorial-retomar-a-paulista.shtml Acessado em 28 de fevereiro de 2016

FOUCAULT, M. Vigiar e Punir: nascimento da prisão; Tradução de Raquel Ramalhete. 27ªed. Petrópolis: Vozes. 288p. 1975.

G1. Rio suspende aumento das tarifas de ônibus, trem, metrô e barcas Passagem de ônibus volta a custar R$ 2,75, mas prefeitura paga diferença: Demais transportes terão valor antigo a partir da próxima sexta-feira (21). Rio de Janeiro. G1 Rio. 19 de junho de 2013. Disponível em: http://g1.globo.com/rio-de-janeiro/noticia/2013/06/apos-protestos-cai-tarifa-de-onibus-no-rio.html Acessado em 6 de dezembro de 2016

HERDY, T. Governo brasileiro não vê indícios de invasão nos sistemas: Ministério da Defesa e Forças Armadas investigam espionagem de dados estratégicos pelos EUA. O Globo, Brasil, 14 de julho de 2013. Disponível em: http://oglobo.globo.com/mundo/governo-brasileiro-nao-ve-indicios-de-invasao-nos-sistemas-9033959. Acessado em 15 de fevereiro de 2017

KEIZER, G. Microsoft: We can remotely delete Windows 8 apps. Oregon: Computerworld. 8 de dezembro de 2011 Disponível em: https://www.computerworld.com/article/2500036/desktop-apps/microsoft--we-can-remotely-delete-windows-8-apps.html Acessado em 11 de janeiro de 2018

KERR I. R. In: STAPLES, W. G. Encyclopedia of Privacy. vol 1-2. Londres: Greenwood Press, pp. 17-19, 2007.

LATOUR, B. Ciência em Ação: Como Seguir Cientistas E Engenheiros Sociedade Afora. 2ªed. São Paulo: Editora UNESP. 440p. 2012.

LAW, J.: Notes on the theory of the actor-network: Ordering, strategy, and heterogeneity, Systemic Practice and Action Research, Vol. 5, Nº 4, agosto, 1992. pp. 379-393.

LYON, D. The Electronic Eye: The Rise of Surveillance Society. Minneapolis: University of Minnesota Press, 270p, 1994.

MARQUES, I. D. C. Engenharias brasileiras e a recepção de fatos e artefatos. In: LIANZA, S. e ADDOR, F. (Ed.). Tecnologia e desenvolvimento social e solidário. Porto Alegre: Editora da UFRGS, 2005. p.13-26. (Sociedade e Solidariedade). ISBN 8570258410

MATTOS, R. Grande imprensa e a repressão policial nas Jornadas de Junho (primeira parte). Disponível em: http://blogconvergencia.org/?p=1767 Acessado em 28 de fevereiro de 2016

O DIA, Eduardo Paes anuncia redução da tarifa dos ônibus para R$ 2,75. Disponível em: http://odia.ig.com.br/noticia/rio-de-janeiro/2013-06-19/eduardo-paes-anuncia-reducao-da-tarifa-dos-onibus-para-r-275.html Acessado em 28 de fevereiro de 2016

PEDRO, R. M. L. R. P. Tecnologias de vigilância: um estudo psicossocial a partir da análise de controvérsias. Trabalho apresentado no GT Tecnologias de Informação e Comunicação: Controle e Descontrole do Encontro Anual da ANPOCS, XXIX, 25-29 de outubro, Caxambu: MG. 2005.

PRIDMORE. Consumer surveillance: Context, perspectives and concerns in the personal information economy. In BALL, K., HAGGERTY, K., LYON, D. Routledge Handbook of Surveillance Studies, Nova Iorque: Routledge, pp. 321-330, 2012

RELATORIA da roda final da oficina-piloto. Rio de Janeiro, 2016

RIO DE JANEIRO. Decreto Nº 44302 de 19/07/2013, Disponível em: https://www.legisweb.com.br/legislacao/?id=256720 Acessado em 28 de fevereiro de 2016

RIO DE JANEIRO. Decreto Nº 44305 de 24/07/2013, Disponível em: https://www.legisweb.com.br/legislacao/?id=256823 Acessado em 28 de fevereiro de 2016

RIO DE JANEIRO. Decreto Nº 44409 de 26/09/2013, Disponível em: https://www.legisweb.com.br/legislacao/?id=258841 Acessado em 28 de fevereiro de 2016

RIO DE JANEIRO. Relatório da Ronda Virtual realizada pela DRCI em 01/03/1991, p.3

ROCHA, T 20 de Janeiro de 2016. Entrevista concedida a Pedro Braga

SOUZA, P. THUM, T. Decreto do RJ que prevê quebra de sigilo causa polêmica. Rio de Janeiro: G1 Rio. Entrevista concedida a Disponível em: http://g1.globo.com/rio-de-janeiro/noticia/2013/07/decreto-de-cabral-que-cria-comissao-para-apurar-vandalismo-cria-polemica.html Acessado em 28 de fevereiro de 2016

SISMONDO, Sergio. An Introduction to Science and Technology Studies. 2ªed. Singapura: Blackwell Publishing. 244p. 2010,

SIMÕES, M., VIANA, N. Meu nome não é Sininho. Agência Pública. 13 de Abril de 2017. Disponível em: https://apublica.org/2017/04/meu-nome-nao-e-sininho/ Acessado em 10 de Janeiro de 2018.

SOBRAL, A.V.L. Ações coletivas em redes: um estudo de caso sobre o Anonymous Rio. 88p. Dissertação (Mestrado) – Universidade Federal do Rio de Janeiro (UFRJ) – Rio de Janeiro, Dezembro de 2016.

MARX, G. T. In: STAPLES, W. G. Encyclopedia of Privacy. vol 1-2. Londres: Greenwood Press, pp. 534-544, 2007.

TATEMOTO, R. "Vigilância em massa é inversão dos princípios democráticos", afirma pesquisador: Sérgio Amadeu, professor da UFABC, fala sobre combate ao terrorismo no contexto das Olimpíadas: depoimento. São Paulo: Jornal Brasil de Fato. Disponível em: https://www.brasildefato.com.br/2016/08/04/vigilancia-em-massa-e-inversao-dos-principios-democraticos-afirma-pesquisador/ Acessado em 17 de julho de 2017

THIOLLENT, M. Metodologia da Pesquisa-Ação. Cortez, 1986.

THIOLLENT, M. Perspectivas da metodologia de pesquisa participativa e de Pesquisa-Ação na elaboração de projetos sociais e solidários. In: LIANZA, S. e ADDOR, F. Tecnologia e Desenvolvimento Social e Solidário. Porto Alegre: UFGRS, pp. 173-189, 2005.

VIANA, N; ROZA, G. Loja de souvenires tecnológicos: Um guia para as compras da vigilância Disponível em: http://apublica.org/vigilancia/loja-de-souvenirs-tecnologicos/. Acessado em 17 de fevereiro de 2017

WELLER. The information state: An historical perspective on surveillance. In BALL, K., HAGGERTY, K., LYON, D. Routledge Handbook of Surveillance Studies, Nova Iorque: Routledge, pp. 57-63, 2012.

WINGFIELD, N. IPhone Software Sales Take Off: Apple's Jobs. Nova Iorque: Wall Street Journal. Disponível em: https://www.wsj.com/articles/SB121842341491928977 Acessado em 12 de janeiro de 2018

ANEXOS

ANEXO 1: QUESTIONÁRIO DE REAÇÕES DA OFICINA-PILOTO

1ª Reação

1 – Qual o seu gênero? _____

2 – Qual a sua raça/cor? _____

3 – Qual a sua idade?_____

4 – Aonde você milita? (Pode marcar mais de um)

a) Movimento social

b) Sindicato

c) Partido Político

d) Outro(s):_____

5 – Qual é o seu espaço de militância?

2ª Reação

1 – Quem seriam os três maiores interessados em vigiar você e a sua organização?

1º – _____

2º – _____

3º – _____

2 – Qual desses seria o mais perigoso? Por que?

3ª Reação

1 – Existe algum “cara de TI” na sua organização que já falou de algum tópico abordado aqui? Se sim, comente.

4 ª Reação

1 – Pra você essa oficina foi útil?

a) Sim b) Não

2 – O que você diria que foi bom?

3 – E o que foi ruim?

4 – Quais tópicos abordados nessa oficina você achou mais útil?

5 – Existe algum tópico que você sentiu falta, e que deve ser abordado em ações futuras?

6 – Mais pessoas da sua organização se interessariam por um espaço de formação como essa oficina?

7 – Você e as pessoas da sua organização se interessariam por um curso mais aprofundado? Quais tópicos que você acha que seriam mais demandados?

(OPCIONAL)

Você tem interesse em construir junto com a gente mais oficinas de segurança para movimentos sociais em seu território/espaço de militância? Se sim, preencha os dados abaixo

Nome ou apelido: _____

Celular (com DDD): _____

E-mail: _____

ANEXO 2: QUESTIONÁRIO DISTRIBUÍDO DE MANEIRA IMPRESSA NO 21º CURSO ANUAL DO NPC (2015) E DISPONIBILIZADO ON-LINE POSTERIORMENTE

Essa é uma pesquisa realizada pelo Núcleo de Solidariedade Técnica da UFRJ (SOLTEC-UFRJ) que tem como objetivo mapear o uso de Tecnologias de Informação e Comunicação (TICs) por movimentos sociais, sindicatos e partidos políticos. Os dados coletados nessa pesquisa serão usados posteriormente para a organização de uma oficina que vise fomentar o uso consciente das TICs por esses grupos.

As informações coletadas pela pesquisa só serão divulgadas de maneira sistematizada e somente de forma que não possibilite a identificação das organizações e das pessoas entrevistadas.

Nome da organização_____

Tipo da organização: _____

( ) Sindicato

( ) Movimento Social

( ) Partido político

( ) Outros

Caso tenha respondido movimento social, por favor informe a(s) sua(s) área(s) de militância

( ) Mulheres

( ) Negras e Negros

( ) LGBTs

( ) Indígenas

( ) Ocupação Urbana

( ) Ocupação Rural

( ) Movimento Estudantil

( ) Movimento de Favelas

( ) Midiativismo

( ) Direitos Humanos

( ) Outros

Caso tenha respondido "outros", favor informar no campo abaixo

OBS: Os dados referentes ao nome e contato são opcionais e não serão divulgadas de forma alguma.

Seu nome ou apelido: _____

E-mail de contato (caso deseje receber o retorno dessa pesquisa e participar de uma oficina de uso de Tecnologias da Informação e Comunicação para Sindicatos, Movimentos Sociais e Partidos Políticos): _____

Cargo/Função na organização: _____

Em que estado você milita?_____

Por que meios você e sua organização usam para divulgar suas ideias e ações?

( ) Telefone

( ) Facebook

( ) Whatsapp

( ) Telegram

( ) Televisão

( ) Rádio

( ) Site

( ) Twitter

( ) Meios impressos

( ) Outros

Se respondeu "outros" na pergunta acima, quais?

_____

Porque vocês usam esses meios (para divulgação/propaganda) e quais beneficios e problemas no uso dessas ferramentas?

Quais meios que você e sua organização utilizam na comunicação INTERNA, isto é, entre militantes, entre a direção e a base, etc?

( ) Telefone

( ) Facebook

( ) E-mail

( ) Whatsapp

( ) Telegram

( ) IRC

( ) Correio

( ) GoogleDocs

( ) Outros

Se respondeu "outros" na pergunta acima, quais?

_____

Porque vocês usam esses meios (para comunicação interna) e quais benefícios e problemas no uso dessas ferramentas?

Existe algum setor ou pessoas que cuidam da parte de informática e comunicação na organização?

( ) Sim

( ) Não

Se você marcou SIM: existe algum detalhe sobre esse responsável que você poderia acrescentar? Qual é a formação dela? Quais são suas responsabilidades? Que ferramentas e sistemas ela gerencia na organização?

Você sabe o que é Software Livre?

( ) Sim

( ) Não

Se você marcou SIM: você e sua organização usam software livres? Quais?

Quais programas vocês usam na sua organização?

( ) Windows

( ) Linux (Ubuntu, Mint, Debian, etc)

( ) MacOS X

( ) Dropbox

( ) Google Drive

( ) Android

( ) iOS

( ) Windows Phone

( ) Mozilla Firefox

( ) Internet Explorer

( ) Google Chrome

( ) Libreoffice

( ) Microsoft Office

( ) TOR (The Onion Router)

( ) Outros

Se você marcou outros na pergunta acima, quais?

_____

Se você marcou NÃO: quais softwares que vocês usam na organização e em seus computadores e dispositivos pessoais?

Você acredita que a organização sofre ou poderia via a sofrer vigilância por parte de algum adversário/inimigo ou outro grupo/instituição (governamental ou não)?

( ) Sim

( ) Não

Quem seriam esses interessados em monitorar as atividades da organização, se existem?

Vocês já sofreram repressão ou perseguição?

( ) Sim

( ) Não

Se SIM, como isso mudou os hábitos da organização?

Já houve alguma conscientização por parte da organização para evitar essa possível vigilância? Explique:

Que medidas vocês tomam atualmente (se tomam) pra evitar essa vigilância?

Você teria interesse em participar de um curso de segurança da informação e contra-vigilância digital voltado para movimentos contra-hegemônicos? (*)

( ) Sim

( ) Não

Sobre a duração do curso, qual(is) seria(m) a sua preferência: (*)

( ) Um curso intensivo com duração de uma semana

( ) Um curso com duração de um mês, com aulas de uma a duas vezes à semana

( ) Um curso com duração de três meses com aulas semanais ou quinzenais

Quais seria(m) o(s) melhor(es) dia(s) da semana e horário(s) para a realização do curso (*)

( ) Dias de semana – Manhã

( ) Dias de semana – Tarde

( ) Dias de semana – Noite

( ) Sábado – Dia inteiro

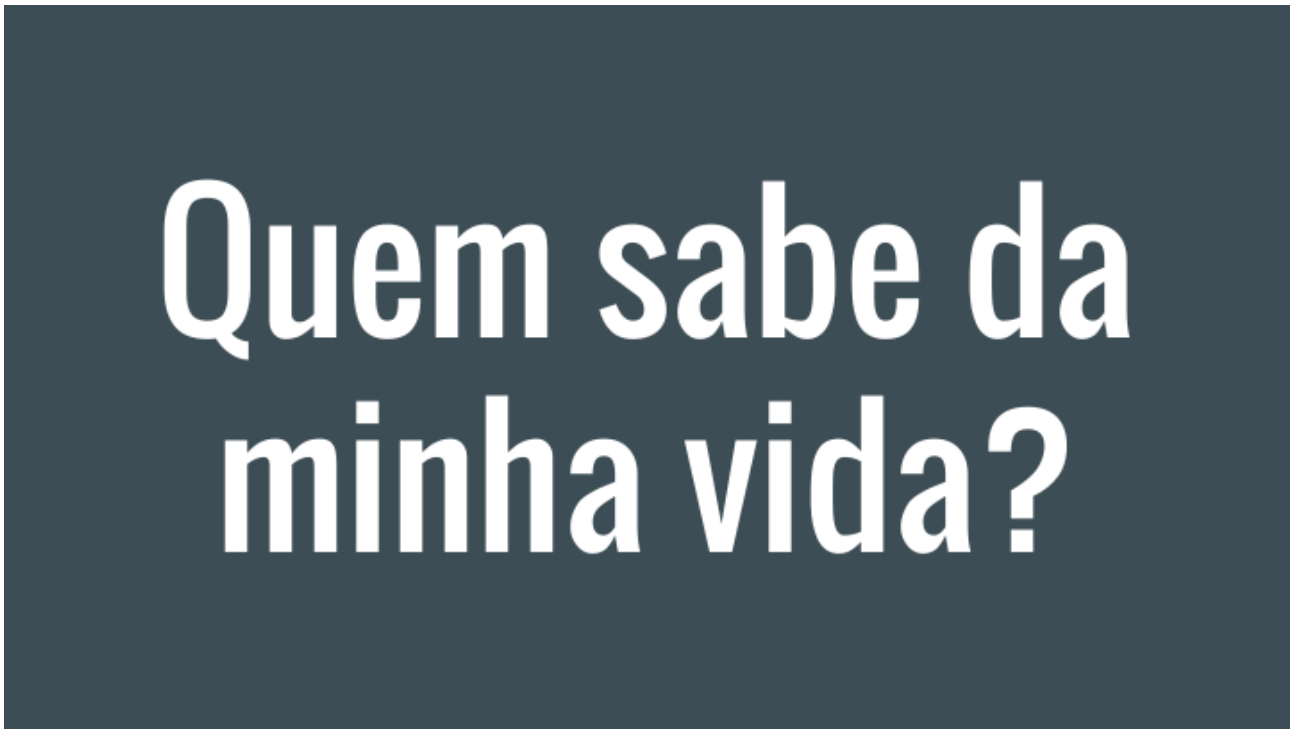
( ) Sábado – Manhã

( ) Sábado – Tarde

Por fim, tem mais alguma questão que você gostaria de relatar/sugerir?

OBS: *As perguntas marcadas com um (*) foram adicionadas no formulário online e não constavam no distribuído fisicamente durante o 21º Curso Anual do NPC.*

ANEXO 3: SLIDES APRESENTADOS NA OFICINA-PILOTO



$3n#@5

Como cuidar da suas senhas da melhor forma

Será que minha senha é boa???????

How secure is my password

https://howsecureismypassword.net/

Eita, e agora, o que eu faço?

- Como criar uma senha segura?
  - Use diferentes caracteres tanto alfanuméricos como não.
  - Evite palavras que sejam de fácil adivinhação e escreva "errado"
  - Use senhas longas
  - Evite usar dados pessoais
  - Use diferentes cifras
- Exemplo: v1V4-@-3nG3nh4r1aP0pu\aR*

Quantas senhas você tem?

- "Tenho uma senha muito boa, nunca vão descobrir"
- "Ahh eu só tenho 1, mas não tem tanto problema assim, né?"

Como organizar minhas senhas?

KeePass

- Armazena as suas senhas criptografadas, precisando você apenas ter a "chave mestra"
- Será possível usar em um pendrive

DICA:

- Quando for escolher a senha do KeyPass, como é a única senha que deverá gravar, formule uma senha longa

[r!pto6rafi@

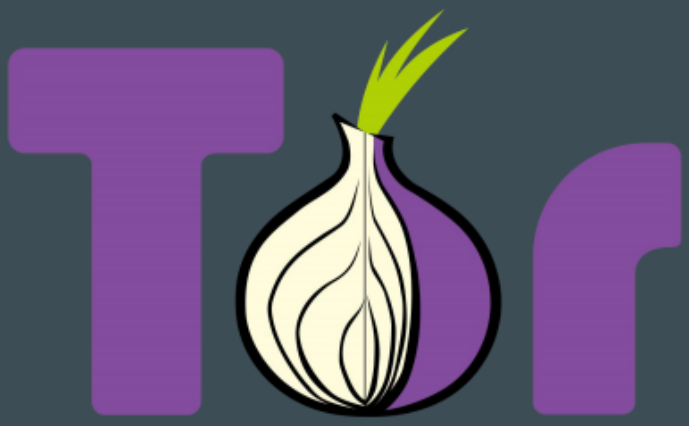
como dificultar que suas informações sejam descobertas

ThunderBird

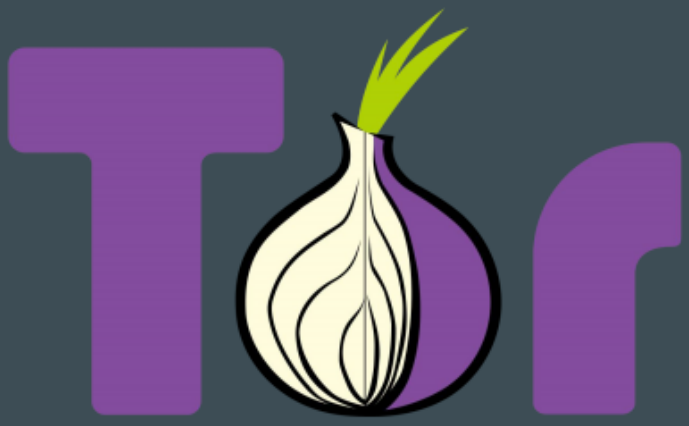
É um cliente de e-mails semelhante ao outlook, porém livre.

Possui uma extensão (Enigmail) que permite criptografar e-mails fazendo de criptografia assimétrica

TOR (The Onion Router)



TOR (The Onion Router)



GnuPG

Software-livre (e por que isso é importante)

Ok, mas o que eu posso fazer tio?

- Para seu Celular:
  - Telegram
  - Signal
  - Firechat
  - Bleep
  - Whatsapp

Características					
Popularizado	x	✓	x	✓	x
Software Livre	✓	✓	✓	x	x
Criptografado	✓	✓*	✓	✓**	✓**
Anonimato*	✓	✓	✓	✓	✓
Uso s/ internet	x	x	✓	x	✓
Mensagens	✓	✓	✓	✓	✓
Ligações	✓	x	x	✓	✓

* Criptografia frágil ** Criptografia não possível de verificar devido ao código ser fechado

Videoconferência segura

E-mails seguros (não-proprietários)

- RiseUp → www.riseup.net
- OpenMailBox → www.openmailbox.org
- ProtonMail → www.protonmail.com
- Autistici →www.autistici.org

Duck Duck Go (https://duckduckgo.com/)

Sistema operacional portátil

- Pode ser usado a partir de um dvd, memória USB ou cartão SD
- Não deixa rastros
- Já vem com várias aplicações instaladas, tais como: TOR, LibreOffice, GIMP, etc

https://tails.boum.org/index.pt.html

Tá mas eu tenho que usar uma rede social/serviço proprietário. O que eu faço?

- Você precisa mesmo?
- Use vários perfis
  - Perfil de militante, profissional, zueiro de bar com os amigos. Assim o Google não sabe quem é você.
- Se necessário use critografia (TOR, criptografia de e-mails, criptografia de arquivos, etc)

Uns pontos importantes

- Nenhum software é perfeito, **nenhum**. Então não confie cegamente em nada, seja redundante na segurança, avalie os riscos de cada ferramenta.

- Mesmo se um software fosse perfeito, não adiantaria nada se tiver um P2 infiltrado, ou se você fica bêbado no bar e fala alto os seus planos de dominação mundial. → A vigilância digital também é analógica

Duvidas

??????????????????

??????????????????

OBRIGADO!

View publication stats