UNIVERSIDADE ESTADUAL DE CAMPINAS
Instituto de Geociências

DANIELA ALBINI PINHEIRO

HACKERS, POLÍTICAS E AMÉRICA LATINA: UM ESTUDO EXPLORATÓRIO

CAMPINAS
2019

DANIELA ALBINI PINHEIRO

HACKERS, POLÍTICAS E AMÉRICA LATINA: UM ESTUDO EXPLORATÓRIO

TESE APRESENTADA AO INSTITUTO DE GEOCIÊNCIAS DA UNIVERSIDADE ESTADUAL DE CAMPINAS PARA OBTENÇÃO DO TÍTULO DE DOUTORA EM POLÍTICA CIENTÍFICA E TECNOLÓGICA

ORIENTADORA: PROFA. DRA. MILENA PAVAN SERAFIM

ESTE EXEMPLAR CORRESPONDE À VERSÃO FINAL DA TESE DEFENDIDA PELA ALUNA DANIELA ALBINI PINHEIRO E ORIENTADA PELA PROFA. DRA. MILENA PAVAN SERAFIM

CAMPINAS

2019

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Geociências
Marta dos Santos - CRB 8/5892

P655h

Pinheiro, Daniela Albini, 1987-
Hackers, políticas e América Latina : um estudo exploratório / Daniela Albini Pinheiro. – Campinas, SP : [s.n.], 2019.

Orientador: Milena Pavan Serafim.
Tese (doutorado) – Universidade Estadual de Campinas, Instituto de Geociências.

1. Hackers - Aspectos políticos. 2. Tecnologia da informação - América Latina. 3. Produção Acadêmica. I. Serafim, Milena Pavan, 1981-. II. Universidade Estadual de Campinas. Instituto de Geociências. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: Hackers, politics and Latin America : an exploratory study
Palavras-chave em inglês:
Computer hackers - Political aspects
Information technologies - Latin America
Academic production
Área de concentração: Política Científica e Tecnológica
Titulação: Doutora em Política Científica e Tecnológica
Banca examinadora:
Milena Pavan Serafim [Orientador]
Marko Synesio Alves Monteiro
Leda Maria Caira Gitahy
Alcides Eduardo dos Reis Peron
Daniela Camila de Araujo
Data de defesa: 27-08-2019
Programa de Pós-Graduação: Política Científica e Tecnológica

Identificação e informações acadêmicas do(a) aluno(a)
- ORCID do autor: https://orcid.org/0000-0002-6587-1136
- Currículo Lattes do autor: http://lattes.cnpq.br/4425981870715184

UNIVERSIDADE ESTADUAL DE CAMPINAS
INSTITUTO DE GEOCIÊNCIAS

AUTORA: Daniela Albini Pinheiro

HACKERS, POLÍTICAS E AMÉRICA LATINA: UM ESTUDO EXPLORATÓRIO

ORIENTADORA: Profa. Dra. Milena Pavan Serafim

Aprovado em: 27 / 08 / 2019

EXAMINADORES:

Profa. Dra. Milena Pavan Serafim - Presidente

Prof. Dr. Marko Synesio Alves Monteiro

Profa. Dra. Leda Maria Caira Gitahy

Prof. Dr. Alcides Eduardo dos Reis Peron

Profa. Dra. Daniela Camila de Araújo

A Ata de defesa com as respectivas assinaturas dos membros, encontra-se disponível no SIGA - Sistema de Fluxo de Tese e na Secretaria de Pós-graduação do IG.

Campinas, 27 de agosto de 2019.

AGRADECIMENTOS

Agradeço primeiramente aos meus queridos pais, Marta e Carlos, pelo amor incondicional, compreensão e paciência enquanto tento encontrar meu caminho. E às vós Marias, que me acompanharam por toda minha trajetória.

Também agradeço a minha orientadora Milena Pavan Serafim pela companhia nessa longa jornada juntas e pelas palavras certeiras de conforto e encorajamento nos momentos certos.

Agradeço a todos os membros da banca – Leda Gitahy, Marko Monteiro, Alcides Peron, Daniela Araujo, Diego Vincentin, Marta Kanashiro, Nanci Stancki e Thales Novaes de Andrade – por aceitarem o convite. É um privilégio poder contar com as contribuições daqueles que me acompanharam ao longo do período de doutoramento.

Aos funcionários do Instituto de Geociências – Adriana, Cris, Max, Alexandre, Valdir e Bia. Agradeço especialmente à Val e à Gorete, tão queridas e donas dos melhores abraços.

Aos queridos amigos da Salaum – Lu, Cris, Yama, Felipe, Isa, Sarah, Rodrigo e Dam. Nosso laboratório é o melhor mundo paralelo. Agradeço por todo apoio, carinho, interrupções, conversas surreais e, principalmente, pela companhia em todos os momentos.

A todos os amigos que fiz no DPCT, meus colegas de caminhada. Em especial, agradeço por todo amor das minhas queridas Jen e Adela, que agora moram longe e deixam saudades. Agradeço também à Bia, minha companheira de aventura acadêmica desde a graduação.

Por fim, agradeço às queridas Nadia e Neide, extensão da família e sempre presentes.

E aos professores do DPCT por todo conhecimento construído.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001.

RESUMO

Este trabalho identifica a literatura acadêmica sobre experiências de hackers de computador na América Latina e analisa as políticas hackers que emergem delas. Hackers de computador, aqui, são entendidos como aqueles que constroem, trabalham e habitam tecnologias da informação, que são parte essencial de suas experiências, políticas, éticas e formas de interagir e ser no mundo. As narrativas hegemônicas sobre hackers reforçam o estereótipo do libertário, solitário e apolítico que escreve *software* e transforma tecnologias para sua satisfação pessoal. Este estereótipo está relacionado a contextos, regiões e comunidades de prática específicos. A literatura mais recente sobre hackers tem se preocupado em recuperar outras genealogias, evidenciar a multiplicidade das políticas e estudar ciclos de politização e cooptação dos hackers pelas forças do capitalismo. A partir de uma pesquisa exploratória e qualitativa, buscou-se identificar como os estudos de caso sobre hackers de computador da América Latina contribuem com o conhecimento sobre políticas hackers e, desta forma, com o campo dos estudos hackers como um todo. A partir dos passos propostos pela Revisão Sistemática de Bibliografia, realizou-se um estudo de escopo, além da busca, seleção e sistematização de publicações acadêmicas. As análises foram complementadas com as anotações realizadas durante a Escola Doutoral de Estudos Digitais na Leuphana University em 2016 e as edições de 2017 e 2018 da CryptoRave no Brasil. O estudo de escopo foi desenvolvido a partir da revisão da literatura conhecida dos estudos hackers, que trata de casos estadunidenses e europeus, e evidenciou que políticas hackers são múltiplas e assumem ora características mais liberais ora mais radicais. Também foram identificados elementos em comum nas motivações que levam hackers a se engajarem politicamente: a percepção de que as condições técnicas e legais que possibilitam a associação e existência hacker (público recursivo) estão em risco e algumas subjetividades políticas, como a valorização da astúcia, o antiautoritarismo e o comportamento extremamente social. A partir da determinação de palavras-chave e de critérios de inclusão, realizou-se a busca em diferentes repositórios de publicações acadêmicas e foram selecionadas setenta publicações, das quais foram extraídas e analisadas informações sobre meios de publicação, autores, métodos, definições e políticas hackers para a construção de um panorama deste conjunto de publicações. A partir da análise do conteúdo, foi possível concluir que as políticas hackers na América Latina são situadas, múltiplas e, ainda que também apresentem elementos comuns às motivações que levam ao engajamento político, assim como algumas semelhanças com as narrativas hegemônicas sobre ser e fazer hacker, apresentam características específicas. Essas especificidades foram encontradas quando o público recursivo foi construído também em torno de outros fatores, como pertencimento a povos tradicionais, ser mulher, ser latino-americano ou viver em um país em desenvolvimento. Ser e fazer hacker, então, acabaram incluindo outras questões do estar, agir e ser no mundo próprias desses atores. As políticas hackers, nesses casos, tomaram forma de resistência contra apropriação por culturas dominantes e invisibilização, luta por autonomia, pela possibilidade de construir tecnologias e pela inclusão digital, cuidados digitais e proteção contra violências no contexto do capitalismo informacional.

Palavras-chave: Hackers – Aspectos políticos; Tecnologia da informação – América Latina; Produção Acadêmica

ABSTRACT

This thesis identifies the academic literature on computer hackers in Latin America and analyzes the hacker politics that emerge from them. Computer hackers here are understood as those who build, work and inhabit information technologies, which are an essential part of their experiences, policies, ethics and ways of interacting and being in the world. The hegemonic hacker narratives reinforce the libertarian, lonely, and apolitical hacker stereotype that writes software and transforms technologies to their personal satisfaction. This stereotype is related to specific contexts, regions and communities of practice. The latest literature about hackers has been concerned with reclaiming other hacker genealogies, highlighting the multiplicity of their politics, and studying cycles of politicization and co-optation of these actors by the forces of capitalism. From an exploratory and qualitative research, we sought to identify how the case studies on computer hackers in Latin America contribute to the knowledge about hacker politics and, thus, to the field of hacker studies as a whole. From the steps proposed by Systematic Review of Bibliography, a scope study was carried out, as well as the search, selection and systematization of academic publications. The analyses were complemented by notes made during the Doctoral School of Digital Studies at Leuphana University in 2016 and the 2017 and 2018 editions of CryptoRave in Brazil. The scope study was developed from a review of the known literature of hacker studies, which deal with US and Eropean cases, and showed that hacker politics are multiple, and sometimes they assume liberal characteristics or radical characteristics. Common elements were also identified in the motivations that lead hackers to engage politically: the perception that the technical and legal conditions that enable hacker association and existence (recursive public) are at risk, and some political subjectivities, such as valuing craftiness, anti-authoritarianism and extremely social behavior. From the determination of keywords and inclusion criteria, we searched different repositories of academic publications and selected seventy publications, from which we extracted and analyzed information on publishing, authors, methods, definitions and hacker politics to build an overview of this set of publications. From the analysis of the content, it was possible to conclude that hacker politics in Latin America are situated, multiple and, although they also present common elements to the motivations that lead to political engagement, as well as some similarities with the hegemonic narratives about being a hacker and hacking, they have specific characteristics. These specificities were found when the recursive public was also built around other factors, such as belonging to traditional peoples, being a woman, being Latin American or living in a developing country. Being a hacker and hacking, then, ended up including other issues of being, acting, and living in the world specific to those actors. Hacker politics, in these cases, have taken the form of resistance against appropriation by dominant cultures and invisibilization, struggle for autonomy, for the possibility of building technologies and for digital inclusion, digital care and protection against violence in the context of informational capitalism.

Keywords: Computer hacker – Political aspects; Information technologies – Latin America; Academic production

LISTA DE ILUSTRAÇÕES

Figura 1 - Número de publicações por ano 81

LISTA DE QUADROS

Quadro 1 - Resumo das buscas realizadas nos repositórios de produção acadêmica 24
Quadro 2 - Número de publicações selecionadas por repositório 25
Quadro 3 - Participação como ouvinte em mesas de duas edições da CryptoRave no Brasil . 37
Quadro 4 - Número de publicações por linguagem de publicação 82
Quadro 5 - Número de publicações por país da revista/livro 82
Quadro 6 - Coautorias 84
Quadro 7 - Formação acadêmica informada pelos autores 86
Quadro 8 - Número de autores e publicações por país do vínculo institucional informado 87
Quadro 9 - Número de publicações por país do meio de publicação e país de vínculo institucional informado (resumido) 88
Quadro 10 - Número de publicações por país do meio de publicação e país de vínculo institucional informado (expandido) 89
Quadro 11 - Número de publicações com menção a apenas um campo de conhecimento 93
Quadro 12 - Número de publicações com menção a mais de um campo de conhecimento 94
Quadro 13 - Países ou região do caso explorado 95
Quadro 14 - Grandes agrupamentos de objetos de estudo 98
Quadro 15 - Palavras-chave de maior incidência no conjunto de publicações 100
Quadro 16 - Agrupamentos de objetos de estudo por perspectiva temporais de análise (DELFANTI & SÖDERBERG, 2018) 102
Quadro 17 - Parâmetros das definições de hackers por origem 105
Quadro 18 - Emergência das políticas hackers 110

LISTA DE ABREVIATURAS E SIGLAS

APC – *Association for Progressive Communications*

APPO – *Asamblea Popular de los Pueblos de Oaxaca*

BDTD – Biblioteca Digital Brasileira de Teses e Dissertações

DDoS – *Distributed Denial of Service*

DPCT – Departamento de Política Científica e Tecnológica

EFF – *Eletronic Frontier Foundation*

ESCT – Estudos Sociais da Ciência e da Tecnologia

EZLN – Exército Zapatista de Liberação Nacional

FISL – Fórum Internacional de *Software* Livre

GAPI – Grupo de Análise de Política de Inovação

GIG@ – Grupo de Pesquisa em Gênero, Tecnologias Digitais e Cultura

IBICT – Instituto Brasileiro de Informação em Ciência e Tecnologia

ICTS – Informação, Comunicação, Tecnologia e Sociedade

IRC – *Internet Relay Chat*

Labjor – Laboratório de Estudos Avançados em Jornalismo

LAVITS – Rede Latino-Americana de Estudos sobre Vigilância, Tecnologia e Sociedade

MIT – *Massachusets Institute of Technology*

NAFTA – Tratado Norte-Americano de Livre Comércio

OLPC – *One Laptop Per Child*

ONG – Organização Não Governamental

Redalyc – *Red de Revistas Científicas de América Latina y el Caribe, España y Portugal*

RSB – Revisão Sistemática de Bibliografia

SciELO – *Scientific Eletronic Library Online*

SOF – Sempreviva Organização Feminista

STEM – *Science, Technology, Engeneering and Matemathics*

UFRJ – Universidade Federal do Rio de Janeiro

UNICAMP – Universidade Estadual de Campinas

USP – Universidade de São Paulo

TI – Tecnologias da informação

SUMÁRIO

RESUMO 6
INTRODUÇÃO 12
CAPÍTULO 1 - Considerações metodológicas 20
1.1 Revisão Sistemática de Bibliografia 20
1.2 Experiências pelo campo 28
CAPÍTULO 2 - Estudos hackers: genealogias e políticas 40
2.1 Genealogias hackers 43
2.2 Políticas hackers como objeto de estudo 53
2.2.1 Características e condicionantes das políticas hackers 57
2.4 Limites das políticas hackers 69
2.5 *Hacklabs*, *hackerspaces*, política e socialização hacker 72
CAPÍTULO 3 – Panorama dos estudos de caso sobre hackers na América Latina 80
3.1 Informações sobre publicação 80
3.2 Sobre os autores e coautorias 84
3.3 Sobre o conteúdo das publicações 90
Aspectos metodológicos 90
Campos de conhecimento 92
Perspectivas sobre os estudos de caso 94
Definições 103
As políticas hackers 109
CAPÍTULO 4 – As políticas hackers segundo os estudos de caso sobre a América Latina 115
4.1 Resistências: ação coletiva, autonomia e o direito de existir 115
Movimentos populares e resistência de povos tradicionais 116
Controle, violência e o indivíduo 125
4.2 As políticas do dia-a-dia: trabalho, comunidades e gênero 133
Comunidades e o movimento de software livre 133
Outros modos de vida 139
Gênero, desigualdade, violência e cuidado 144
4.3 Transposição do ser hacker para outros meios 154
Comportamentos hackers 154
Metodologias hackers 157
4.4 Outras formas de fazer política pública, influenciar tomada de decisões ou se expressar politicamente: democracia e tecnologia 158
4.5 Violência e ilegalidade: hackers, delitos e controvérsias 165
4.6 Considerações sobre as políticas hackers e as disputas pelo ordenamento do mundo 167
CONCLUSÃO – Hackers, políticas, América Latina e a literatura dos estudos hackers 173
REFERÊNCIAS 185
ANEXO A - Referências bibliográficas do conjunto de publicações selecionadas 189
ANEXO B – Agrupamentos e categorias de análise por publicação 195

INTRODUÇÃO

O objetivo desta tese é identificar as contribuições dos estudos de caso sobre hackers de computador na América Latina para o corpo de conhecimento sobre políticas hackers e, em decorrência, para os estudos hackers como um todo. A partir de uma pesquisa exploratória e qualitativa, buscou-se identificar a literatura acadêmica sobre experiências de hackers de computador na América Latina e as políticas hackers que emergem delas.

Os estudos hackers, ou literatura sobre hackers, é um campo que agrega uma série de pesquisas e publicações interdisciplinares que descrevem e analisam aspectos éticos, morais, políticos, sociais e materiais das práticas cotidianas e espaços de socialização dos hackers. Söderberg (2013) estabelece a existência de dois momentos nos estudos hackers. As primeiras literaturas sobre hackers tiveram como objetivo caracterizar hackers, sua origem e *ethos* como forma de contextualizá-los, revelar sua existência e difundir suas práticas, de forma que funcionaram como frestas para o público espiar um universo desconhecido, exótico e contido em si mesmo. Já as literaturas mais recentes expressam, de alguma forma, a percepção de que hackers não são exógenos ao mundo, mas parte das relações cotidianas entre tecnologia e sociedade. Nesse sentido, as implicações políticas dos imaginários hackers se tornaram tema central dos textos atuais dessa literatura e tópicos relacionados porque as últimas gerações de hackers foram bem-sucedidas em disseminar seus futuros (SÖDERBERG, 2017). Além disso, a literatura mais recente sobre hackers também tem se preocupado em recuperar outras genealogias hackers, evidenciar a multiplicidade de suas políticas e estudar ciclos de politização e cooptação desses atores pelas forças do capitalismo de uma perspectiva europeia e estadunidense.

Hackers de computador, nesta tese, são entendidos como aqueles que constroem, trabalham e habitam tecnologias da informação, que são parte essencial de suas experiências, políticas, éticas e formas de interagir e ser no mundo. Da mesma forma, tecnologias da informação se referem às atividades, recursos e infraestrutura de computação voltadas para produção, armazenamento, transmissão, acesso, uso e segurança das informações. A partir deste ponto, a utilização do termo “hacker” carrega consigo esses dois conceitos. Dessa forma, a escolha por estas definições foi realizada com o propósito de conectar esta pesquisa com a literatura dos estudos hackers em relação a qual os estudos de caso sobre hackers de computador na América Latina são comparados. Os hackers que interessam aqui são aqueles que valorizam formas de liberdade, privacidade e acesso, habitam as tecnologias da

informação através da programação, da administração de sistemas ou da Internet, da criação de ferramentas de segurança ou hackeando *hardware* e incorporam uma estética em que ofício (normas, tradições e aprendizado) e artifício (práticas de modificar, quebrar e encontrar limitações tecnológicas de forma criativa) convergem (COLEMAN, 2017).

A literatura dos estudos hackers entende o termo "política" das mais diferentes formas. Nesse sentido, nenhuma das publicações consultadas definiu o conceito, mas utilizaram o termo para se referir a conjuntos de ideologias e motivações que ordenam as práticas hackers, as influências dos hackerismos para o capitalismo informacional, disputas entre hackers e outros atores e seus impactos, engajamento hacker em arenas políticas mais tradicionais (eleições, políticas públicas, protestos e manifestações, entre outros) e posicionamentos sobre as configurações e organização intra-comunidades. Apesar dessa multiplicidade, as experiências apresentadas e análises realizadas parecem indicar certo consenso de que as políticas hackers são performadas através das práticas em torno da experimentação, apropriação e construção de tecnologias da informação. Hackers, nesse sentido, comporiam um público específico, denominado recursivo, uma vez que é constituído por uma preocupação compartilhada pelas condições técnicas e legais que possibilitam sua associação e existência, no caso, desde os aspectos de técnicos de funcionamento das tecnologias da informação até questões de governança da Internet e leis de propriedade intelectual (KELTY, 2005).

As relações entre hackers, tecnologias da informação e políticas aqui adotadas refletem os pressupostos dos Estudos Sociais da Ciência e da Tecnologia (ESCT) da não-neutralidade das tecnologias e dos arranjos tecnológicos como arenas de disputa entre diferentes grupos de interesse. Nesse sentido, se políticas são entendidas como os arranjos de poder e autoridade em associações entre indivíduos, bem como as atividades que acontecem no interior desses arranjos, as tecnologias se tornam formas de ordenar o mundo (WINNER, 1980). Essa definição de política de tecnologia permite entender as políticas hackers como formas de disputar o ordenamento do mundo através do reordenamento de tecnologias da informação e suas infraestruturas. Nesse sentido, as tecnologias da informação não determinam as políticas hackers, mas são parte de sua expressão (COLEMAN, 2011).

No início da trajetória de pesquisa, enquanto explorava o que Söderberg (2017) identificou como primeiro momento dos estudos hackers, surgiu a estranheza em relação ao contraste entre as narrativas sobre hackers europeus e estadunidenses, cujas experiências são retratadas nos estudos hackers, e aquelas identificadas em publicações e discussões sobre hackers no Brasil. As narrativas hegemônicas sobre hackers reforçavam o estereótipo do

homem, branco, de classe média e com ensino superior, libertário, solitário e apolítico que escreve *software* e transforma tecnologias para sua satisfação pessoal. Porém, até então, esta pesquisa compartilhava da percepção de que hackers eram representantes de um movimento de não-aceitação da condição de caixa-preta de tecnologias e informações, envolto em subversão, liberdade e autonomia e circunvenção das imposições do Estado e das grandes corporações sobre como as tecnologias deveriam funcionar e o que deveria ser feito com seus dados. A partir das leituras e da convivência com pesquisadores que estudavam manifestações e gêneros hackers específicos – como hacktivismo e as intersecções entre hackers, feminismo e movimentos sociais no contexto brasileiro, movimento de *software* livre e comunidades e desenvolvedores – outras percepções e dimensões analíticas foram sendo notadas.

Em uma tentativa de entender as diferenças entre percepções sobre hackers, o caminho tomado foi explorar a literatura que Söderberg (2017) determina como o segundo momento dos estudos hackers, que se preocupa em trazer outras genealogias e aspectos políticos dos hackers e, de certa forma, tenta abranger pluralidades e combater as narrativas hegemônicas sobre suas origens e práticas. Essa literatura, que é conformada por estudos exploratórios que identificam, descrevem, exemplificam e comparam experiências situadas nos contextos estadunidense e europeu, busca propor teorias sobre hackers como cultura e movimento social e político, mas ainda não captura as especificidades das práticas e políticas hackers de outros contextos geopolíticos, como o caso da América Latina.

A proposta de realização desta pesquisa partiu do pressuposto que experiências e manifestações hackers são situadas e da percepção de que outras discussões sobre hackers e políticas já estavam sendo desenvolvidas na América Latina. Esta pesquisa, portanto, explora o conhecimento existente sobre hackers de computador na América Latina, buscando olhar como esses hackers disputam o ordenamento do mundo a partir do reordenamento das tecnologias da informação e suas infraestruturas e considerando as especificidades dessas políticas hackers.

Assim sendo, as questões que nortearam a realização desta pesquisa foram: i) quais são as características das políticas hackers na América Latina?; ii) em comparação com outros contextos, quais as especificidades das políticas hackers na América Latina?, e iii) como os pesquisadores estão olhando para essa temática?

A terceira pergunta é particularmente central para o objetivo geral da pesquisa. O interesse aqui é identificar as discussões realizadas e suas contribuições para o corpo de conhecimento sobre políticas hackers e os estudos hackers como um todo.

Trajetória de pesquisa

A definição das políticas hackers como objeto de pesquisa aconteceu já em fase avançada do período do doutoramento e foi resultado de uma série de explorações sobre hackerismos. No início da trajetória, o interesse repousava em hackers em decorrência das pesquisas que foram realizadas para disciplinas do programa de pós-graduação sobre hackers do Pirate Bay e todas as brincadeiras, controles e invasões policiais que sofreram em nome da livre circulação de conteúdo na Internet. Foi nesse momento que tomei conhecimento da existência de *hackerspaces* através, também, da pesquisa de outros colegas de programa.

Um dos aspectos mais interessantes dos estudos de caso sobre *hackerspaces* eram as reinterpretações dos diferentes autores do conceito sobre esses espaços em que pessoas com diferentes interesses e motivações se encontram para compartilhar conhecimentos, ferramentas, recursos e práticas em lugares fixos ou não e estão ligados a uma cultura mais ampla dos laboratórios experimentais. Os *hackerspaces* eram explorados desde as perspectivas mais emancipatórias – como espaços de resistência através da apropriação, transformação e interferência em tecnologias que pareciam se configurar como crítica e potencialmente alternativa às dinâmicas sociotécnicas existentes, como a lógica de mercado, o consumismo exacerbado e a obsolescência programada – até aquelas que os avaliavam como espaços de trabalho qualificado gratuito cooptado pelas forças do capitalismo.

A tese começou a tomar forma a partir do objetivo de entender como tem se configurado o fenômeno dos *hackerspaces* no Brasil. Grande parte da literatura a qual tive acesso sobre o tema tratava de casos estadunidenses ou europeus, de modo que o conhecimento sobre sua história e genealogia dependia dessas fontes, mesmo para o caso do Brasil. As exceções foram alguns estudos de caso parte de dissertações sobre *hackerspaces* brasileiros, que estavam focados principalmente nas descrições dos ambientes, atividades e dinâmicas dos espaços. A necessidade de começar a identificar e construir essa narrativa partiu da percepção de que esse fenômeno é situado histórica e geograficamente, de modo que as narrativas europeias e estadunidenses parecem se configurar como influência em termos de organização, práticas e políticas, mas não devem ser adotadas como nossas.

A exploração realizada sobre os *hackerspaces* coincidiu com minha participação na Escola Doutoral de Estudos Digitais em agosto de 2016 na Leuphana University. A Escola contou com palestras e aulas de diversos pesquisadores dos estudos sobre hackers, como Gabriella Coleman, Christopher Kelty e Maxigas, além de hackers e outros profissionais relacionados com segurança da informação, privacidade e criptografia. Nessa escola, foi possível conhecer parte da bibliografia dos estudos hackers e seus desenvolvimentos mais

recentes, além de identificar a percepção dos pesquisadores sobre as discussões acadêmicas e não acadêmicas sobre hackers nos EUA, Canadá, Alemanha e outros países europeus.

Alguns dos temas propostos para a escola doutoral que tocavam as leituras que já havia realizado sobre hackers e *hackerspaces* – como igualdade e elitismo no hacking e lógicas de perturbação e tratavam de pontos de representatividade, desigualdade e alternativas – foram explorados nas palestras dos professores convidados. Porém, os temas de pesquisa de outros alunos, assim como as palestras dos especialistas e hackers e as conversas informais ficavam restritas a questões sobre vigilância e segurança da informação. Os temas de gênero, movimentos sociais e hacking dificilmente eram mencionados, o que causou estranheza, uma vez que meu primeiro contato com hackers aconteceu por meio desses assuntos.

Em termos do andamento da pesquisa, o passo seguinte foi tentar realizar trabalho de campo em *hackerspaces* brasileiros. Foi nesse ponto da trajetória que surgiu o interesse em participar da CryptoRave na tentativa de conseguir algum espaço de inserção no *hackerspace* feminista MariaLab. A CryptoRave é um evento aberto e gratuito, pensado e organizado como um espaço para disseminar conceitos, cultura e ferramentas de privacidade, segurança, criptografia, hacking e liberdade na Internet por 24 horas, que conta com diversos espaços de discussão e oferece palestras e oficinas, instalações em massa de sistemas operacionais e *softwares* livres (*installfests*), entre outras atividades. Além disso, se configura como um espaço interessante para conhecer as discussões de interesse de quem, de alguma forma, está envolvido com ou interessado nos desdobramentos do movimento hacker. A MariaLab havia proposto atividades para a edição de 2017 e pareceu uma oportunidade interessante para fazer um primeiro contato.

Ainda que as tentativas de inserção na MariaLab tenham sido malsucedidas – que somados os custos de transporte e estadia em São Paulo e os prazos para realização do doutorado levaram à escolha em não realizar trabalho de campo –, essas experiências e as mesas assistidas na CryptoRave foram importantes para construção do meu entendimento sobre a importância das discussões sobre privacidade e segurança de dados e sobre a urgência em discutir essas temáticas no contexto brasileiro.

Somada às experiências na Escola Doutoral de Estudos Digitais, minha participação nas edições de 2017 e 2018 da CryptoRave transformou as percepções de que as experiências e manifestações hackers são situadas e de que hackers e políticas são discutidos na América Latina em inquietações e objetos de pesquisa. Além da existência de um consenso na literatura mais recente sobre hacker ser um conceito em disputa e transformação, de forma que as definições são constantemente exploradas, a escolha em focar nas políticas também foi

baseada outros dois fatores. Primeiro, porque foi um dos principais temas abordados na Escola Doutoral em Estudos Digitais e faz parte da literatura mais recente dos estudos hackers. Segundo, porque ainda que políticas hackers sejam discutidas na América Latina, não pareceu haver nenhum estudo que as agrupasse para análise.

Metodologia

Para responder as perguntas desta pesquisa – que se constitui como um estudo exploratório e utiliza abordagem qualitativa – e alcançar o objetivo geral proposto, foram utilizadas três formas de coleta de dados: revisão de literatura, consulta a repositórios de produção acadêmica e observação participante em eventos acadêmicos e não acadêmicos.

Em relação as duas primeiras formas de coleta de dados, as etapas propostas pela Revisão Sistemática de Bibliografia (RSB) foram consideradas adequadas ao objetivo de realizar uma primeira identificação e sistematização de publicações que explorassem estudos de caso sobre hackers de computador na América Latina e possibilitassem o diálogo com a literatura já explorada sobre o tema. A RSB se configura como um método para descobrir, mapear, examinar e sintetizar o corpo de conhecimento existente sobre um objeto ou tema e propõe uma série de passos que vão da identificação das principais discussões sobre o objeto a partir da literatura já conhecida, passam pela busca de publicações nos repositórios de trabalhos acadêmicos escolhidos e seleção das publicações e terminam na sistematização e análise do conteúdo.

A revisão de literatura foi realizada em dois momentos no contexto da RSB: na realização do estudo de escopo e na sistematização do conteúdo dos estudos de caso sobre hackers de computador na América Latina, com foco nas políticas hackers, que conformam o segundo e quarto capítulos, respectivamente.

O estudo de escopo se configura como uma forma preliminar de avaliar o montante de literatura existente sobre o objeto de pesquisa. Para sua construção foi realizada a revisão da literatura dos estudos hackers já conhecida, buscando abranger os dois momentos identificados por Söderberg (2017). O principal objetivo, porém, foi apresentar as discussões mais recentes sobre políticas hackers, em especial, as desenvolvidas por Söderberg (2013), Coleman (2017), Maxigas (2017) e Delfanti & Söderberg (2018). Já para o quarto capítulo, a revisão de literatura foi construída como forma de sistematização do conteúdo das publicações selecionadas através da RSB, com o objetivo de evidenciar as perspectivas dos

autores sobre hackers e suas políticas e apontar os aspectos que determinaram como relevantes em suas pesquisas.

Por fim, a observação participante foi realizada em dois eventos. Primeiro, na II Escola Doutoral de Estudos Digital, que aconteceu de 28 de agosto a 2 de setembro de 2016, organizada pela Leuphana University, em Luneburgo, Alemanha. Segundo, nas edições de 2017 e 2018 da CryptoRave. A edição de 2017 aconteceu na Casa do Povo, na cidade de São Paulo (Brasil), nos dias 5 e 6 de maio. Já a edição de 2018 foi realizada na Cinemateca Brasileira, também em São Paulo, nos dias 4 e 5 de maio.

Como apontado anteriormente, ambos os eventos foram importantes na construção da minha percepção sobre o tema e na identificação de discussões relevantes. Ainda que não seja o objetivo dessa tese analisar os acontecimentos nesses eventos, as experiências na Escola Doutoral de Estudos Digitais e nas duas edições da CryptoRave exemplificam – ou expandem – algumas análises realizadas pelos autores sobre os hackers na América Latina. Dessa forma, as anotações realizadas foram comparadas e incluídas, quando pertinente, junto da literatura utilizada para a construção do estudo de escopo no segundo capítulo e da sistematização das publicações selecionadas através da RSB no quarto capítulo.

Estrutura da tese

A tese está estruturada em quatro capítulos, além desta introdução e da conclusão, que condizem com os passos propostos pela Revisão Sistemática de Bibliografia.

No primeiro capítulo são apresentadas as considerações metodológicas. Num primeiro momento, o processo de busca, seleção e sistematização de estudos de caso sobre hackers na América Latina é desdobrado e as escolhas de pesquisa são justificadas em um esforço de tornar a coleta de dados transparente. Num segundo momento, são apresentadas as experiências na Escola Doutoral de Estudos Digitais, nas duas edições da CryptoRave e na tentativa de inserção em um *hackerspace* feminista.

O segundo capítulo se configura como o estudo de escopo. Nele, são apresentadas as principais discussões desenvolvidas pela literatura conhecida considerando os dois momentos dos estudos hackers identificados por Söderberg (2017). A partir da revisão de literatura, foi possível evidenciar que as definições de hackers são múltiplas e identificar a origem do estereótipo do hacker libertário, solitário e apolítico, além de algumas de suas implicações para as políticas hackers. Também foi possível evidenciar que a literatura mais recente sobre hackers se preocupa em descrever e evidenciar sua multiplicidade como

fenômeno, combatendo o estereótipo mencionado e suas implicações, mas sem negá-lo ou diminuir sua importância em contextos e espaços hackers específicos. As discussões sobre políticas hackers fazem parte desse movimento. Os estudos hackers têm buscado identificar os condicionantes e características das políticas hackers recuperando informações históricas e analisando os fenômenos mais recentes para a proposição de teorias sobre engajamento político.

O terceiro e quarto capítulos conformam a síntese da literatura encontrada proposta pela RSB. O terceiro capítulo é construído como um panorama dos estudos de caso sobre hackers na América Latina. As publicações selecionadas, neste capítulo, foram tratadas como conjunto. São apresentadas informações sobre os meios de publicação, autores e conteúdo, este último com objetivo de caracterizar os métodos e campos de conhecimento utilizados nos estudos, assim como construir categorias de análise sobre objeto, definições para hackers e políticas hackers. O quarto capítulo parte das categorias de análise criadas para as políticas hackers e, através da revisão bibliográfica, apresenta as principais características – assim como elementos relevantes identificados pelos autores – das políticas dos hackers de computador na América Latina.

Por fim, a conclusão busca apresentar as principais contribuições dos estudos de caso sobre hackers de computador na América Latina para o conhecimento em políticas hackers e para os estudos hackers como um todo a partir dos achados do quarto capítulo em comparação com as discussões do estudo de escopo. Considerando as políticas, foi possível identificar semelhanças com aquelas descritas no segundo capítulo principalmente em relação às dinâmicas internas às comunidades de desenvolvedores e no hacking cívico, cujas características parecem ser comuns a essas formas específicas de hackerismo, independente do contexto. Especificidades latino-americanas foram encontradas quando as análises sobre políticas hackers se entrelaçaram com movimentos sociais, questões de gênero, dependência tecnológica e falta de acesso às tecnologias que caracterizariam o contexto latino-americano.

CAPÍTULO 1 - Considerações metodológicas

O objetivo deste capítulo é apontar e justificar as escolhas metodológicas realizadas ao longo desta pesquisa. Primeiro, é apresentado como decorreu o processo de busca, seleção e sistematização de estudos de caso sobre hackers na América Latina. Para esse processo, as etapas propostas pela Revisão Sistemática de Bibliografia foram consideradas adequadas e aplicáveis ao objetivo de realizar uma primeira identificação e sistematização de publicações que trouxessem evidências das políticas hackers na América Latina e possibilitassem o diálogo com a literatura já explorada sobre o tema. Segundo, são introduzidas as experiências nos eventos: a participação da Escola Doutoral de Estudos Digitais na Leuphana University, a tentativa de inserção em um *hackerspace* feminista e as discussões nas edições da CryptoRave.

Este capítulo se configura, também, como um esforço para tornar a coleta de informações realizada transparente.

1.1 Revisão Sistemática de Bibliografia

A revisão de bibliografia, como um todo, se configura como um método para descobrir, mapear, examinar e discutir o corpo do conhecimento existente sobre um objeto ou tema específico com o objetivo de reunir evidências para embasar análises, práticas e políticas em qualquer disciplina (TRANFIELD, DENYER & SMART, 2003). De acordo com Levy & Ellis (2009), no contexto da pesquisa acadêmica, a revisão de literatura auxilia o pesquisador não só a determinar uma pergunta de pesquisa que desenvolva ainda mais o corpo de conhecimento existente[1], mas a justificar a abordagem escolhida, a seleção dos métodos e a importância do estudo que será realizado. Entendida dessa forma, a revisão de literatura torna-se um primeiro passo essencial para qualquer pesquisa.

Nesta pesquisa, utilizo a definição de Levy & Ellis (2009)[2] para o processo de revisão de literatura:

[1] Levy & Ellis (2009) entendem corpo de conhecimento como o conhecimento apoiado em pesquisas cumulativas, feitas com base nos achados de pesquisa umas das outras (LEVY & ELLIS, 2009, p. 182).

[2] Levy & Ellis (2009) se preocupam em explicar detalhadamente os passos de uma Revisão Sistemática de Bibliografia para qualquer disciplina e, depois, com foco em pesquisas em sistemas de informação. Os autores apresentam alguns conceitos interessantes sobre pesquisa com método bola de neve, pesquisa bibliográfica e de produção acadêmica para trás e para frente, entre outros.

> *"[...]sequential steps to collect, know, comprehend, apply, analyze, synthesize, and evaluate quality*[3] *in literature in order to provide a firm foundation to a topic and research method. Moreover, the output of the literature review process should demonstrate that the proposed research contributes something new to the overall body of knowledge."* (LEVY & ELLIS, 2009, p. 182)

Especificamente, a RSB foi desenvolvida como ferramenta em campos com práticas baseadas em evidências, como a área da saúde (TRANFIELD, DENYER & SMART, 2003[4]), com o objetivo de apresentar uma síntese das evidências de resultados de intervenções ou testes clínicos (SAMPAIO & MANCINI, 2007). Nesse contexto, segundo Sampaio & Mancini (2007), as revisões sistemáticas permitiram agrupar informações de estudos diferentes sobre o mesmo método, intervenção ou terapia e tornar os resultados conflitantes ou corroborantes analisáveis entre si, indicando melhores práticas e direcionando pesquisadores e profissionais para outras investigações[5]. Os artigos de Tranfield, Denyer & Smart (2003), Sampaio & Mancini (2007) e Levy & Ellis (2009) propõem passos para realização de uma RSB em disciplinas além daquelas da área da saúde e deram suporte aos passos realizados ao longo dessa pesquisa.

Em termos de procedimento, a RSB difere da revisão bibliográfica tradicional (denominada narrativa) porque adota um processo científico transparente e replicável que procura reduzir vieses e erros de pesquisa através da busca de estudos e da análise de suas decisões, procedimentos e resultados de pesquisa (TRANFIELD, DENYER & SMART, 2003).

De forma geral, são três os principais passos de uma RSB propostos pelos autores:

1) Planejamento: realização de um estudo de escopo com o objetivo de avaliar o conjunto da literatura existente sobre o objeto escolhido e considerar as diferentes disciplinas e abordagens nas quais é explorado;
2) Condução: série de procedimentos que culminam na realização das buscas e na seleção dos resultados encontrados, e;
3) Síntese: leitura, extração de informações e sistematização dos estudos encontrados, análise dos resultados e escrita do relatório final.

---

[3] Por qualidade, de acordo com Levy & Ellis (2009, p. 182), entende-se abrangência e profundidade apropriadas, consistência, rigor, clareza e análise e síntese efetivas.

[4] Tranfield, Denyer & Smart (2003) escrevem sobre a história da abordagem baseada em evidência, que começa na área da saúde e se espalha para outras disciplinas, e sobre a importância da Revisão Sistemática de Bibliografia para o desenvolvimento de uma ciência baseada em evidência, além de propor uma série de passos para se realizar uma RSB com rigor.

[5] Um dos procedimentos associados à RSB de uso comum é a meta-análise, que oferece um método estatístico para sintetizar achados de pesquisa com o objetivo de transformar em comparáveis os dados e resultados de estudos diferentes (TRANFIELD, DENYER & SMART, 2003; SAMPAIO & MANCINI, 2007).

Em relação ao planejamento deste trabalho, a RSB foi instrumental para a busca e seleção de produção acadêmica porque seus passos garantem que, dentro das escolhas de pesquisa, a busca seja extensiva. Ao mesmo tempo, a realização da RSB também auxilia no estabelecimento de uma estrutura argumentativa, que começa com o estudo da literatura mais geral conhecida pelo pesquisador, parte para a busca de outros conhecimentos mais específicos e interessantes ao objeto de pesquisa e se encerra com a análise do conteúdo encontrado. Nesse sentido, o segundo capítulo se configura como o estudo de escopo e foi construído com base nas leituras realizadas ao longo da trajetória de pesquisa. Já o terceiro e quarto capítulos são resultado das buscas realizadas utilizando a RSB e correspondem à sistematização, leitura e análise dos artigos e capítulos de livro selecionados.

A condução das buscas foi realizada respeitando os passos propostos por Tranfield, Denyer & Smart (2003) para definir os seguintes elementos: pergunta de pesquisa, termos de busca, critérios de inclusão e exclusão, repositórios de produção acadêmica e limite das buscas.

A definição de uma pergunta de pesquisa deve ser a primeira etapa da RSB pois é dela que deriva outras escolhas de pesquisa, como população ou amostra, palavras-chave e termos de busca, estratégias de pesquisa e critérios de inclusão e exclusão dos estudos (SAMPAIO & MANCINI, 2007). No caso de uma pesquisa qualitativa mais exploratória em que muitos dos possíveis caminhos de pesquisa são descobertos ao longo da RSB, a pergunta de pesquisa pode ser substituída por uma discussão conceitual do problema e de sua importância e o protocolo do processo de busca, desenvolvimento e escrita, ao invés de determinado a priori, pode ser configurado como um relatório detalhado dos passos e decisões tomadas ao longo da RSB (TRANFIELD, DENYER & SMART, 2003).

Em relação à pesquisa aqui apresentada, houve mudança na pergunta para condução da RSB durante o exame de qualificação. Num primeiro momento, a pergunta estava voltada ao país de publicação dos estudos e à nacionalidade dos pesquisadores, pois o interesse era encontrar a produção latino-americana sobre hackers. Com a realização das buscas na Redalyc e SciELO e sistematização dos estudos encontrados, foi possível classificá-los em dois grupos: estudos teóricos e estudos de caso. No primeiro, os estudos tinham como objetivo discutir ou analisar literatura já existente sobre hackers, principalmente em relação à ética e trabalho hackers. No segundo, o foco estava em apresentar e analisar manifestações hackers na América Latina, como grupos, espaços, atividades, práticas ou eventos ligados aos hackers. Como este segundo grupo de estudos pareceu ser capaz de contribuir de forma mais interessante à discussão sobre políticas hackers, a pergunta para condução da RSB se voltou

para a identificação de manifestações hackers latino-americanas, independente da nacionalidade dos pesquisadores. De fato, a mudança na pergunta levou a alterações nos termos de busca, nos critérios de inclusão e exclusão e repositórios de produção acadêmica selecionados.

O principal parâmetro para a escolha dos termos de busca foi a literatura dos estudos hackers, a partir da qual os estudos de caso selecionados seriam discutidos e potencialmente contribuiriam com o corpo de conhecimento. Dessa forma, nas buscas, o termo "hacker*" (a própria palavra e suas variações) foi acompanhado "América Latina" e "computador". O acréscimo deste último termo buscou conectar hackers ao conjunto de materialidades e práticas que eram de interesse da pesquisa – o das tecnologias da informação – como apontado na introdução.

Em testes de busca excluindo o termo "computador", notou-se um aumento de resultados, mas principalmente relacionados a referências bibliográficas de autores de sobrenome Hacker ou Hacking, uma vez que as buscas foram realizadas para todos os campos disponíveis (autor, título, resumo, conteúdo, palavras-chave etc.).

Os três termos de busca foram traduzidos para inglês e espanhol, quando possível e necessário, e pesquisados nos seguintes repositórios de produção acadêmica: Google Acadêmico, JSTOR, *Web of Science*, *Directory of Open Access Journals* (DOAJ), a *Red de Revistas Científicas de América Latina y el Caribe, España y Portugal* (Redalyc) e *Scientific Eletronic Library Online* (SciELO) e SCOPUS. A utilização de diferentes repositórios para as buscas teve como objetivo ampliar o número de resultados encontrados e tentar evitar vieses em relação ao tipo de acesso e país de publicação[6].

Os termos de busca também refletiram os critérios de inclusão para seleção de estudos. Como o interesse eram as manifestações hackers latino-americanas, os estudos selecionados atenderam necessariamente a dois critérios de inclusão: i) ser um estudo de caso sobre grupos, espaços, atividades, práticas ou eventos ligados aos hackers de computador e ii)

[6] Em termos de tipo de produção acadêmica, artigos foram os mais encontrados, pois são o cerne dos repositórios pesquisados. Quando o foco da pesquisa ainda era os pesquisadores latino-americanos, foi realizada uma busca extensiva por teses e dissertações sobre hackers por entender que parte do estado-da-arte da pesquisa acadêmica é encontrado nessas formas de publicação. Primeiro, foram procuradas as teses e dissertações brasileiras através da Biblioteca Digital Brasileira de Teses e Dissertações do Instituto Brasileiro de Informação em Ciência e Tecnologia (BDTD/IBICT), que agrega teses e dissertações de 109 instituições de ensino superior. Como outros países da América Latina não possuem base semelhante e pesquisar os repositórios de teses de dissertações de cada instituição um a um demandaria tempo além daquele disponível para cumprimento dos primeiros prazos dessa pesquisa, escolhi deixar as teses e dissertações, inclusive as brasileiras já catalogadas, para um outro momento. Com foco em estudos de caso sobre hackers da América Latina, o volume de teses e dissertações nos resultados do Google Acadêmico foi ínfimo e a escolha foi por não os incluir.

os grupos, espaços, atividades, práticas ou eventos estarem geograficamente localizados na América Latina.

Utilizo a definição de Selltiz et al. (1975) para estudos de caso, que os compreendem como o estudo intensivo de exemplos selecionados de um fenômeno de interesse. Nesse sentido e com base nos agrupamentos sugeridos pelos autores, foram selecionados estudos cujos objetivos de pesquisa envolveram de alguma forma: i) familiarização ou nova compreensão de um fenômeno, ii) apresentação precisa de características de uma situação, grupo ou indivíduo e iii) verificação da frequência com que algo ocorre ou se relaciona com alguma outra coisa.

O limite para as buscas em cada repositório foi delimitado ou pelo esgotamento dos resultados ou, no caso de um número muito grande de resultados, quando estudos novos ou relevantes se tornaram escassos e muito espaçados. O quadro abaixo resume as buscas realizadas:

Quadro 1 - Resumo das buscas realizadas nos repositórios de produção acadêmica

Base	**Língua**	**Termos de busca (todos os termos)**	**Resultados**	**Resultados consultados**
Google Acadêmico	Inglês	"*computer hacker*" "*Latin America*"	24.700	500
	Português	"hacker*" "computador" "América Latina"	5.770	500
	Espanhol	"hacker*" "*computadora*" "América Latina"	3.060	500
JSTOR	Inglês	"*computer hacker*" "*Latin America*"	845	220
Directory of Open Access Journals (DOAJ)	Espanhol Inglês Português	"hacker*"	361	361
SCOPUS	Inglês	"hacker*" "*Latin America*"	2.179	200
Web of Science	Inglês	"hacker*" "*Latin America*"	4	4
Redalyc e SciELO	Espanhol Inglês Português	"hacker*"	466	466
Total			**37.385**	**2.751**

Fonte: elaboração própria com base das buscas realizadas nos repositórios de produção acadêmica.

No total, setenta estudos atenderam os critérios de inclusão e foram selecionados para análise, sendo que quarenta e três deles foram encontrados em apenas um dos repositórios consultados e vinte e sete em mais de um deles. O quadro abaixo resume essas informações:

Quadro 2 - Número de publicações selecionadas por repositório

Repositório	**Número de publicações**
Google Acadêmico	31
JSTOR	6
Directory of Open Access Journals (DOAJ)	5
SCOPUS	0
Web of Science	1
Redalyc + SciELO	14
Google Acadêmico + JSTOR	4
Google Acadêmico + DOAJ	1
Google Acadêmico + Redalyc + SciELO	5
JSTOR + Redalyc + SciELO	1
Google Acadêmico + DOAJ + Redalyc + SciELO	2
Total de artigos incluídos	**70**

Fonte: elaboração própria com base das buscas realizadas nos repositórios de produção acadêmica.

A síntese das buscas foi iniciada com a sistematização de informações retiradas dos estudos selecionados em um quadro com o objetivo de criar categorias e agrupamentos para análise.

O quadro foi construído com as seguintes informações:

1) Repositórios nos quais o estudo foi encontrado;
2) Sobre o estudo:
    a. País de publicação;
    b. Ano de publicação;
    c. Tipo de publicação: artigo ou capítulo;
    d. Nome do periódico ou livro;
    e. Título;
    f. Palavras-chave, e;
    g. Língua de publicação.
3) Sobre os autores:
    a. Nome;
    b. Gênero;

c. Formação acadêmica;
d. País de vínculo institucional, e;
e. Grupo/projeto de pesquisa vinculado.

4) Sobre o conteúdo:
   a. Objeto de pesquisa;
   b. Localização do fenômeno/grupo/evento;
   c. Tipo de estudo;
   d. Forma de obtenção de dados para a análise;
   e. Campo/abordagem;
   f. Referências à literatura sobre hackers;
   g. Definições de hacker/hackerismo identificadas, e;
   h. Políticas hackers identificadas.

Sobre o conteúdo dos estudos, alguns comentários são necessários. Em primeiro lugar, a identificação do tipo de estudo foi realizada tendo como parâmetro as proposições de Selltiz et al. (1975) para classificação de estudos em exploratórios ou descritivos. Retomando os agrupamentos de objetivos de pesquisa mencionados anteriormente, os autores denominam como estudos exploratórios aqueles que buscam se familiarizar ou conseguir nova compreensão de um fenômeno e como descritivos aqueles com o objetivo ou de apresentar precisamente características de uma situação, grupo ou indivíduo ou verificar a frequência com que algo ocorre ou se relaciona com alguma outra coisa.

De acordo com Selltiz et al. (1975), estudos exploratórios têm várias funções: formular problemas de pesquisa mais exatos, auxiliar na criação de hipóteses, aumentar o conhecimento sobre situação ou fenômeno a ser explorado em outras pesquisas, esclarecer conceitos, obter informações sobre melhores práticas de pesquisa em relação a um objeto em particular, entre outros. Esse tipo de estudo é especialmente recomendado quando o conhecimento sobre um problema é muito reduzido.

Em termos de método, estudos exploratórios podem incluir:

- Exame da literatura: resenha de estudos realizados por outros autores sobre um problema de pesquisa;
- Estudo da experiência: obtenção e sintetização de experiências através da seleção de pessoas e realização de entrevistas para compreensão de relações entre variáveis e;
- Análise de exemplos que estimulam a compreensão.

Neste último caso, Selltiz et al. (1975) sugerem como método examinar registros existentes e realizar entrevistas não-estruturadas e observação participante: quando não existem hipóteses formuladas anteriormente pela literatura existente ou por experiências, cabe ao pesquisador se orientar pelas características do objeto estudado, buscando constantemente reformular e reorientar a pesquisa a partir das novas informações obtidas do indivíduo, grupo, comunidade, situação, fenômeno etc.

Já os estudos descritivos são realizados quando há um grande volume de conhecimento anterior à pesquisa sobre o problema. Esse tipo de estudo pressupõe que o objetivo de pesquisa envolve obter informações completas e exatas e que o pesquisador seja capaz de definir com exatidão tanto o objeto que deseja medir quanto os métodos necessários para obter as informações. Portanto, ao contrário dos estudos exploratórios que permitem ao pesquisador flexibilizar os métodos ao longo do processo, no caso dos descritivos é necessário planejá-los cuidadosamente antes da realização da pesquisa (SELLTIZ et al., 1975). Como os estudos descritivos envolvem informações completas e exatas, os passos sugeridos por Selltiz et al. (1975) passam pela definição da pergunta de pesquisa, planejamento do método de coleta de dados, escolha da amostra, execução da coleta e análise de resultados através da codificação e tabulação dos dados e da realização de cálculos estatísticos.

Continuando com os comentários sobre os itens criados no quadro para sistematização dos estudos selecionados, em segundo lugar, foi extraído dos estudos a forma de obtenção de dados para a análise, com o objetivo de identificar se o pesquisador trabalhou com dados primários ou secundários e quais as formas de obtenção: entrevistas estruturadas, semiestruturadas ou não estruturadas, etnografia, observação participante, revisão de bibliografia etc.

Em terceiro lugar, o item campo/abordagem buscou identificar através das discussões realizadas e das referências bibliográficas com qual campo ou abordagem do conhecimento o estudo buscou conversar ou contribuir. Para os estudos multidisciplinares e interdisciplinares foram identificados e incluídos mais de um campo/abordagem.

Também com base nas referências bibliográficas, em quinto lugar, foi criado um item para identificar se o estudo selecionado utilizou outros autores que estudam hackers.

Por fim, foram criados dois itens especificamente sobre hackers e hackerismos, cujas informações foram sistematizadas em categorias para análise do conjunto de estudos selecionados. O primeiro deles para coletar as definições de hacker/hackerismos utilizadas pelos estudos, com objetivo de identificar se os autores usam como base para suas definições a literatura já existente ou partem suas definições dos casos que pesquisam. O segundo para

identificar quais são as políticas hackers dos indivíduos e grupos ou manifestadas em eventos e comunidades.

Levy & Ellis (2009) apontam que, durante a realização da RSB, o único pré-requisito para um estudo ser encontrado é sua disponibilidade para o público. De fato, não houve problemas de acesso aos estudos porque realizei as buscas nos diferentes repositórios diretamente de computadores conectados à rede da Unicamp ou por acesso remoto seguro, o que garantiu acesso aberto aos periódicos assinados pela universidade.

Os itens do quadro de sistematização com informações mais escassas foram referentes aos autores, uma vez que não são todos os periódicos que exigem dos autores descrições sobre instituição de vínculo e formação acadêmica. O objetivo com a coleta dessas informações era analisar os autores no momento da publicação do estudo como forma de registro de um momento específico da trajetória acadêmica em que hackers e hackerismos foram objeto de pesquisa. Dessa forma, buscar informações mais completas e precisas sobre os autores além daquelas fornecidas pelos estudos, muitas vezes anos após a publicação, não traria as informações de interesse.

Ainda assim, numa primeira tentativa, foi decidido procurar informações sobre cada autor separadamente utilizando a busca do Google e Google Acadêmico. Os resultados foram mistos. Enquanto alguns dos autores já eram mais reconhecidos e possuíam páginas próprias ou de redes acadêmicas, para a maioria deles não havia como garantir que as informações encontradas eram legítimas. De modo geral, as fontes encontradas eram imprecisas e pouco confiáveis. Além disso, como os dados sobre trajetória e produção acadêmica dos pesquisadores brasileiros, devido à existência da Plataforma Lattes e sua atualização obrigatória, são mais facilmente obtidos em relação aos dos outros pesquisadores que nem sempre contam com ferramenta semelhante, foi decidido se ater às informações extraídas apenas dos estudos, e não de fontes externas, e entender a escassez de informações sobre autores nos artigos encontrados como um achado de pesquisa.

1.2 Experiências pelo campo

Neste item, será apresentado rapidamente o processo de inserção no campo, parte da trajetória de pesquisa, através da descrição e contextualização desses eventos específicos. Trata-se especificamente da Escola Doutoral de Estudos Digitais de 2016, das tentativas de inserção em um *hackerspace* feminista e das edições de 2017 e 2018 da CryptoRave.

As experiências e tentativas de inserção foram essenciais para a definição do objeto de estudo e para construir a percepção de que as políticas hackers na América Latina têm especificidades em relação àquelas discutidas na literatura. As anotações realizadas nesses eventos foram comparadas e incluídas junto da literatura utilizada para a construção do estudo de escopo e dos resultados da RSB quando pertinente.

Escola Doutoral de Estudos Digitais

A oportunidade de participar da II Escola Doutoral em Estudos Digitais (Hackademia) na Universidade da Leuphana em Luneburgo na Alemanha veio por um e-mail enviado para a lista de alunos do Departamento de Política Científica e Tecnológica (DPCT). A seleção foi realizada a partir da análise de uma carta de interesse sobre as potenciais contribuições da Escola para a pesquisa acadêmica do aluno e do aluno para as discussões que seriam realizadas.

Logo antes da viagem, recebemos um documento com todos os palestrantes e alunos de doutorado que participariam. A maioria deles era norte-americano e europeu, exceto por três alunos (um colombiano, um mexicano que estudava na Inglaterra, e eu, uma brasileira) e uma palestrante (programadora indiana). Todos os alunos ali presentes estudavam algum aspecto de hacking e intersecções com saúde, gestão pública, política, música, indústria, segurança a partir de uma variedade de métodos e marcos-teóricos em Humanidades.

No documento também foram apresentados os principais temas de discussão: regimes de propriedade intelectual (*software* livre, *software* proprietário, pirataria etc.), controle e vigilância, centralização de poder, igualdade versus elitismo no hacking e lógicas de perturbação (a perturbação do Vale do Silício versus a perturbação do "vamos destruir tudo"). Os principais palestrantes foram Maxigas, Gabriella Coleman, Christopher Kelty, Adam Fish e Goetz Bachmann, que apresentaram os desenvolvimentos mais recentes de suas pesquisas e artigos que estavam para ser publicados[7].

O primeiro encontro aconteceu no domingo no escritório do grupo de pesquisa responsável pela organização da escola doutoral, o *Digital Cultures Research Lab*, enquanto as outras atividades ocorreram no campus central da Leuphana University.

[7] Os artigos explorados no estudo de escopo de Coleman (2017) e Maxigas (2017) foram apresentados nas palestras da Escola Doutoral de Estudos Digitais.

As atividades da Escola Doutoral ocorreram no domingo à tarde e de segunda a sexta das 9hs às 20hs. O dia era dividido em cinco atividades, além do almoço: café/conversa e palestras nas manhãs, trabalho em grupo, tempo livre para compartilhamentos e palestra da noite. Nas manhãs, quando não havia palestra, aconteciam os painéis de especialistas, em que hackers, desenvolvedores ou ativistas compartilhavam suas experiências.

Os alunos foram alocados previamente em grupos de trabalho puderam trocar ideias sobre a apresentação. No documento com informações sobre a escola também foram apresentados os temas do trabalho (Wikileaks através do tempo, diversidade no hacking, desenvolvedores e hackers como as novas estrelas de rock, a ascensão e queda do Ethereum/Dao, Science Hub e o lançamento de aplicativos) e questionamentos que poderiam guiar a discussão do grupo.

O grupo de trabalho do qual participei foi composto por quatro alunos e o tema foi "o lançamento de aplicativos". A proposta era discutir os processos internos de uma equipe de desenvolvedores, principalmente relacionados à gamificação do trabalho buscando produtividade e melhores marcadores de performance, as experiências durante a demonstração, os mecanismos sociais e econômicos inerentes que revelam o tipo de produção, as estruturas de poder e sensibilidades incluídas e excluídas.

O grupo decidiu focar em demonstração de *software* e fazer entrevistas com dois programadores que foram chamados para contar de suas vivências, ainda que tenhamos nos focado apenas nos relatos da programadora indiana. Seu relato chamou atenção por ser acrítico em relação ao funcionamento do desenvolvimento de um recurso do aplicativo no qual trabalhava: alguém chegava com o problema, desenvolvia o recurso e mandava a solução para o responsável. Quando a solução não era boa o suficiente, o problema era encaminhado para outro funcionário. O desenvolvedor nunca via seu trabalho incorporado ao produto e, mesmo assim, a lógica de coletivismo e produção em grupo era difundida pela empresa em que trabalhava. A hierarquia era bem estabelecida durante o processo de trabalho, ainda que os chefes buscassem incorporar elementos mais lúdicos e espaços e momentos de convivência. Os incentivos eram coletivos, mas os trabalhos e a recompensa financeira eram individuais. Falamos sobre o conceito de alienação e ela nos disse que, apesar de não se importar em trabalhar desse jeito, as vezes ela gostaria de ver como sua criação foi incorporada no aplicativo.

O trabalho em grupo foi uma das grandes reclamações sobre a organização da escola. Em uma página de *pad* do Riseup que utilizamos como meio de avaliação (por permitir contribuições anônimas), os comentários se focaram nos temas pouco interessantes e

a obrigatoriedade em trabalhar com outras pessoas ao invés de poder conversar livremente com outras. Além disso, uma falha da escola foi não conversar sobre as pesquisas dos alunos. Em conversas individuais ou informais, o assunto sempre surgia e acabei ouvindo sobre diversos marcos teóricos que desconhecia. Essa questão também foi levantada aos organizadores.

Outras questões durante o período da Escola Doutoral chamaram a atenção. Primeiro, na primeira manhã da escola, Gabriella Coleman fez uma apresentação com vídeos e áudios sobre a multiplicidade do ser hacker, um dos temas da sua pesquisa e da Escola Doutoral. A única citação sobre a questão de gênero foi em relação a uma mulher transgênero cuja transição foi recebida sem preconceitos pela comunidade hacker. Uma das alunas, que havia publicado um artigo sobre mulheres em comunidades de desenvolvedores[8], apontou que mulheres cisgênero não têm a mesma aceitação. Nesse momento, vários dos alunos e panelistas técnicos começaram a discordar, comentando que a percepção dela era enviesada e que o parâmetro para a aceitação de um hacking ou código deveria ser apenas sua qualidade. Desse momento em diante, toda discussão sobre representatividade e desigualdade (entre gêneros, regiões etc.) era seguida por protestos, principalmente vindos dos representantes do Vale do Silício e norte-americanos ali presentes.

Segundo, alguns dos temas propostos para a escola doutoral, como igualdade e elitismo no hacking e lógicas de perturbação, que tocavam nesses pontos de representatividade, desigualdade e alternativas, foram explorados principalmente nas palestras, enquanto temas sobre vigilância e segurança da informação foram amplamente explorados nos painéis técnicos e nas conversas informais entre alunos, palestrantes e especialistas.

Tentativa de inserção em um hackerspace feminista

Ainda no início da trajetória de pesquisa, quando *hackerspaces* eram um objeto provável, busquei caminhos para realização de trabalho de campo. Em 2017, havia basicamente um *hackerspace* por estado, exceto em São Paulo, com dois ou três na capital. Primeiro contato com um membro de um *hackerspace* foi na CryptoRave de 2017, quando fui

[8] O artigo discorre sobre como o código de mulheres é recebido/avaliado na comunidade de desenvolvedores chamada Github quando os membros da comunidade sabem que a postagem original foi feita por uma mulher ou não. A principal conclusão foi que, quando sabem, a nota é muito mais baixa do que quando desconhecem. Outra conclusão foi que várias mulheres, identificadas ou não, reproduzem os machismos que encontram para conseguir participar do grupo de programadores homens.

apresentada a uma das responsáveis pela organização da MariaLab por uma colega que começava a fazer parte do coletivo. Apresentei-me por nome e como pesquisadora e falei que tinha interesse em acompanhar as atividades por causa da minha pesquisa. No mesmo momento fui avisada que pesquisadores não são benquistos porque são forasteiros e espiões e logo a pessoa a qual fui apresentada mudou de assunto e foi embora. Tentei começar conversas com outros membros da MariaLab, mas o dia parecia estar agitado.

Um tema comum tanto nas dissertações sobre *hackerspaces* quanto nas discussões entre os alunos da Escola Doutoral foram as dificuldades em realizar trabalho de campo. Até então, só havia tido conhecimento de espaços de sociabilidade hacker predominantemente masculinos em que os pesquisadores identificaram como barreira à entrada a falta de conhecimento técnico sobre programação e hacking, reforçando a percepção de que esses espaços são regidos por um forte *ethos* tecnomeritocrático. Um dos casos mais interessantes foi de uma das alunas da Escola Doutoral que participou de uma edição do *Chaos Communication Congress* (congresso anual do *Chaos Computer Club*, *hackerspace* alemão e um dos maiores do mundo). Segundo seu relato, mesmo tentativas de conversas informais foram repelidas pelos membros do *hackerspace* e interações só foram possíveis após ser apresentada formalmente por um colega hacker também membro que deu seu atestado de confiança. No caso dos coletivos hackers feministas, as pesquisadoras com quem conversei deram início ao processo de inserção ao participar das atividades organizadas por eles e não como pesquisadoras. A percepção é que, nesses casos, a barreira de entrada não seria a falta de conhecimentos técnico, mas a perspectiva que as integrantes desses coletivos têm sobre as dinâmicas e objetivos da pesquisa acadêmica – algo que se intromete, analisa e expõe – e as consequências para sua segurança como espaço de proteção e cuidado contra violência na Internet e de apoio a outros coletivos feministas.

Nos meses seguintes a CryptoRave, em que comecei a fazer parte da lista de e-mail do MariaLab e do grupo aberto do Telegram, fiquei atenta sobre atividades do coletivo. Sendo o primeiro *hackerspace* feminista criado no Brasil, surgiu da vivência de mulheres e pessoas transgênero que não se sentiam incluídas ou seguras em *hackerspaces* porque, apesar do discurso de serem abertos a pessoas de todos os gêneros, o público era majoritariamente masculino. Essa percepção, consoante com os motivos do movimento de criação de *hackerspaces* alternativos apontado por Toupin (2014), levou à criação da MariaLab em 2013 por mulheres que buscaram construir um lugar onde o protagonismo seria feminino, com encorajamento e autodeterminação das mulheres através do interesse pela cultura hacker

Araujo & Gitahy (2016) apontam que apesar de não ter um espaço físico fixo, a MariaLab pode ser considerada um *hackerspace* porque estimula experimentação, colaboração e compartilhamento de conhecimento entre as frequentadoras das atividades, sempre itinerantes. Dentre suas atividades estão encontros, mesas de discussão e oficinas e cursos abertos para mulheres, feministas e outros coletivos e ativistas sobre tecnologia da informação, principalmente sobre segurança de dados, privacidade e outras formas de proteção e autonomia de mulheres por meio do conhecimento e apropriação da tecnologia da informação.

De maio a setembro de 2017, a lista de e-mail foi utilizada principalmente para avisos de vagas de emprego tanto gerais quanto específicas para mulheres. Já o grupo do Telegram, composto por cerca de 160 mulheres cisgênero, transgênero e pessoas de gênero não-binário, apresentou os assuntos mais diversos. Além de oportunidades de emprego e eventos futuros, também eram discutidos os feminismos e os papéis da mulher na tecnologia, além de denúncias e procura por ajuda e conselhos legais para casos de crimes e assédios virtuais. Até quando ainda lia ativamente o chat (setembro de 2017), as conversas eram dominadas pelas mesmas seis ou sete pessoas.

As únicas atividades realizadas nesse período foram dois cursos: redes autônomas feministas e servidoras feministas, oferecidos pela MariaLab. Participei do segundo curso, ministrado por quatro sábados do mês de julho de 2017, das 10 às 18 horas na empresa ThoughtWorks, na cidade de São Paulo. O grupo de alunas era bastante diverso em termos de formação, interesse, origem, gênero e cor. No começo, havia cerca de trinta mulheres cisgênero e transgênero e pessoas de gênero não-binário de coletivos feministas, movimentos sociais e academia. No último sábado de curso, a tarde foi livre para conversas e foi muito interessante ouvi-las. Até então, nunca tinha participado de um espaço livre de conversas envolvendo uma multiplicidade de mulheres e de assuntos, que iam de astrologia para ancestralidade, sexualidade, comandos do Linux, violência e de volta para astrologia. Sendo a única acadêmica com intenções de pesquisa presente naquele momento, fiquei receosa em fazer muitas anotações, então apenas participei e, apenas quando possível, anotava algo.

Houve um episódio em especial quando fomos ensinadas sobre quais informações de um site deveriam ou não estar disponíveis ao público por questão de segurança e alguém da MariaLab falou que o site Think Olga estava exposto havia algum tempo. No período, o coletivo feminista Olga estava com um projeto em que as consultas em mecanismos de buscas por mensagens que incitavam ou indicavam interesse em pornografia infantil eram direcionadas para seu site, especificamente para uma página sobre crime e denúncia. O link

exposto dava acesso a várias estatísticas sobre o site, inclusive qual foram os termos consultados no mecanismo de busca que levou ao redirecionamento. As primeiras (e depois as mais horríveis variações) eram todas mensagens buscando por pornografia infantil de meninas. O redirecionamento dificultava, mas não impedia que o indivíduo procurasse novamente por pornografia depois de obrigado a entrar no Think Olga.

As experiências com o trabalho da MariaLab contribuíram para a reflexão sobre abertura-fechamento não só do coletivo, mas também em relação a outros relatos de pesquisadores que buscavam acessar espaços de socialização hackers para realização de campo. Em termos de conteúdo, o curso, que era aberto para todas as mulheres e em sua proposta acessível inclusive àquelas que não pertencessem à área de tecnologia, foi extremamente difícil de acompanhar e muito denso, o que pode ter refletido no fato de que apenas um terço das alunas finalizou o curso. A proposta de abertura (para todas as mulheres) vai contra o conhecimento técnico básico necessário para acompanhar o conteúdo do curso. Ainda que conhecimento técnico não seja utilizado como uma forma de excluir não-especialistas do espaço, como é verificado em espaços de socialização hackers majoritariamente masculinos (TOUPIN, 2014), acabou dificultando a permanência e acompanhamento do curso. Ao mesmo tempo, toda escolha técnica sobre os passos tomados era acompanhada de justificativas e exemplos em termos de segurança da informação, privacidade e autonomia para ativistas, coletivos e movimentos sociais. Nesse sentido, o curso foi bastante intensivo em termos de conscientização e discussão sobre as intersecções entre tecnologias da informação e feminismos. A MariaLab é um coletivo que se preocupa com proteção, autonomia e conscientização de mulheres sobre questões de segurança da informação e privacidade na Internet e, através do projeto Vedetas[9], se propõe a construir e manter infraestrutura segura para que ativistas, coletivos e movimentos sociais consigam acessar e garantir formas de associação, organização e desenvolvimento de atividades. Nesse sentido, as discussões realizadas e o exemplo do Think Olga – que é um dos vários sites voltados para empoderamento feminino – ajudaram na reflexão do motivo de outro fechamento – o do coletivo para pesquisadores: a exposição dos resultados da pesquisa acadêmica poderia colocar em risco esses indivíduos e grupos.

As indefinições em relação ao objeto de pesquisa, somados à dificuldade em firmar um espaço naquele meio, aos custos de transporte e estadia em São Paulo e aos prazos para realização do doutorado levaram à escolha em encerrar as tentativas em encontrar um

[9] O projeto Vedetas é mencionado no quarto capítulo, junto das discussões sobre políticas do dia-a-dia e intersecções com gênero.

coletivo ou comunidade para realizar etnografia e entrevistas. Essa experiência, porém, foi essencial na construção do meu entendimento sobre a importância da criptografia e outras ferramentas de privacidade e segurança de dados e sobre o sentimento de urgência em discutir essas temáticas em eventos como a CryptoRave.

Experiências na CryptoRave

O interesse em participar da CryptoRave nasceu das tentativas de inserção no *hackerspace* feminista. A MariaLab normalmente propõe atividades para a CryptoRave, de forma que várias das integrantes estariam presentes no evento e nas mesas de debate e eu poderia fazer um primeiro contato com elas, além de identificar e presenciar como as ideias sobre hacking normalmente entram nos debates em eventos como a CryptoRave.

A CryptoRave é um evento organizado, promovido e frequentado principalmente por tecnoativistas, de forma que não deve ser compreendido como um evento de e para hackers, mas sim como um espaço que reúne uma série de temáticas que se entrelaçam com práticas e interesses relacionados a eles, no caso, criptografia, privacidade e segurança na Internet. Como aponta Araujo (2018), o evento congrega pessoas politicamente engajadas na cultura hacker, preocupadas em discutir os efeitos da intensificação do uso de tecnologias no dia-a-dia. Nesse sentido, ainda que aconteçam discussões mais técnicas sobre tecnologias da informação, o evento se configura como um espaço para identificação de discussões entre aqueles que estão envolvidos ou interessados nos desdobramentos do movimento hacker de uma forma mais ampla.

A organização das edições é realizada por um grupo de coletivos e organizações ativistas, tais como a Escola de Ativismo[10], Saravá[11], Actantes[12], Intervozes[13] e Encripta[14]. A cada edição da CryptoRave são feitas chamadas públicas para financiamento coletivo, proposição de atividades e trabalho voluntário durante realização do evento, anunciados pelo site do evento, no Twitter e por lista de e-mail. As chamadas para financiamento coletivo são cheias de memes e deixam bem claro que ou a CryptoRave é totalmente financiada ou não acontece. As doações são feitas através do Catarse, plataforma de financiamento coletivo de

[10] https://escoladeativismo.org.br (último acesso em 7 de julho de 2019).
[11] https://sarava.org (último acesso em 7 de julho de 2019).
[12] https://actantes.org.br (último acesso em 7 de julho de 2019).
[13] http://intervozes.org.br (último acesso em 7 de julho de 2019).
[14] https://encripta.org (último acesso em 7 de julho de 2019).

projetos, ou diretamente à carteira de Bitcoins do evento. Os doadores são recompensados com menções, adesivos, canecas e camisetas dependendo do valor doado.

As experiências com as edições da CryptoRave de 2017 e 2018 se deram apenas nos dias de evento, durante as atividades oferecidas, e não na fase da organização. Em 2017, houve a quarta edição da CryptoRave no Brasil, que aconteceu na Casa do Povo, na cidade de São Paulo, nos dias 5 e 6 de maio, começando às 18 horas do dia 5, sexta-feira, até às 19 horas do dia 6, sábado. A edição de 2018 foi realizada na Cinemateca Brasileira, também em São Paulo, nos dias 4 e 5 de maio. Nessas edições, os indivíduos e grupos que apresentaram atividades na CryptoRave eram bastante diversos em termos de gênero, formação, ocupação e nacionalidade: homens cisgênero, mulheres transgênero e cisgênero, profissionais de tecnologia da informação, acadêmicos e ativistas vindos de diferentes países da América Latina e dos Estados Unidos.

Dentre as atividades disponíveis para as edições de 2017 e 2018 estavam palestras, mesas de debate em grandes temas denominados trilhas (política, gênero, segurança, criptografia e hacking), exibição de filmes, *installfest*, oficinas de Arduino e programação, lançamento de livros e rodas abertas de conversa. Os espaços organizados para as atividades, muitas vezes separados apenas por panos pretos, foram nas duas edições identificados com nomes de indivíduos importantes na história da computação, da criptografia ou do hacking, como Alan Turing, Ada Lovelace, Edward Snowden, Chelsea Manning e Aaron Swartz.

Na edição de 2017, todos os três andares da Casa do Povo, além do terraço, foram ocupados com atividades. No primeiro andar havia mesas e cadeiras de uso comum e indefinido e a pequena área de alimentação. O tráfego era bastante intenso no sábado, com algumas mesas e cantos ocupados com os *installfest*, onde todos estavam com seus *notebooks* instalando programas, sistemas operacionais ou compartilhando arquivos, por oficinas de programação e Arduino ou simplesmente por rodas de conversas que se organizavam espontaneamente. Os segundos e terceiros andares foram organizados com cadeiras, telões e projetores para as mesas de debates e palestras e o terraço com lançamento de livro e rodas de conversa, além de um espaço para a exibição de filmes.

Já a edição de 2018 foi em um espaço mais amplo. A Cinemateca Brasileira em São Paulo é repleta de salas e auditórios com janelas grandes e portas de vidro, tornando possível observar outras atividades e movimentos ao longo do dia. Ao contrário da edição de 2017, havia muito espaço para circulação e atividades, de forma que, nesta edição, não encontrei o espaço reservado para *installfest*. Além disso, ao menos no dia que participei

(sábado), havia mais mesas discutindo criptografia, privacidade e política em relação à edição de 2017.

Enquanto as mesas da edição de 2017 duraram cerca de uma hora, sem necessariamente haver tempo para as perguntas, as da edição de 2018 foram mais curtas, com quinze a vinte minutos de apresentação, mais vinte minutos para discussões. Dessa forma, em todas as mesas foi possível ter uma ideia do assunto apresentado, mas nenhuma discussão foi muito profunda porque logo tínhamos que esvaziar as salas para as mesas seguintes. As duas mesas mais longas aconteceram no final do evento simultaneamente: a de Fernanda Bruno e a equipe do MediaLab da Universidade Federal do Rio de Janeiro (UFRJ) e a de Sérgio Amadeu da Silveira.

Além das observações ao longo dos dias de evento, participei de quatorze atividades: uma palestra, uma atividade artística[15] e doze mesas de discussão. O quadro a seguir apresenta um resumo das atividades:

Quadro 3 - Participação como ouvinte em mesas de duas edições da CryptoRave no Brasil

Ano	Trilha	Título
2017	Palestra	Resistindo à distopia – práticas para dialogar com não especialistas
2017	Atividade	Definições do ser com as tecnologias da informação
2017	Gênero	De volta ao ciberfeminismo: história e os desafios para o resgate e promoção da participação das mulheres na tecnologia
2017	Política	Criptografia e agroecologia: alternativas feministas em defesa dos comuns - nossas tecnologias, outras formas de vida. Como semear a resistência feminista?!
2017	Gênero	(Cyber)espaços seguros: redes autônomas feministas
2018	Privacidade	A GDPR chegou!! Como se preparar?
2018	Anonimato	*Investigación y Desarrollo del proyecto Tor*
2018	Política	Criptografia, privacidade e política
2018	Gênero	SaferManas
2018	Gênero	Ciberseguras
2018	Privacidade	Cidadão Quem? Usos e Abusos da Biometria no Brasil
2018	Segurança	*Whatsapp y comunidades vulnerables*
2018	Hacking	*Leakydata*
2018	Política	A economia psíquica dos algoritmos

Fonte: elaboração própria. Uma primeira versão deste quadro contava com os links para as atividades. Porém, o site das edições de 2017 e 2018 da CryptoRave foi tirado do ar na última consulta realizada (em abril em 2019).

[15] Tanto a palestra "Resistindo à distopia – práticas para dialogar com não especialistas" quanto a atividade artística foram ministradas por Sasha Costanza-Chock e Lili_Anaz na edição de 2017.

Em 2018, tomei conhecimento de outro evento relacionado à cultura hacker na América Latina, chamado Primavera Hacker, que acontece em Santiago, no Chile. De acordo com a descrição do site, o evento parte do pressuposto de que tecnologias não são neutras e se configura como um encontro aberto sobre as relações entre tecnologia, política e práticas criativas voltadas para a criação de dissidência na lógica econômica dominante. O evento declara sua perspectiva pós-colonial ao escrever que "*Debemos cuestionar y discutir la tecnología que utilizamos desde Latinoamérica y la periferia, para comprender hasta qué punto se ha expandido el colonialismo mediante las tecnologías digitales y de qué forma podemos desarrollar autonomía sobre nuestro território*"[16]. As edições do evento são temáticas, sendo que os seguintes temas já foram desenvolvidos: "*Opensource y práctivas creativas*" (2013), "*Tecnopolítica*" (2014), "*Desobediencia tecnológica*" (2015) e "*phacker*" (2016 e 2017). As duas últimas edições foram semelhantes a CryptoRave em termos de temática (vigilância em massa, ferramentas de segurança na Internet, desníveis de poder entre grandes corporações e indivíduos/movimentos sociais), em relação aos temas das mesas (autodefesa digital, gênero, tecnologias livres) e também quanto a alguns coletivos e palestrantes (Escola de Ativismo, Lili_Anaz, Projeto Tor, Ciberseguras). De forma geral, a Primavera Hacker pareceu um evento também organizado por tecnoativistas, além de bastante politizado. O acesso ao site da Primavera Hacker permitiu consolidar minha percepção de que a CryptoRave trabalha com assuntos que também estão sendo discutidos em outros eventos interseccionados com hackers na América Latina. No período de escrita da tese, o site da Primavera Hacker estava fora do ar e seu conteúdo não foi utilizado para o desenvolvimento do estudo.

Para finalizar, voltando a CryptoRave, ainda que não seja um evento específico de e para hackers, minha experiência começou com uma história: chegando na Casa do Povo, fui informada de que um estudante de Humanidades que estava lá para coletar dados para sua pesquisa, anotando tudo em seu *notebook* com *software* proprietário (Windows) foi hackeado rapidamente e perdeu todos seus arquivos. A história era contada repetidamente em tom de deboche, seguida da esperança de que o garoto houvesse feito *backup*.

A história, verdadeira ou não, remete a características atribuídas aos hackers: valorização da brincadeira, pegadinhas e humor em sua aparência ou em suas habilidades técnicas e seu código (EVANGELISTA, 2010; COLEMAN, 2013) e a rigidez em relação a como um indivíduo deve se portar para ser considerado um hacker (RAYMOND, 1996,

[16] Trecho retirado do site do evento (https://phacker.org, última consulta em 2 de agosto de 2019).

revisão 1.51 out. 2017). O garoto teria sido hackeado não porque poderia estar colocando todos ali em risco ou porque seus dados eram armazenados pela grande corporação responsável pelo sistema operacional que utilizava, mas como brincadeira, como lição: quem está na CryptoRave não deve usar *software* proprietário. Porém, o detalhe de que o garoto era um estudante de Humanidades não deve passar despercebido: a história funcionou como um conto preventivo para as interações que logo teria com o MariaLab e ajudou a validar as percepções dos pesquisadores de que é necessário transpor uma série de barreiras para a inserção nos grupos e comunidades hackers, que podem ir da desconfiança e das escolhas de adoção de tecnologias para o dia-a-dia até a falta de conhecimento especializado sobre tecnologias da informação.

CAPÍTULO 2 - Estudos hackers: genealogias e políticas

O objetivo deste capítulo é apresentar os principais autores dos estudos hackers e trazer as discussões mais recentes sobre políticas hackers identificadas na literatura consultada, constituindo, assim, o estudo de escopo. O conteúdo aqui desenvolvido traz histórias de origem, genealogias e localiza geográfica e historicamente grupos, comunidades e gêneros hackers, além de apresentar como essa temática vem sendo trabalhada pelos estudos hackers. Nesse sentido, são apresentadas definições e categorias de análise criadas pelos autores estudados com o objetivo de identificar posteriormente o que é próprio do ser e fazer hacker – e portanto comum a diferentes manifestações e gêneros – e o que é característico dos hackers de computador na América Latina.

Os estudos hackers são compostos, pelo que aponta Söderberg (2017), por momentos. O primeiro deles é composto por uma literatura que impactou na consolidação do imaginário sobre o que significa ser hacker em termos de comportamentos e práticas, uma vez que abriu frestas para o público espiar um universo desconhecido, exótico e contido em si mesmo. Um dos primeiros escritos sobre hackers foi lançado em 1984 por Steven Levy: o livro "*Hackers: heroes of the computer revolution*", de cunho jornalístico, se constitui como resultado de um extenso trabalho de observação e entrevista com diferentes gerações de hackers. O texto, ao descrever fisicamente os personagens, contar histórias pessoais e cenas observadas, remonta como as relações, práticas e lógicas dos grupos foram se construindo entorno das brincadeiras, manipulações e aperfeiçoamentos de máquinas e computadores. O impacto de sua publicação foi tão grande que não só influenciou na popularização do termo "hacker", como estimulou a realização da primeira conferência hacker, que reuniu Levy e outros indivíduos entrevistados por ele, e originou um documentário de 1985 chamado "*Hackers: wizards of the eletronic age*", depois transmitido em rede nacional (EVANGELISTA, 2010).

Em termos de gerações, Steven Levy explora os hackers dos laboratórios do MIT dos anos 1950 e 1960, os hackers de *hardware* da Califórnia dos anos 1970 e os hackers de jogos de computador pessoal dos anos 1980. Na quarta parte do livro, o autor trata de Richard Stallman, criador da *Free Software Foundation*, ao qual chama de o último dos verdadeiros hackers por sua luta pela manutenção dos preceitos da ética hacker nos laboratórios do MIT, que fora observada por Steven Levy nos anos 1950 e 1960 e, nas décadas seguintes, começaram a se desvanecer frente às leis de direitos autorais, ao uso de *software*s

proprietários e à dinâmica menos cooperativa e experimental que se instaurava nos laboratórios.

Ainda dentro do primeiro momento dos estudos hackers estão Eric Raymond, Manuel Castells e Pekka Himanen, que tratam de aspectos diferentes do hackerismo, mas conversam entre si, construindo uma narrativa específica importante tanto para o imaginário do ser e fazer hacker quanto para como essa temática começa a ser abordada pelos pesquisadores.

Mais especificamente, em "*How to become a hacker?*" (1996, revisão 1.51 out. 2017) e "A Catedral e o Bazar" (1999), Eric Raymond – programador de *software* proprietário que passa a escrever para a comunidade desenvolvedora manuais e reflexões sobre hackers e seu processo de criação de código a partir de suas experiências com o desenvolvimento de *software* – conecta hackers ao movimento do código aberto, do qual se proclama porta-voz. Raymond posiciona-se contra os caminhos tomados pelo movimento de Stallman ao restringir, profissionalizar e abrir possibilidades de capitalização do trabalho hacker e descrevendo o trabalho hacker como divertido, desafiador e voltado para a satisfação pessoal.

A definição de hacker de Eric Raymond é, de certa forma, absorvida por Manuel Castells (2001; 2003) e Pekka Himanen (2001), uma vez que estes autores escrevem sobre aspectos que refletem dinâmicas das comunidades de *software* livre e código aberto. As maiores contribuições estão nas discussões sobre ética e trabalho hacker e sobre o contexto no qual esses atores estão inseridos – o capitalismo informacional (CASTELLS, 2001)[17]. Pekka Himanen, filósofo de formação, empresta o conceito de capitalismo informacional de Castells para contextualizar a ética do trabalho hacker como alternativa à ética protestante do capitalismo industrial no pós-industrialismo (HIMANEN, 2001). A partir de então, a ideia de que o trabalho hacker existe fora da lógica capitalista torna-se presente na literatura.

O segundo momento dos estudos hackers é marcado por uma institucionalização da produção de conhecimento. Os autores cuja produção se enquadra neste momento são pesquisadores e acadêmicos, de forma que os escritos abandonam o tom jornalístico (LEVY, 1984) ou o caráter de manual (RAYMOND, 1996, revisão 1.51 out. 2017; 1999) e assumem características de texto científico. Para o segundo momento dos estudos hackers, o estudo de escopo se focou nos trabalhos de Gabriella Coleman (2004; 2011; 2016; 2017), Christopher

[17] Comentários sobre o capitalismo informacional são feitos no terceiro capítulo, uma vez que a maior parte do conjunto de publicações selecionadas utilizou este contexto para situar os estudos de caso sobre hackers na América Latina.

Kelty (2005); Maxigas (2017); Johan Söderberg (2013) e seu artigo em conjunto com Alessandro Delfanti (2018).

Em termos de formação acadêmica, estes autores vêm da antropologia sociocultural (Gabriella Coleman) e dos Estudos Sociais da Ciência e da Tecnologia (Christopher Kelty, Alessandro Delfanti, Maxigas e Johan Söderberg)[18] e desenvolvem suas pesquisas sobre temáticas relacionadas a hacking e contraculturas digitais a partir de perspectivas da antropologia, sociologia, economia política, história, entre outras. Os casos estudados por esses autores provêm de comunidades e espaços de socialização, como aqueles relacionados ao *software* livre e código aberto (Coleman, Kelty e Söderberg) e os *hackerspaces*, *hacklabs* e laboratórios experimentais (Delfanti, Maxigas e Söderberg).

A decisão por trabalhar com esses autores também passou pela forma com que discutem a literatura do primeiro momento, por se identificarem como parte deste corpo de conhecimento e por dialogarem entre si sobre os casos e as proposições teóricas sobre hackers que desenvolvem, além do fato de estarem presentes na Escola Doutoral da Estudos Digitais, de onde surgiram questões que levaram ao desenvolvimento deste estudo. Em relação à literatura do primeiro momento, estes autores não excluem suas definições, descrições e proposições sobre hackers, mas buscam desconstruir sua rigidez, identificando e analisando a multiplicidade das origens, práticas, políticas e localização das manifestações hackers a partir do estudo de caso de experiências estadunidenses e europeias. Especificamente, esses cinco autores se voltaram para a discussão das diversas formas em que as políticas hackers emergem, que é de interesse para esta pesquisa. De acordo com Söderberg (2017), o interesse desses autores nas políticas hackers nasceu da percepção de hackers são bem-sucedidos em disseminar seus futuros, de modo que olhar para os hackers no presente se conforma como uma janela para as relações entre sociedade e tecnologia no futuro próximo.

A entrada das políticas na agenda de pesquisa dos estudos hackers se configura como reflexo da potência dos imaginários hackers e acontece, a partir da literatura consultada, no começo dos anos 2000. Dois dos primeiros estudos explorados que se preocuparam em discutir características das políticas hackers foram "*The political agnosticism of free and open source softwares*" (COLEMAN, 2004) e "*Geeks, social imaginaries, and recursive publics*" (KELTY, 2005), que tratam de aspectos tecnopolíticos dos hackers. Enquanto o primeiro estudo focou nas discussões acerca da inclinação em deixar diferenças ideológicas de lado para resolver problemas técnicos, o segundo teve como propósito tratar das implicações na

[18] No caso dos Estudos Sociais da Ciência e da Tecnologia, alguns dos programas aparecem como Ciência e Sociedade ou Ciência, Tecnologia e Sociedade.

constituição de grupos de hackers que se alinham por conta da preocupação compartilhada em relação às condições técnicas e legais que possibilitam sua associação e existência.

Estudos mais recentes têm se preocupado em evidenciar a multiplicidade de políticas (COLEMAN & GOLUB, 2008; MAXIGAS, 2012; SÖDERBERG, 2013; TOUPIN, 2014; COLEMAN, 2017; MAXIGAS, 2017), identificar os movimentos e ciclos da politização (GRENZFURTHNER & SCHNEIDER, 2009; MAXIGAS, 2012; COLEMAN, 2017; DELFANTI & SÖDERBERG, 2018) e propor arcabouços para análise das políticas hackers (MAXIGAS, 2017; DELFANTI & SÖDERBERG, 2018).

Neste sentido, buscando apresentar as discussões sobre políticas hackers, este capítulo está estruturado em quatro partes. Primeiro, apresento algumas genealogias hackers, a origem do estereótipo hacker e algumas implicações da sua força para as políticas hackers. Em seguida, procuro apresentar as discussões mais recentes sobre políticas hackers com dois conceitos que perpassam os textos consultados – agnosticismo político e público recursivo – e as conjeturas sobre quais são as características e condicionantes das políticas hackers e do engajamento desses atores. De acordo com a literatura consultada, as formas com que os hackers percebem o que é liberdade – acesso, expressão, pensamento, ação, autonomia – são fundamentais para como os hackerismos se manifestam e como hackers se politizam. Nesse sentido, é quando sentem sua existência como público ameaçada – quando suas liberdades são atacadas – que hackers se engajam politicamente. Ainda no segundo item, também trato de outras duas discussões identificadas na literatura consultada: as relações entre determinismo tecnológico–ação política dos hackers e os aspectos luditas do hackerismo, em outras palavras, quais são algumas das racionalidades por traz do engajamento políticos dos hackers e como se manifestam. No terceiro item, são apresentadas as discussões sobre limitações das políticas hackers, que atravessam o movimento de absorção e cooptação das práticas subversivas e tecnologias hackers pelo capitalismo e, por fim, discorro sobre as políticas do *hacklabs* e *hackerspaces*, espaços livres de socialização hacker cuja história e desenvolvimento são exemplares das discussões apresentadas ao longo do capítulo.

2.1 Genealogias hackers

A versão mais conhecida da origem dos hackers remete a um pequeno grupo de entusiastas de computadores e modelos de trem do *Tech Model Railroad Club* do MIT (*Massachusetts Institute of Technology*) na década de 1950 que passou a utilizar o termo hacker como forma de identificação e diferenciação em relação aos outros engenheiros do

instituto (LEVY, 1984; HIMANEN, 2001; CASTELLS, 2003). O grupo acreditava que as convenções seguidas pelos engenheiros enrijeciam o processo inventivo, que deveria ser contingencial e quebrador de regras. Os hackers, para este grupo, eram aqueles que davam outros propósitos às ferramentas buscando melhorar ou transformar sua utilidade.

> *"As I talked to these digital explorers, ranging from those who tamed multimillion-dollar machines in the 1950s to contemporary young wizards who mastered computers in their suburban bedrooms, I found a common element, a common philosophy which seemed tied to the elegantly flowing logic of the computer itself. It was a philosophy of sharing, openness, decentralization, and getting your hands on machines at any cost to improve the machines, and to improve the world. This Hacker Ethic is their gift to us: something with value even to those of us with no interest at all in computers. It is an ethic seldom codified, but embodied instead in the behavior of hackers themselves. I would like to introduce you to these people who not only saw but lived the magic in the computer, and worked to liberate the magic so it could benefit us all. These people include the true hackers of the MIT artificial intelligence lab in the fifties and sixties; the populist, less sequestered hardware hackers in California in the seventies; and the young game hackers who made their mark in the personal computer age of the eighties."* (LEVY, 1984, pp. ix-x)

Neste trecho do livro, o autor Steven Levy os caracteriza como um grupo de indivíduos que, mesmo pertencentes a diferentes décadas e grupos de prática, apresentam elementos em comum: a materialidade concentrada no computador, suas redes e estruturas, a filosofia do compartilhamento, abertura e do fazer, desconfiança em relação às autoridades e a crença na capacidade dos computadores em ser a base de um mundo melhor – chamada ética hacker[19]. Foi no centro da primeira geração de hackers – formada por jovens do sexo masculino, fãs de ficção científica, interessados em explorar tecnologias, socialmente retraídos, com bom desempenho escolar, mas avessos às estruturas acadêmicas do MIT nos anos 1950 – que os preceitos da ética hacker emergiram, implícitos nas práticas e culturas que se desenvolveram entorno do uso do computador TX-0, o computador Experimental Transistorizado zero, e foram organizados por Levy (1984) como:

> "*Access to computers – and anything which might teach you something about the way the world works – should be unlimited and total. Always yield to the Hands-On Imperative! [...]*
> *All information should be free [...]*
> *Mistrust authority – promote decentralization [...]*
> *Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position [...]*
> *You can create art and beauty on a computer [...]*

[19] Evangelista (2010) discute extensamente semelhanças e diferenças entre as éticas hacker apresentadas por diferentes autores (LEVY, 1984; RAYMOND, 1996 revisão 1.51 out. 2017; 1999; HIMANEN, 2001) e quais suas implicações para o ser hacker.

> *Computers can change your life for the better [...] like Aladdin's lamp, you could get it to do your bidding"* (LEVY, 1984, pp. 28-34)

De forma geral, esses preceitos incorporam uma série de comportamentos e conceitos que se tornaram características dos hackers ao longo dos anos, principalmente quanto à centralidade da liberdade da informação para expandir o conhecimento e a consequente indisposição contra toda e qualquer regra ou organização que crie barreiras para tal, além do *ethos* meritocrático e da percepção de que saber usar, criar e transformar por meio dos computadores pode levar a uma vida melhor.

A segunda geração retratada por Levy (1984), os hackers de *hardware* dos anos 1970, começou a surgir com a contracultura nos anos 1960 e, ainda que o engajamento político não possa ser generalizado, muitos de seus representantes eram ativistas, o que refletiu em seu entendimento de que computadores e outras tecnologias deveriam ser popularizados por se configurarem como instrumentos potenciais para a luta política e libertação pessoal. Dentre esses hackers, o grupo mais conhecido foi o *Homebrew Computer Club*, formado por figuras que se tornaram conhecidas no Vale do Silício, como Steve Jobs e Steve Wozniak, e onde os primeiros modelos de Apple foram vendidos. De acordo com Levy (1984):

> *"These were people intensely interested in getting computers into their homes to study, to play with... and the fact that they would have to build the computers were no deterrent. The introduction of the Altair had told them that their dream was possible, and looking at others with the same goal was a thrill in itself."* (LEVY, 1984, p. 202)

Além dos assuntos mais técnicos, os membros do *Homebrew Computer Club* também discutiam sobre suas expectativas em cooperar e compartilhar naquele espaço e especulavam sobre quais seriam as atividades que pessoas realizariam se tivessem computadores em casa. Como reforça Evangelista (2010), através da apropriação e aperfeiçoamento do conjunto montável de computadores do Altair 8800 e dos microchips, um dos impactos dessa geração de hackers foi a disseminação dos computadores pessoais.

Por fim, em decorrência da popularização dos computadores pessoais, uma terceira geração de hackers, os hackers de jogos, despontou nos anos 1980 em torno dos jogos eletrônicos. Evangelista (2010) descreve sucintamente a terceira geração a partir de Levy (1984):

> "O período é de explosão da indústria de *software*, calcada especialmente nos games. Como eram programas ainda rudimentares, o esforço para sua criação podia ser desenvolvido às vezes por um único indivíduo. Levy conta histórias que envolvem a crescente profissionalização dessa indústria, cujos profissionais muitas vezes eram adolescentes que batiam na porta das empresas produtoras e distribuidoras com um game praticamente pronto. Em comum com os outros hackers, os 'hackers dos games' teriam a paixão pelo trabalho criativo; a abordagem não tradicional em relação aos horários de trabalho; a cultura do compartilhamento e de liberdade de expressão; o sentimento de satisfação pela capacidade de controlar a máquina e por obter respostas lógicas aos comandos apresentados a ela; e uma atitude um tanto desinteressada com relação ao dinheiro. No campo pessoal, esses novos hackers seriam semelhantes aos antigos, nerds com paixão pela ficção científica, jogos de fantasia e inabilidade social." (EVANGELISTA, 2010, p. 178)

De forma geral, a literatura que caracteriza esse primeiro momento dos estudos hackers costuma definir o conceito de hacker como um grupo de indivíduos com história compartilhada ou engajamento em práticas comuns. Castells (2003), como exemplo, afirma que indivíduos se tornam hackers a partir de características como autonomia em relação às instituições, programação criativa e organização das comunidades em torno da rede de computadores como base material e tecnológica. Castells (2003) coloca os hackers, mais especificamente a cultura hacker, como elemento fundamental na construção da Internet. Isso porque o autor entende que a defesa da autonomia, da liberdade e da cooperação, elementos essenciais dessa cultura, fomenta inovações tecnológicas com base em colaboração e comunicação livre.

Himanen (2001) é mais abrangente. Para o autor, hackers podem ser entendidos como entusiastas ou especialistas de diversas áreas para quem o acesso e compartilhamento de conhecimento e a colaboração para criação e invenção são essenciais e sua relação com essas atividades é prazerosa e desafiadora. Nesse sentido, hacker seria uma forma de ser e agir e não estaria relacionado a um grupo de atividades específicas.

As definições propostas pela primeira geração dos estudos hackers muitas vezes polarizavam hackers moralmente (COLEMAN & GOLUB, 2008; SCHROCK, 2014). É o caso de Eric Raymond, Pekka Himanen[20] e Manuel Castells, cuja primeira preocupação em "A Galáxia da Internet" é desfazer o mal-entendido gerado pela mídia[21]:

[20] De acordo com Himanen (2001), Levy (1984) não viu necessidade em distinguir hackers e *crackers* porque os vírus e *softwares* maliciosos se propagaram a partir da segunda metade dos anos 1980. Porém, nas reedições de "*Hackers: heroes of the computer revolution*" (2010) também não há menções do termo (exceto pelo nome das bolachas).

[21] As definições de Eric Raymond, Pekka Himanen e Manuel Castells são bastante semelhantes. Castells escreveu o posfácio de Himanen (2001) e cita o autor em "A Galáxia da Internet" (2003). Himanen (2001) utiliza os textos de Eric Raymond e o Jargon File para suas definições. O Jargon File é um compêndio de gírias e termos sobre tradição, folclore e humor hacker organizado por Eric Raymond.

> "Os hackers não são o que a mídia diz que são. Não são uns irresponsáveis viciados em computador empenhados em quebrar códigos, penetrar em sistemas ilegalmente, ou criar o caos no tráfego dos computadores. Os que se comportam assim são chamados 'crackers', e em geral são rejeitados pela cultura hacker, embora eu pessoalmente considere que, em termos analíticos, os crackers e outros cibertipos são subculturas de um universo hacker muito mais vasto e, via de regra, são destrutivos." (CASTELLS, 2003, p. 38)

Existe um esforço na literatura mais recente dos estudos hackers em recuperar outras origens, de forma que o ser hacker deixa de estar ligado somente à ética e às práticas de um grupo específico de especialistas em *software* e se torna múltiplo. Ainda que não seja possível afirmar que esse movimento veio em resposta aos primeiros escritos sobre hackers nos anos 1980 e 1990, o estabelecimento dos estudos hackers como campo do conhecimento trouxe uma série de estudos interdisciplinares e dados etnográficos de comunidades que se identificam com diferentes formas do ser hacker.

Coleman & Golub (2008) apontam que as primeiras literaturas tendem a propagar duas visões: ou dos hackers como jovens do sexo masculino viciados em Internet obcecados por brincadeiras, buscar conhecimento e provar suas habilidades ou dos hackers como agentes da emancipação do mundo das restrições da modernidade e do capitalismo. A reafirmação dessas duas visões, porém, apagaria a multiplicidade da significância cultural dos hackers de computador e o fato de que, em realidade, não existe só uma ética hacker. Mais importante, hackers não estão circunscritos a apenas uma prática ou gênero.

De acordo com Coleman (2016), uma das características que perpassa as várias manifestações técnicas e morais do ser hacker é a convergência na prática entre ofício e artifício (*craft* e *craftiness*, no original em inglês). Enquanto a ideia de ofício incorporaria questões como estabelecimento de normas, tradições e aprendizado em espaços de socialização, a de artifício apontaria para a prática hacker de modificar ou quebrar regras, códigos, artefatos e limitações tecnológicas existentes para exercer o direito à criatividade, à individualidade e ao fazer.

> *"To be sure, hackers can be grasped by their similarities. They tend to value a set of liberal principles: freedom, privacy, and access. Hackers also tend to adore computers—the glue that binds them together—and are trained in specialized and esoteric technical arts, primarily programming, system, or Net administration, security research, and hardware hacking. Some gain unauthorized access to technologies, though the degree of illegality varies greatly (and much of hacking is legal). Foremost, hacking, in its diference forms and dimensions, embodies an aesthetic where craft and craftiness tightly converge. Hackers thus tend to value playfulness, pranking, and cleverness, and will frequently perform their wit through source code, humor, or both: humorous code."* (COLEMAN, 2013, p. 17).

O reconhecimento do caráter complexo da história do hackerismo faz emergir outras formas do ser hacker até então apagadas, situadas em contextos históricos, culturais e materiais específicos. Desobediência, transgressão e subversão passam a lembradas como condições indissociáveis do ser hacker pelo seu papel no estabelecimento das características culturais e técnicas do *phreaking*, uma das histórias recuperadas dos hackers. Situada nos anos 1950 e 1960, os *phreaks* exploravam equipamentos de telefonia para conseguir acesso ao sistema telefônico público e se conectar gratuitamente com qualquer outro telefone no mundo.

> "*When phreaking (originally called freaking) and hacking stabilished their cultural and technical legs in the late 1950s and early 1960s, rule breaking was often essencial to gaining access to any equipment. For phone freaks, rule breaking was simply unavoidable. Their entire raison d'être was the exploration of phone systems and to link up with other phone enthusiasts in the doing, even if profit or malice were rarely part of their calculus, they nevertheless violated state and federal laws every time they phreaked."* (COLEMAN, 2017, p. S93)

Mesmo com o esforço em resgatar outras origens e a crescente percepção de que hacker é um conceito em disputa e transformação (COLEMAN & GOLUB, 2008; COLEMAN; 2016; ARAUJO; 2018; DELFANTI & SÖDERBERG, 2018), persiste o estereótipo de que hackers são homens brancos libertários, apolíticos, aficionados por tecnologia da informação e interessados em provar seu valor pela qualidade do que criam ou transformam. De fato, essas são as características de membros de diversas comunidades hackers e podem ser observadas em conferências, listas de e-mail, fóruns de *software* livre e código aberto, e outros espaços de convivência e socialização hackers. O problema estaria em deixar esse estereótipo dominar as narrativas e se tornar a representação de todas as manifestações hackers.

Um exemplo da pervasividade deste estereótipo é discutido por Coleman (2016): pesquisas acadêmicas costumam ter como o ponto de partida o hacker libertário e apolítico. Isso aconteceria por dois motivos. Primeiro, porque esse estereótipo é desproporcionalmente forte, uma vez que parte da literatura publicada e conhecida trata dos hackers de regiões onde o libertarianismo domina, de forma que essas descrições acabam generalizadas para toda cultura hacker. Estão incluídos, aqui, os textos de Raymond e todo material dos tecnólogos do Vale do Silício, cujas atividades e valores circulam muito mais rápido que os de outras formas do ser hackers em decorrência da quantidade de recursos envolvidos. Segundo, porque

existiria uma escassez de estudos históricos sobre as múltiplas genealogias hacker e de pesquisas contemporâneas sobre diferenças regionais[22].

O estereótipo em questão foi reforçado e propagado por um dos primeiros autores dos estudos hackers, Eric Raymond. O conteúdo dos seus textos são citados exaustivamente tanto na literatura quando em comunidades de discussão e grupos de prática e refletem um momento de expansão da profissionalização e da cultura do compartilhamento, portanto, quando os hackers de *software* começam a entrar em conflito com as leis de propriedade intelectual e revolver em torno de dois movimentos específicos: o do *software* livre e o do código aberto.

Raymond (1996, revisão 1.51 out. 2017) esclarece desde o início sobre quais hackers escreve, os hackers de *software*, conectando-os a uma historicidade específica:

> *"There is a community, a shared culture, of expert programmers and networking wizards that traces its history back through decades to the first time-sharing minicomputers and the earliest ARPAnet experiments. The members of this culture originated the term 'hacker'. Hackers built the Internet. Hackers made the Unix operating system what it is today. Hackers make the World Wide Web work. If you are part of this culture, if you have contributed to it and other people in it know who you are and call you a hacker, you're a hacker."* (RAYMOND, 1996, revisão 1.51 out. 2017).

Ao contrário da narrativa construída por Steven Levy, Eric Raymond assume o lugar de porta-voz deste grupo de hackers e seus textos[23] funcionam como manuais com prescrições para os indivíduos que queiram participar dessa comunidade. Nesse sentido, hackers devem ser tecnicamente habilidosos, resolver problemas, construir coisas e acreditar na liberdade e na ajuda voluntária – apenas quem segue e acredita nisso pode ser reconhecido como um hacker (RAYMOND, 1996, revisão 1.51 out. 2017). Tão importante quanto, Raymond também demarca quem deve ser excluído desse grupo: aqueles que se autodenominam hackers ou invadem computadores e sistemas telefônicos, isso porque crimes não demandam nenhum conhecimento excepcional em tecnologia. Esses, segundo Raymond, são vistos com maus olhos e chamados de *crackers* pelos verdadeiros hackers.

---

[22] A afirmação de Gabriella Coleman sobre a escassez de estudos sobre outras genealogias ou diferenças regionais das manifestações hackers é imprecisa. Esta pesquisa, como exemplo, apresenta um conjuto de publicações acadêmicas que trata de especificidades na América Latina. Durante a Escola Doutoral em 2016, quando a existência de estudos sobre hackers em outras regiões foi levantada, Coleman argumentou que o problema, então, seria uma barreira linguística, já que a maioria dos estudos são publicados em espanhol e português.

[23] "*How to become a hacker*", originalmente publicado em 1996 e atualizado constantemente, "A Catedral e o Bazar" de 1999.

Desta caracterização é possível extrair algumas questões para entender a proposta de Raymond sobre o ser hacker.

Primeiro, que hackers devem ser avaliados por seus pares e reconhecidos na comunidade por suas habilidades, de forma que apenas os próprios hackers podem definir quem é hacker ou não e quais são os parâmetros para se tornar um e ter reconhecimento na comunidade. Esse argumento acaba sendo utilizado pelo próprio Raymond como forma de legitimação de seu texto quando escreve que muitos hackers o consideram definitivo em assuntos hackers:

> "*Back in 1996 I noticed that there didn't seem to be any other FAQs or web documents that addressed this vital question, so I started this one. A lot of hackers now consider it definitive, and I suppose that means it is. Still, I don't claim to be the exclusive authority on this topic; if you don't like what you read here, write your own."* (RAYMOND, 1996, revisão 1.51 out. 2017)

Quando Raymond (1996, revisão 1.51 out. 2017) determina que os parâmetros para a inclusão na comunidade hacker são as habilidades do indivíduo em resolver problemas e escrever programas para distribuição, utilização e divertimento de toda comunidade, o autor faz a conexão entre a cultura hacker e o movimento do código aberto (*open source*) que descreve em pormenores e além do técnico (como se comportar, como se referir a si mesmo, o que não fazer quando entre pares, quais atividades empreender ou não, o que ler, entre outros pontos). A qualidade do código como parâmetro torna-se parte da forma de existir desses hackers. A atitude hacker, envolta nesse conjunto de regras, deve ser cultivada não pelo bem de uma comunidade, mas por ser importante para o desenvolvimento do indivíduo. As motivações devem ser sempre pessoais, as habilidades múltiplas e as atividades desenvolvidas devem quebrar as fronteiras entre trabalhar/se divertir e ciência/arte. Raymond (1996, revisão 1.51 out. 2017; 1999) acaba criando, assim, critérios bastante restritos de inclusão e exclusão na comunidade.

Segundo, Raymond afirma a importância da satisfação dos egos e da construção da reputação na comunidade como na geração do interesse dos hackers para que decidam despender esforços aos se envolverem em projetos. Portanto, se o projeto for divertido ou desafiador o suficiente, de forma que engajar-se nele gere reconhecimento na comunidade hacker, será bem-sucedido. Raymond utiliza o caso do Linux como exemplo de sucesso porque, segundo ele, o gerente do projeto Linus Torvalds conseguiu lidar com a atitude hacker no contexto do desenvolvimento do sistema operacional (RAYMOND, 1999). Ao discutir esse caso e o do *software* que desenvolveu da mesma forma, Raymond compara duas

formas de desenvolvimento, a catedral e o bazar, e acaba por inserir outro ponto frequentemente visitado nos estudos sobre hackers subsequentes: a organização do trabalho hacker.

Nesse sentido, em termos de conteúdo, "A Catedral e o Bazar" contém aprendizados e sugestões para o desenvolvimento e gestão de um projeto de *software* de código-fonte aberto. Raymond trata de detalhes técnicos e de gestão de códigos e pessoas, assim como dificuldades e sucessos ao longo do processo de desenvolvimento do *software fetchmail* e comenta o trabalho de outros colegas desenvolvedores que tentaram fazer o mesmo[24].

Terceiro, em relação às políticas e representações hackers. Anarquista libertário de viés conservador (EVANGELISTA, 2010), Raymond afirma que "verdadeiros hackers" prezam pela liberdade e pela qualidade do código escrito. Por esse motivo, não haveria contradições entre escrever um código que qualquer pessoa (com habilidades) pode testar, modificar, reescrever e a propriedade intelectual sobre o código, desde que o objetivo seja sempre a excelência. Consequentemente, a interação entre hackers e a indústria, seja na produção ou comercialização do código, seria livre e desejada. Ao mesmo tempo em que abre caminho para certas associações, Raymond encerra outras que envolvem o posicionamento político explícito, como defendido pelo movimento relacionado ao *software* livre, e cunha a expressão que é utilizada exaustivamente para demarcar o que deve ser a prática hacker: *"shut up and show them the code"*, mostrando que o verdadeiro hacker se prova pela qualidade técnica de seu código, não por sua política.

Isto posto, é interessante que uma das implicações da força do estereótipo do hacker propagado por Eric Raymond tem sido a longa discussão sobre o lugar da política nessa cultura, especificamente em relação ao papel da política na representação do ser hacker, que tomou forma na cisão entre *software* livre e código aberto, que compartilham das mesmas materialidades e práticas.

Eric Raymond, ao longo dos seus textos, traçou críticas bastante diretas a Richard Stallman, hacker criador da *Free Software Foundation* e representante do movimento do

[24] Raymond propõe olhar as formas de programação de *software* e sistemas como uma catedral ou um bazar. De um lado, o estilo catedral é centralizado em um pequeno grupo de desenvolvedores. Bugs e outros problemas de desenvolvimento são vistos como ocorrências catastróficas que levarão muito tempo e esforço para serem corrigidas, sendo que, no final, o *software* é lançado com atraso numa versão normalmente não perfeita. Do outro lado, o estilo bazar entende os problemas de desenvolvimento como algo simples de ser resolvido porque o código está disponível para inúmeros codesenvolvedores explorarem a cada nova versão de forma que, eventualmente, o erro será encontrado e corrigido.

software livre, por ter atribuído uma ideologia à prática de utilizar código aberto, conectando-a a questões políticas mais amplas.

> *"The hacker community has some specific, primarily defensive political interests — two of them are defending free-speech rights and fending off 'intellectual-property' power grabs that would make open source illegal. Some of those long-term projects are civil-liberties organizations like the Electronic Frontier Foundation, and the outward attitude properly includes support of them. But beyond that, most hackers view attempts to systematize the hacker attitude into an explicit political program with suspicion; we've learned, the hard way, that these attempts are divisive and distracting. If someone tries to recruit you to march on your capitol in the name of the hacker attitude, they've missed the point. The right response is probably 'Shut up and show them the code'."* (RAYMOND, 1996, revisão 1.51 out. 2017)

Raymond não nega a existência de interesses políticos, desde que circunscritos aos preceitos do que move a atitude, trabalho e curiosidade hackers: a defesa da livre expressão que garante a existência e a legalidade do código aberto. A política de Richard Stallman criticada por Eric Raymond está relacionada ao entendimento do primeiro de que qualquer barreira construída para impedir a criação e difusão de conhecimento é antiética – como os direitos autorais que privatizam informação (COLEMAN & GOLUB, 2008). Nesse sentido, desenvolver, distribuir ou utilizar *software* livre não é mandatório porque são práticas que se configuram como soluções econômicas e tecnológicas mais eficientes, mas porque são condições necessárias para que a informação seja, de fato, livre[25].

> *"The disagreement, in addition to concerning diferences over licensing schemes, focused on diferente uses of language. Adherents of the Open Source Initiative were closest to the image of technophilic engineers whose apolitical front rested on unacknowledged, liberal or libertarian commonsensical opinions. In their advocacy of open source solutions they chose to foreground technical efficiency and economic benefits over political considerations."* (SÖDERBERG, 2013, p. 1281)

Portanto, enquanto a forma de escrever código e desenvolver *softwares* pelos princípios de compartilhamento e coletividade são comuns aos dois movimentos, para o código aberto a justificativa é a eficiência econômica e técnica e, para o *software* livre, uma questão moral e ética. As associações previstas entre comunidades hackers e setor privado, assim como comercialização dos *softwares*, fariam parte das barreiras à livre informação antagonizadas por Richard Stallman[26].

O exemplo da disputa entre *software* livre e código aberto aponta para algumas questões sobre as políticas hackers. Primeiro, que hackers têm política e se politizam quando

[25] Seu posicionamento e a criação da *Free Software Foundation*, segundo Coleman & Golub (2008), foram reflexos dos valores de compartilhamento, reciprocidade, ensino e abertura aprendidos com os hackers do MIT.
[26] Evangelista (2010) trata com profundidade a história e os conflitos entre *software* livre e código aberto.

sua existência está em risco, em outras palavras, quando surgem impedimentos à liberdade de escrever e compartilhar código e desenvolver tecnologias, que são as condições materiais e legais de sua existência e associação[27]. Coleman & Golub (2008) argumentam que a discussão sobre liberdade e o que significa ser livre constitui o discurso moral dos hackers. Segundo, e em decorrência, que há uma resistência dos hackers como movimento em incluir na agenda política problemas que não consideram ser essenciais a sua existência, como reivindicações de movimentos sociais e questões de gênero (DELFANTI & SÖDERBERG, 2018).

> *"The importation of political agendas not of their own making can be received as another threat to their autonomy, and is a source of tension between politically minded hackers, on the one hand, and hackers of na avowedly apolitical persuasion, on the other."* (DELFANTI & SÖDERBERG, 2018, p. 463)

Terceiro, e mais importante, que existem múltiplas políticas hackers, muitas vezes em disputa, o que pressupõe que hackers não são um movimento monolítico e que os hackerismos também são múltiplos (COLEMAN & GOLUB, 2008).

2.2 Políticas hackers como objeto de estudo

> "*Technology does not simplistically determine the politics of hacking, even if technological experiences usually inform its expression. Just as there are many ways to hack, there are many ways for hackers to enter the political arena. From policy making to engagements with Pirate Parties, from reinventing the law through free software to performing risky acts of civil disobedience, the geek and hacker are not bound to a single political sentiment, such as libertarianism, and they certainly don't agree on how social change should proceed. What they all have in common is that their political tools, and to a lesser degree their political sensibilities, emerge from the concrete experiences of their craft*." (COLEMAN, 2014, p. 107)

A citação de Coleman (2014) funciona como ponto de partida para a discussão sobre as políticas hackers pois dela transborda apontamentos recorrentes entre os autores do segundo momento dos estudos hackers: a tecnologia não é condição única e suficiente para determinar o caráter das políticas hackers, existem vários caminhos pelos quais entram na arena política e, ainda que existam discordâncias entre hackers sobre ideologias e motivos para o engajamento político, algo em comum entre eles são as ferramentas, táticas e subjetividades políticas que emergem de suas práticas.

---

[27] Isso remete ao conceito de público recursivo (*recursive public*) cunhado por Kelty (2005) e apresentado mais adiante.

As questões levantadas pela literatura consultada trataram tanto da identificação das características e condicionantes do engajamento político (KELTY, 2005; COLEMAN & GOLUB, 2008; SÖDERBERG, 2013; COLEMAN, 2017) quanto dos significados políticos e das limitações do hacking (COLEMAN, 2016; MAXIGAS, 2017; DELFANTI & SÖDERBERG, 2018). É importante mencionar que os estudos sobre políticas hackers apresentam dados etnográficos e reflexões sobre gêneros hackers como se manifestam principalmente nos Estados Unidos. Por isso, conversam diretamente com o hacker propagado por Eric Raymond e situam-se nas intersecções entre liberalismo/libertarianismo e culturas hackers. A exceção é Maxigas (2012; 2017), que trata principalmente dos hackers, *hacklabs* e *hackerspaces* europeus.

Antes destas questões, é necessário apresentar dois conceitos que são debatidos constantemente pelos autores para caracterizar hackers e suas políticas: público recursivo e agnosticismo político.

Público recursivo

O termo público recursivo (*recursive public* no original em inglês) foi cunhado por Christopher Kelty para se referir a grupos sociais específicos cuja característica definidora é ser recursivo, em outras palavras, grupos constituídos pela preocupação compartilhada pelas condições técnicas e legais que possibilitam sua associação e existência[28] (KELTY, 2005, p. 185). Públicos recursivos seriam inerentemente políticos porque se encontram nas encruzilhadas entre tecnologia e política. Quando hackers discutem sobre e por meio da Internet, estão discutindo sobre estruturas técnicas e legais que criam e transforam e que, ao mesmo tempo, são pré-condição da própria discussão. A Internet, portanto, pode ser vista como um produto-efeito das políticas hackers e da qual hackers dependem para continuar a existir como grupo (COLEMAN, 2017). Nesse sentido, Kelty (2005) afirma que o conceito que propõe funciona como um imaginário social específico da Internet:

> *"[...] not only do they argue about these rules by rewriting and reimplementing the core protocols (the 'rules') and core software that give the Internet its structure; they also consider it essential that individuals and groups in society have the right to reimplement privately ordered legal regimes to achieve these ends. These are the*

[28] Kelty (2005) escolhe utilizar o termo "*geek*" e não "hacker" para se referir aos cryptoanarquistas, ativistas de rede, piratas, desenvolvedores de *software*, hacktivistas, e outras subcategorias culturais relacionadas a computadores e Internet para evitar as associações com subversão e criminalidade que normalmente o segundo termo carrega consigo.

> *imaginaries of what giver the Internet its present order or how it should me ordered in the future."* (KELTY, 2005, p. 185)

Dessa forma, as escolhas em relação às tecnologias, técnicas, desenhos, práticas e outros princípios utilizados na criação de *softwares*, protocolos e infraestruturas dão base à ordem moral e social dos hackers e se tornam formas de ordenar o mundo. Dentro os princípios, a abertura é o mais importante para sua recursividade: sem conhecimento e acesso a códigos e protocolos, hackers não conseguem garantir sua associação ou realizar atividades.

Agnosticismo político

O conceito de agnosticismo político é utilizado por Coleman (2004) para se referir à indiferença dos hackers em relação às diferenças ideológicas quando estas podem se tornar um obstáculo ao processo de encontrar a melhor solução para um problema. O agnosticismo político derivaria do *ethos* tecnomeritocrático ao qual os hackers pertencem e é uma atitude pragmática que possibilitaria cooperação entre hackers de diferentes ideologias (SÖDERBERG, 2013).

Em particular, Coleman (2004) se refere ao comportamento hacker observado nas comunidades de *software* livre e código aberto de abraçar a interseccionalidade política e tolerar trabalhar entre linhas ideológicas. Especificamente nessas comunidades, existe um comprometimento em impedir que a liberdade de outros seja limitada para garantir que a circulação de pensamentos não seja restringida durante o desenvolvimento do *software*. Isso porque o "livre" em *software* livre remeteria a uma noção anglo-europeia abrangente sobre direitos de expressão, com base em autonomia individual, desenvolvimento próprio e mercado livre de valor para expressão de ideias (COLEMAN, 2004).

> *"The hacker aesthetic distaste for politics and their free speech codes can only be meaningfully ascertained as 'cultural practice' if placed within the scope of their lived practical and material actions, not just in relation to how their values express or map perfectly onto some existing regime of value such as liberalism; If not, we construe their moral orders as vacuous and thus, decouple their values from a particular way of life and the historical conditions that enable and constrain what they do."* (COLEMAN, 2004, p. 511)

Portanto, ainda que a liberdade defendida pelos hackers seja influenciada por sensibilidades liberais, o seu significado é construído a partir das práticas da programação e do contexto social do uso da Internet, onde se comunicar e criar através do computador tornam-se espaços de liberdade de produção, ensino, sociabilidade e diversão (COLEMAN,

2004). Posicionamentos políticos entre hackers seriam rechaçados porque reivindicações fora da esfera da liberdade poderiam prejudicar a livre circulação de pensamento, expressão e ação, além de criar barreiras para a participação de pessoas (ferindo a transparência garantida pela meritocracia idealizada) e tornar obscuros os processos de decisão, que devem ter base no técnico. No contexto dos projetos ou na defesa das condições de sua existência, os julgamentos pragmáticos seriam mais importantes que os ideológicos (COLEMAN, 2017).

Como hackers vêm de diferentes origens e ideologias, o agnosticismo político é mencionado nos estudos hackers como uma das bases do comportamento cooperativo. Porém, não implica na convivência pacífica fora do contexto e da necessidade de resolver problemas técnicos específicos (SÖDERBERG, 2013). Além disso, como apontam Delfanti & Söderberg (2018), vários dos problemas com os quais os hackers se deparam não seriam vistos por eles como inerentemente políticos, mas como senso comum, como é o caso das restrições criadas por leis de propriedade intelectual, a vigilância massiva e a censura.

Público recursivo e agnosticismo político parecem conceitos contraditórios, uma vez que o primeiro é inerentemente tecnopolítico e o segundo se apresenta como uma não-política, mas os autores consultados para o estudo de escopo não tratam dessa contradição. Alguns comentários podem ser feitos em relação aos motivos.

Como apontado anteriormente, Coleman (2004) desenvolve o conceito a partir da observação das dinâmicas dos hackers em comunidades de *software* livre e código aberto nos Estados Unidos e o situa nesse contexto. O agnosticismo político foi sendo generalizado aos poucos para outras manifestações hackers, passando primeiro por outras também caracterizadas como mais liberais, como os *cypherpunks* e os hackers *underground* (COLEMAN & GOLUB, 2008). A generalização do conceito de agnosticismo político não parece ser problemática para esses autores pelo motivo de que grande parte deles tem como objeto de estudo as mesmas manifestações hackers (ou semelhantes) que Gabriella Coleman ou tratam do mesmo contexto geopolítico, de modo que o agnosticismo político parece ter sido observado também por eles.

Mesmo situando em determinados grupos, comunidades e contextos, o conceito ainda é controverso, uma vez que afirmar que não há política no momento da resolução de problemas técnicos é contrário ao pressuposto da não-neutralidade da tecnologia, em outras palavras, à ideia de que toda tecnologia é política. Nesse sentido, a aceitação da generalização do agnosticismo político como característica hacker pode refletir, também, a percepção que esses autores têm de política. O fato de o agnosticismo político não negar a existência de ideologias ou conflitos entre os hackers, mas funcionar como uma regra tácita quando se torna

necessário priorizar o técnico parece ser satisfatória em muitos dos casos e apenas em Delfanti & Söderberg (2018) foi encontrada a discussão de que a escolha pela não-política é, em si, uma escolha política – na forma do argumento de que a supressão de conflitos ideológicos e a priorização do técnico se conformam como ideologia. As exceções para as generalizações do conceito foram encontradas quando agnosticismo político foi situado no contexto original das comunidades de *software* livre e código aberto (KELTY, 2008) ou não foi mencionado (MAXIGAS, 2012; 2017). Esses autores, junto de Delfanti & Söderberg (2018), parecem entender como políticas não só o engajamento relacionado às ações coletivas e ativismos, mas também as disputas de ordenamento das dinâmicas, escolhas e práticas internas aos grupos e comunidades.

2.2.1 Características e condicionantes das políticas hackers

A discussão sobre políticas hackers desenvolvida por Gabriella Coleman em "*From Internet Farming to Weapons of the Geek*" (2017) parte da migração massiva de hackers de diferentes ideologias para a arena política na última década, de modo que não seria mais possível olhar para essa cultura como se fosse exótica, pois suas políticas se entrelaçam com as políticas de não-hackers. Ao falar desse contexto, Coleman (2017) parece tratar especificamente do ativismo, ou hacktivismo, particularmente conectados com táticas hackers como criação de ferramentas (*softwares*, plataformas e protocolos de compartilhamento de conhecimento e bens culturais), reformulação da legislação, vazamentos, denúncias e ações diretas de hacking e de desobediência civil eletrônica e suporte técnico e serviços para garantir a privacidade de indivíduos, coletivos e ativistas em suas lutas por transformação social.

Ao questionar sobre os condicionantes históricos das políticas hackers, Coleman (2017) identifica uma série de fatores que direcionaram e mobilizaram as políticas de diferentes gêneros hackers ao longo dos anos. Em síntese, os condicionantes seriam ***subjetividades hackers*** e as habilidades para manter e governar tecnologias que possibilitam sua ação e associação, mas o catalizador seria percepção de que o ***público recursivo*** ao qual pertencem está em risco.

Subjetividade hacker, a emergência das sensibilidades políticas

Coleman (2017) identifica três características comuns aos hackers que ajudam a compreender sua inclinação para a ação política:

- Valorização do artifício (*craftiness*): manifesta-se como crítica constante e disposição em investigar profundamente, com intenção de identificar inconsistências, subverter convenções e contornar limitações tecnológicas. A performance do artifício é uma disposição estética que emerge da prática técnica e encontra diferentes expressões entre hackers, como escrever código, quebrar regras, pregar peças e implantar "*easter eggs*" e quebra-cabeças em *softwares*, documentos e manuais. De acordo com Coleman (2017), a maior evidência do valor que hackers atribuem ao artifício é a forma com que o humor se entrelaça com suas práticas e tecnologias;
- Cultivo histórico ao antiautoritarismo: ceticismo direcionado a instituições centralizadoras de poder, muitas vezes registrado em manifestos, zines e outros textos políticos hackers. Especificamente, essa característica exprime a relação dos hackers com regras, normas e leis. Desobediência e subversão, de acordo com Coleman (2017), devem ser entendidas como condição originária dos hackers. Nos anos 1960, as atividades dos *phreaks* pressupunham a quebra de leis federais e estaduais. Mesmo os hackers de universidades, cujas práticas não eram ilegais, contornavam várias regras para acessarem computadores. O teor das respostas das instituições, como perseguições, prisões e punições descabidas, que começaram na década de 1960 e escalaram nos anos 1990, também ajudaram a cimentar o antiautoritarismo, e;
- Coletivismo e comportamento extremamente social: todos os tipos de hacking envolvem formas de entrelaçamento social e convivência online ou física em espaços coletivos. Cooperação, associação, ajuda mútua e construção de comunidades são inerentes a todas experiências hackers. Espaços de sociabilidade (chamados de espaços livres por incorporarem uma lógica de independência) impulsionam o desenvolvimento coletivo de tecnologias e hackers continuamente os criam e habitam. Coleman (2017) cita como exemplo listas de e-mail, *imageboards* (*chans*), repositórios de

> código, projetos de *software* livre, *hackerspaces* e *makerspaces*, *Internet Relay Chat* (IRC) e conferências de hackers e/ou desenvolvedores.

Essas três características da subjetividade hacker reforçariam e reproduziriam hábitos de pensar independente e engendrariam as habilidades necessárias para manter e governar tecnologias que possibilitam ação, associação autônoma e suporte mútuo. Ainda assim, não seriam condição suficiente para o engajamento político dos hackers.

Público recursivo em risco, existência em risco

Ainda que tratem de aspectos e momentos diferentes das políticas hackers, há um consenso entre os autores de que o catalisador do engajamento político dos hackers seria a percepção de que o público recursivo ao qual pertencem está em risco (KELTY, 2005; SÖDERBERG, 2013; COLEMAN, 2017; MAXIGAS, 2017; DELFANTI & SÖDERBERG, 2018).

Portanto, um fator que levaria ao engajamento político dos hackers seria o contexto geopolítico. As políticas hackers carregam consigo especificidades geopolíticas porque as manifestações hackers são situadas. Ainda que exista uma agenda política comum aos hackers, essas estariam mais relacionadas ao público recursivo e ao entendimento compartilhado do ser hacker como movimento. As sensibilidades políticas, entre os hackers, costumam espelhar padrões políticos regionais ou dominantes (MAXIGAS, 2012; COLEMAN, 2017). Ademais, historicamente, hackers se engajam politicamente em resposta a agressões dos governos e corporações direcionadas aos próprios hackers e às suas tecnologias e práticas, que dependem das especificidades das leis federais e estaduais e das percepções socioculturais e institucionais sobre propriedade intelectual, vigilância e privacidade.

As primeiras prisões de hackers aconteceram em 1961, com os *phreaks*. Nas décadas de 1980 e 1990, em que hackers invadiam computadores e roubavam códigos-fonte e outras informações, normalmente sem fins lucrativos, as acusações e sentenças começaram a exceder em muito os crimes cometidos. Um dos casos mais conhecidos foi de Kevin Mitnik, perseguido e preso por dois anos enquanto esperava julgamento, sendo oito meses em isolamento. A justificativa da promotoria para os excessos ilustrou desconhecimento sobre atividades hackers: as autoridades acreditavam que Mitnik seria capaz de começar uma guerra nuclear se tivesse acesso aos telefones públicos (COLEMAN & GOLUB, 2008). Um dos exemplos mais recentes foi de Aaron Swartz, ativista da liberdade na Internet, sentenciado a

trinta e cinco anos de prisão e ao pagamento de US$1 milhão em multas pelo *download* de milhões artigos acadêmicos do repositório JSTOR através dos computadores do MIT. Swartz acreditava que o conhecimento gerado nas universidades públicas e financiado pelo governo estadunidense deveria ser público e de acesso aberto e gratuito[29]. Portanto, haveria entre os hackers a consciência compartilhada de que sua história como movimento é repleta de casos em que sua existência é desafiada por forças maiores a eles mesmos (COLEMAN, 2017).

Sobre a última década, Coleman (2017) argumenta que grandes acontecimentos críticos como os Wikileaks, a intensificação da ação dos Anonymous, os vazamentos de Edward Snowden sobre os programas de vigilância da Agência Nacional de Segurança estadunidense e sua luta pela privacidade serviram como modelos de ação política e gatilho para o engajamento dos hackers. A violência da retribuição das autoridades àqueles que expuseram segredos de estado ou criaram ferramentas para tal, como Julian Assange, Chelsea Manning, Aaron Swartz e o próprio Snowden teriam impulsionado os hackers a estenderem a agenda de privacidade, segurança e autonomia para além do público recursivo em direção à sociedade civil como um todo. De acordo com a fala de Gabriella Coleman na Escola Doutoral, essa seria a novidade da onda mais recente de politização hacker: as políticas hackers estão acontecendo em resposta a problemas de não-hackers, que também estão sofrendo agressões e intervenções de governos e corporações e compartilhando de pautas sobre privacidade e autonomia.

Por fim, a agenda política comum entre os hackers mencionada anteriormente é aquela das liberdades civis. Liberdade, da forma que é construída e performada dentro das comunidades hackers emerge das práticas. A liberdade individual de criar, usar e distribuir *software* permitiria que outros pudessem igualmente criar, usar e distribuir e seria garantida por documentação e compartilhamento, de forma que o código acaba por ser tornar universal. Nesse sentido, Coleman (2004) argumenta que escrever código se torna uma forma de discurso e a liberdade em escrever código se equipara à liberdade de expressão.

Quando as liberdades civis são desafiadas ou restringidas, hackers se mobilizam porque são delas que emana o compromisso compartilhado em preservar a autonomia dos indivíduos em pensar, agir e ser e tomam forma das agendas de privacidade, liberdade de expressão (escrever e distribuir código) e liberdade de informação:

[29] Aaron Swartz foi encontrado morto enforcado em seu apartamento em 2013 aos vinte e seis anos, dois dias após ter rejeitado o acordo proposto pela promotoria estadunidense – que exigia que Swartz se declarasse culpado por treze crimes de fraude eletrônica – para obrigá-los a justificar os motivos da perseguição exagerada.

> "*Hackers both fight for alternative notions of the law and insist on the realization of the cherished legal principles that they believe have been corrupted. One class of legal precepts in particular, those of civil liberties – privacy and free speech – have settled so deeply into the cultural and technical sinews of hacking that much of their advocacy is almost inseparable from the idea of hacker itself*." (Coleman, 2017, p. S97)

Ainda que as liberdades civis façam parte de uma agenda política comum, o espaço que ocupam nos movimentos e os objetivos pelos quais são perseguidas são diferentes entre os hackers e determinam se suas políticas são consideradas liberais ou radicais (COLEMAN, 2017).

As políticas liberais

As políticas liberais têm intersecções com preceitos liberais e libertários e entendem as liberdades civis como condição essencial dos direitos individuais, dos direito de expressão, da autonomia, do acesso e da participação política. Alguns dos exemplos de políticas hackers liberais seriam os Partidos Piratas, o movimento por direitos digitais e sua luta para que os direitos de liberdade de expressão fossem aplicados a escrever, lançar e compartilhar código, e o hacking cívico. A agenda política deste último, em particular, envolve o desenvolvimento de ferramentas que solucionem problemas inerentes à ordem política estabelecida, como serviços locais ou transparência governamental, e fazem parte da ação política de hackers dos mais variados comprometimentos ideológicos.

No contexto estadunidense, onde prevalecem os hackers de políticas mais liberais, Coleman & Golub (2008) argumentam que a discussão sobre liberdade e o que significa ser livre constitui o discurso moral dos hackers, principalmente em intersecções com liberdade de expressão, meritocracia, privacidade, autonomia e poder do indivíduo, e se articula com diferentes éticas hackers, de forma que o liberalismo se torna um contexto importante no qual hackers entendem a si mesmos e ao mundo e justificam suas práticas.

Para ilustrar como mesmo dentro das políticas liberais os objetivos são múltiplos, Coleman & Golub (2008) discutem três gêneros morais hackers e suas políticas: *cypherpunks* e a política da tecnologia; *software* livre e de código aberto e a política de inversão; e hacker *underground* e a política de transgressão.

Quanto ao primeiro, a origem da criptografia pode ser traçada até 1975 no MIT, com o desenvolvimento de uma chave-pública para encriptação, que possibilitou o envio de informações de forma segura por canais inseguros. As ferramentas de encriptação, até então,

eram utilizadas principalmente por grandes corporações para assegurar transações financeiras, cada vez mais dependentes dos computadores. O desenvolvimento e difusão da criptografia para computadores pessoais eram impedidos por patentes.

O primeiro método de criptografia para uso em computadores pessoais foi desenvolvido em 1991 por um criptógrafo amador que queria garantir que todos tivessem controle sobre sua própria privacidade, até então, direito reservado apenas aos governos e grandes corporações. A criptografia, portanto, chega ao público articulada com valores liberais de autonomia individual e liberdade em relação à intervenção governamental no dia-a-dia. O simples desenvolvimento da ferramenta foi um ato de desobediência civil em relação tanto à propriedade intelectual das ferramentas de criptografia quanto às leis de segurança nacional (COLEMAN & GOLUB, 2008). Os denominados *cypherpunks* tomaram corpo como gênero hacker por listas de e-mail e reuniões presenciais na Califórnia em 1992, que contavam com hackers, programadores e ativistas de direitos civis. Suas atividades – criação e manutenção de tecnologias de criptografia contra leis que cerceavam a privacidade dos indivíduos – foram uma resposta tecnopolítica às ameaças à privacidade.

Ao contrário dos *cypherpunks*, o gênero hacker relacionado ao *software* livre trabalha em conformidade com a lei. Nesse sentido, quando Richard Stallman cria a GNU *Public License* para garantir que *softwares* sejam livremente distribuídos no futuro, sua base são os ideais liberais de liberdade de expressão e compartilhamento.

> "*Through the GPL Stallman used copyright not to enforce a monopoly of his right as an author, but to ensure that software was unable to be monopolized. The result was the creation of a 'safe zone' of publicly available code that could not be privatized by corporate interests, a sort of open space in which Stallman's dream hacker community could work in freedom.*" (COLEMAN & GOLUB, 2008, p. 261).

Dessa forma, o *software* livre e a *GNU Public Licence* utilizaram da lei de direitos autorais para invertê-la. Para Coleman & Golub (2008), o movimento do código aberto também faz parte desse gênero por sua preocupação com o acesso à informação, ainda que a mensagem por trás da necessidade de adoção de um modelo de desenvolvimento aberto seja a busca por eficiência. Tanto o *software* livre quanto o código aberto, porém, fazem parte do mesmo público recursivo (SÖDERBERG, 2013): são caracterizados por uma intensa sociabilidade entre os hackers, que se agregam em comunidades para garantir a difusão, uso e reprodutibilidade do código. Repositórios, chats e listas de e-mail tornam-se espaços que facilitam o trabalho hacker e garantem um público com conhecimento técnico para dar apoio e apreciar os produtos (COLEMAN & GOLUB, 2008).

Por fim, os hackers *underground*, com origem nos *phreaks* dos anos 1960, veem o hackerismo como uma corrida armada entre aqueles com conhecimento e poder para criar barreiras e aqueles com ferramentas equivalentes para destruí-las. Nesse sentido, ideais como total acesso à informação e direito à privacidade seriam inalcançáveis, pois sempre são criadas ferramentas e barreiras para impedi-los de se realizar.

Neste gênero hacker, segundo Coleman & Golub (2008), a prática valorizada é o processo de circunvenção e transgressão. Como as ações são ilícitas, quando hackers *underground* reivindicam para si a glória da conquista, identificam-se apenas por apelidos. A segurança necessária para as práticas de transgressão tornaria esses hackers mais solitários e mais interessados em defender ideais como autonomia. Ao mesmo tempo, o caráter ilícito das atividades e a força desproporcional que os governos e grandes corporações despendem para identificar e punir os hackers *underground* impulsionaram sua organização política, de forma que à política de transgressão foram somadas outras formas de ação mais tradicionais e públicas, como protestos, marchas, editoriais, documentários e conferências. Os hackers *underground* têm intersecções com os indivíduos que Raymond (1996, revisão 1.51 out. 2017) denomina como *crackers* e exclui da comunidade hacker.

As políticas radicais

As políticas radicais entendem que liberdades civis são porta de entrada para projetos mais robustos voltados à luta por igualdade e justiça. Particularmente, a desobediência civil eletrônica congrega um conjunto de táticas conectadas às políticas hackers[30]. Como comenta Wray (1999) – ao falar da previsão do *Critical Art Ensemble* sobre futuras táticas de movimentos sociais para mostrar dissidência política e chamar atenção das autoridades e da sociedade civil para certos problemas – assim como o capitalismo se tornava mais nômade, disperso e eletrônico, as resistências também deveriam se transformar em nômades, dispersas e eletrônicas. Consequência da crescente informatização dos ativistas e politização dos hackers, a desobediência civil eletrônica seguiria os mesmos preceitos da desobediência civil tradicional, mas o lócus de ação seria o ciberespaço:

[30] A fusão entre tecnologias da informação com formas tradicionais de desobediência civil é chamada de desobediência civil eletrônica. O termo é emprestado do livro de 1996 "*Eletronic Civil Disobedience and Other Unpopular Ideas*" do *Critial Art Ensemble*, que por sua vez retoma o termo "desobediência civil" de Henry David Thoreau (WRAY, 1999).

> *"Just as the Vietnam War and the Gulf War brought thousands into the streets to disrupt the flow of normal business and governance, acting upon the physical infrastructure; future interventionist wars will be protested by the clogging or actual rupture of fiber optic cables and ISDN lines, acting upon the electronic and communications infrastructure. Just as massive non-violent civil disobedience has been used to shut down or suspend governmental or corporate operations, massive non-violent e-mail assaults will shut down government or corporate computer servers. Where a typical civil disobedience tactic has been for a group of people to physically blockade, with their bodies, ECD will utilize virtual blockades and virtual sit-ins."* (WRAY, 1999, p. 108-109)

A desobediência civil eletrônica de fato tomou força com o movimento global pró-levante zapatista e com as atividades do *Eletronic Disturbance Theater* na segunda metade dos anos 1990. Um exemplo mais recente, de acordo com Coleman (2014; 2017), seria os Anonymous.

Nascido dos fóruns do 4chan, *imageboard* conhecido pelo anonimato, liberdade de expressão e legiões de *trolls*, os Anonymous começou a surgir como movimento com a mobilização massiva em protestos de rua, brincadeiras online e ataques distribuídos de negação de serviço (DDoS) contra a Igreja da Cientologia em 2008[31] como forma de expressar seu descontentamento em relação à centralização, autoritarismo e censura.

> *"The story began with a group of 'trolls' hanging out on the infamous Internet forum 4chan. They were brought together by a tasteless sense of humor and the satisfaction of having a laugh at someone else's expense. This is captured in the term 'lulz', used as shorthand for 'laughing out loud'. The attitude seems to be entirely devoid of politics, but it presupposes at least one heartfelt commitment from the people involved: an absolutist stance on free speech. Although limited as far as a political analysis goes, that conviction gave them the impetus to direct their pranks against targets with political clout. The reactions provoked new pranks and, at least for some of them, led to a more serious engagement with the various issues at stake."* (SÖDERBERG, 2017, p. 971)

Assim como outras vertentes do movimento hacker, os Anonymous congregam uma miríade de relações e indivíduos de diferentes origens que nem sempre estão em concordância com os termos das ações, mas um aspecto específico do movimento é a centralidade do anonimato como ferramenta de ação política.

De acordo com Coleman (2014), o passo para o ativismo foi dado com a *Operation: Payback*, em que o Anonymous mobilizou uma campanha de ataques de DDoS em retaliação a organizações, bancos e sistemas de pagamento como a Amazon, MasterCard e

[31] O surgimento e as atividades dos Anonymous são extensivamente tratados no documentário "*We Are Legion"* (2014) e em no livro "*Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of* Anonymous" de Gabriella Coleman (2014).

PayPayl que se recusaram a prover serviços de hospedagem e processar doações ao Wikileaks depois do vazamento de documentos diplomáticos do governo estadunidense em 2010.

Operation: Payback trouxe diversas questões sobre a condução das ações para discussão nos Anonymous, principalmente em relação à organização e táticas. Durante a execução da operação, os Partidos Piratas do Reino Unido e Estados Unidos escreveram uma carta ao AnonOps[32] pedindo o fim dos ataques de DDoS da *Operation: Payback* porque a ilegalidade das táticas utilizadas feria os esforços daqueles interessados em reformar as leis de direitos autorais por meios legais, promovendo o comportamento criminoso e justificando a formulação de leis mais duras contra a liberdade de expressão e a criatividade.

A resposta do AnonOps, depois de muita deliberação, ajudou a cimentar o posicionamento político do coletivo em relação aos seus interesses e táticas: ainda que compartilhem valores com os Partidos Piratas em relação à liberdade de informação e expressão, a preocupação dos Anonymous era a legitimidade, não a legalidade. Isso porque aqueles que fazem e aplicam as leis são os mesmos favoráveis tanto a ataques de DDoS aos sites que vão contra seus interesses quanto a operações massivas de extorsão por organizações que impõem direitos autorais, assediam a população e violam liberdades civis (COLEMAN, 2014).

A partir de então, o AnonOps tornou a tomada de decisões um processo mais deliberativo e coletivo e assumiu a desobediência civil eletrônica como molde para suas atividades – desfiguração de sites, vazamentos de dados e outras táticas ilegais e controversas sempre tornadas públicas e com autoria assumida para reforçar a dissidência política na Internet. Para Söderberg (2017), o posicionamento radical dos Anonymous em relação à liberdade de expressão abriu o coletivo para interações com movimentos sociais tradicionais e promoveu trocas: os hackers foram expostos a novas ideias e arcabouços teóricos pelo contato com os ativistas que, por sua vez, aprenderam novas ferramentas e táticas de luta.

Ainda dentro das políticas radicais, algumas políticas hackers posicionam-se contra o liberalismo e o capitalismo. Coleman (2017) dá como exemplo a Indymedia, iniciativa de mídia alternativa que desenvolveu toda uma infraestrutura e gerência alternativa de conteúdos que possibilitou incorporar vídeos e fotos as suas notícias online e criou uma rede de hackers que tomaram a frente dos movimentos antiglobalização. A infraestrutura criada pela Indymedia era constituída por provedores independentes de serviços de Internet organizados com base em consenso e princípios anarquistas. Um dos desdobramentos mais

[32] O AnonOps é o *Internet Relay Chat* (IRC) dos Anonymous utilizado para discussão livre.

conhecidos é o Riseup, formado por alguns dos fundadores do Indymedia e provedor de serviços cuja principal base de usuários são especialistas em tecnologia da informação e organizações de esquerda cuja agenda política inclui problemas tecnológicos.

Determinismo tecnológico e a ação coletiva dos hackers

Johan Söderberg, em "*Determining social change: The role of technological determinism in the collective action framing of hackers*" (2013), discute a existência de uma polarização nos estudos hackers entre autores que criticam os hackerismos porque os percebem como ferramentas da globalização neoliberal cada vez mais cooptadas por governos, grandes corporações e organismos internacionais, e outros que exaltam hackers como vanguarda tecnológica e inovativa, colocando-os como solução para as economias das sociedades capitalistas. A conclusão em comum destas duas visões é a de que hackers, partindo de uma compreensão senso comum, liberal ou libertária de mundo, entendem que a mudança social depende do desenvolvimento tecnológico. Sob essa perspectiva, para os hackers, tecnologias se desenvolveriam a partir de lógicas próprias exógenas à sociedade e moldariam a sociedade em seus padrões quando introduzidas. Em decorrência, acadêmicos deduzem que os hackers, por serem tecnologicamente deterministas, são avessos ao engajamento político uma vez que a tecnofilia inevitavelmente superaria o potencial emancipatório do hackerismo. Söderberg (2013) argumenta que a tensão entre determinismo tecnológico e ação coletiva é uma das características da ciberpolítica.

Söderberg (2013) esclarece que não pretende abranger todas as possibilidades de políticas dos hackers, mas que conversa diretamente com o estereótipo de hacker libertário e apolítico propagado por Eric Raymond, que costuma ser entendido como principal exemplo da relação entre determinismo tecnológico e hackers. O autor argumenta que a comunidade acadêmica não deve ignorar esse estereótipo ao tratar de políticas hackers porque mesmo em suas práticas e ética tecnologicamente determinista existe engajamento político. Delfanti & Söderberg (2018), posteriormente, reforçam essa ideia sugerindo que o pragmatismo, a visão orientada para resolução de problemas e a supressão de conflitos ideológicos são uma ideologia em si e compõem uma narrativa abrangente dos hackers.

A sociedade da informação é atraente aos hackers por poder ser invocada quando disputam questões sobre propriedade intelectual, vigilância e censura. É nesse contexto em que, de acordo com Söderberg (2013), os hackers constroem as narrativas de interpretação do mundo que dão significado a sua luta, que é constantemente criada, disputada e transformada.

Nessa narrativa, o desenvolvimento de uma sociedade da informação não apontaria para a ascensão de governos tecnocráticos e mercados globais, mas para tomada de decisões entre pares, economia digital da dádiva e o fim dos monopólios de propriedade intelectual. Se a informação é livre e reprodutível, a legislação de propriedade intelectual é obsoleta. A ideia de novidade, criatividade e abertura são reivindicados e apropriados pelos hackers e, em suas mãos, os adversários passam a ser os defensores da propriedade intelectual e monopólios que se tornam barreira para um mundo globalizado e para livre fluxo de informações.

Questões tecnologicamente deterministas nas práticas e políticas hackers são evidenciadas com Eric Raymond em "A Catedral e o Bazar" (1999). O modelo bazar de desenvolvimento suplantaria o modelo catedral porque mobilizar uma comunidade de hackers para resolução de problemas seria evolutivamente superior em termos de eficiência técnica e econômica. De acordo com Söderberg (2013), no contexto da sociedade da informação, a principal contribuição de Raymond (1999) foi situar a comunidade hacker no centro da Ideologia Californiana (BARBROOK & CAMERON, 1996), que uniu utopismo tecnológico com pregação sobre o livre mercado, e na retomada dos conceitos de produção em rede: "*From then onwards, free and open source software development has invariably been the cornerstone in any argument about the rise of a networked mode of production*." (SÖDERBERG, 2013, p.1284).

A resistência acadêmica em tratar das relações entre determinismo tecnológico e engajamento político seria justificada pelo fato do primeiro ser utilizado como argumento para aliviar conflitos do trabalho, além justificar decisões impopulares e processos de decisão pouco democráticos sobre desenho de tecnologias (SÖDERBERG, 2013).

Aspectos luditas do hackerismo

Maxigas (2017) utiliza a expressão "aspectos luditas do hackerismo" para se referir às práticas de resistência dos hackers de crítica e recuperação em ciclos tecnológicos, mais especificamente, em atos contra a recuperação da Internet pelo capital e a restrição ao anonimato. Especificamente, Maxigas (2017) procura essas resistências em casos de hackers que combatem o progresso tecnológico – o que parece contraditório à preconcepção de que esses atores são entusiastas acríticos de novas tecnologias e os primeiros a adotá-las – e as encontra em um grupo de homens brancos de meia idade, extremamente qualificados, profissionais de tecnologia e moradores de centros urbanos membros de um *hackerspace*

europeu. Essa população é denominada por Maxigas (2017) de "usuários sofisticados" e escolhida como objeto de pesquisa por sua reflexividade e identificação com a tecnologia, portanto, por compor o público recursivo dos hackers.

Os aspectos luditas do hackerismo emergem de escolhas de adoção ou não-adoção, que dependem das preferências tecnológicas e se manifesta quando questões éticas ou estéticas são mais importantes para os hackers que a funcionalidade e o avanço tecnológico (DELFANTI & SÖDERBERG, 2018), de forma que a não adoção de interfaces, extensões de navegador e novas gerações de dispositivos móveis funcionam como posicionamento político. Para Maxigas (2017), a não-adoção por usuários sofisticados teria um significado político maior do que a não-adoção pelo público geral porque, quando um grupo de usuários que normalmente participa das escolhas na criação de tecnologias não adota uma tecnologia ou funcionalidade, uma das consequências pode ser a exploração de caminhos alternativos de desenvolvimento tecnológico.

A partir do exemplo da não-adoção de uma extensão de navegador, Maxigas (2017) escreve:

> *"Even though their equipment is configured to 'break' certain websites on their end of the screen, at the outset the hackers are startled and they will say so; after looking into the matter they make it clear that the website is at fault.[...] Yes, they know that the website was supposed to work by the browser pulling it together from multiple sources. Indeed, they know that the website works well for users who do not take special precautions againt these mainstream industry practices; but that is exactly where the problem lies, they will tell you. In other words, the particular website is not buggy or broken according to the technological ideals – and technological practices – of the website makers, or even most of the website users. It is buggy and broken – or more precisely it becomes buggy and broken on the hackers' screen – according to the technological ideals of these particular users."* (MAXIGAS, 2017, pp. 848-849).

Maxigas argumentou durante a Escola Doutoral que trazer a perspectiva sobre tecnologia dos usuários sofisticados contribuiriam muito mais para os ESCT. Quando o autor apontou ser esta a principal contribuição de sua pesquisa, pareceu dialogar diretamente com parte da literatura dos ESCT que trata de resistências tecnológicas (AKRICH, 1992; PFAFFENBERG, 1992; FEENBERG, 2016). No caso destes autores, a resistência tecnológica parte de usuários normalmente excluídos dos processos de decisão do desenho tecnológico e se configura como manifestações de disputas entre diferentes interesses e visões de mundo. Nesse sentido, quando Pfaffenberg (1992) argumenta que grupos ou indivíduos que participam do desenho de uma tecnologia são capazes de dar significado ou implementar coercitivamente uma visão construída de sociedade, que surge de forma recíproca e recursiva

em interação com o processo de desenho da tecnologia, as resistências tecnológicas se configuram como enfrentamento às formas de controle, ordenamento e exclusão.

A participação em processos decisórios sobre desenho tecnológico, porém, são parte do público recursivo ao qual pertencem os usuários sofisticados de Maxigas. Ainda assim, há uma disputa de reordenamento das tecnologias da informação, uma vez que os desenhos tecnológicos implementados não são aqueles ideais para esses usuários. A diferença em relação a outros usuários, porém, seria que as exclusões e os contratempos da não-adoção das tecnologias partem da escolha desses atores e não processo de implementação de conjuntos de tecnologias intrinsecamente excludentes. É por esse motivo que o autor argumenta que estudar resistência tecnológica sob a perspectiva dos usuários sofisticados traz mais contribuições para os ESCT – porque são esses os atores capazes de ir contra os desdobramos do progresso técnico digital, uma vez que compartilham valores e possuem expertise técnica e consciência história em relação à cultura hacker, portanto, a memória de quando a Internet ainda não havia sido cooptada pelo capitalismo. Este argumento, porém, soa como uma defesa do caráter excludente das comunidades de usuários sofisticados, legitimando a exclusão de outros usuários dos processos de decisão sobre desenhos tecnológicos da Internet, cujas contribuições seriam, desse ponto de vista, pouco relevantes.

2.4 Limites das políticas hackers

A adoção, adaptação e reaproveitamento de discursos, práticas e inovações hackers por corporações e instituições seriam parte do significado político e das limitações do hacking.

> *"[...] by teasing out hacker claims about having a proative approach to technology, rebelling against epistemic hierarchies, disrupting estabilished codes of knowledge, and so on, we develop a critique of hackers immanent to their own justifications and interpretative frameworks. From such a perspective we can see that it is not only individual technologies that are regularly being repurposed. It is repurposing as such, as a mode of engaging wiith the world, and not only with technologies, that has been adopted and cultivated by institutional and corporate actors."* (DELFANTI & SÖDERBERG, 2018, p. 461).

De acordo com Delfanti & Söderberg (2018), é possível encontrar diversos exemplos de práticas e tecnologias hackers que, se um dia consideradas subversivas, foram apropriadas pela cultura da inovação de corporações e instituições.

Esse processo aconteceria por dois motivos. Primeiro, porque as atividades hackers normalmente envolvem associações com atores institucionais e industriais mais poderosos e com diferentes valores e objetivos. Esse processo, denominado recuperação pelos autores, é marcado por uma contradição: a subversão dos objetivos hackers por outros atores garante que sejam realizados. Segundo, porque é característica do capitalismo como sistema absorver culturas e práticas críticas, cooptando-as e as absorvendo para seus fins (GRENZFURTHNER & SCHNEIDER, 2009; DELFANTI & SÖDERBERG, 2018). Nesse sentido, pensar em casos de crítica e recuperação, de acordo com Maxigas (2017), permite compreender como funciona a dinâmica de inovação no capitalismo informacional.

A recuperação é um movimento cíclico. Delfanti & Söderberg (2018) afirmam que hackers continuam a desenvolver tecnologias e práticas subversivas e passam por ondas de repolitização, resistência à cooptação e absorção. Especificamente em relação à mobilização hacker da última década, Coleman (2017) aponta que os riscos à despolitização hackers seriam a cooptação das sensibilidades e projetos hackers pelo empreendedorismo do Vale do Silício, a apropriação de práticas hackers – como os hackatons – para fins corporativos e o incentivo a individualização, profissionalização e carreirismo do trabalho hacker.

Delfanti & Söderberg (2018) situam seu trabalho em um corpo nascente de conhecimento sobre hackers que busca sair da promessa emancipatória comum aos estudos de caso para capturar movimentos de médio e longo prazo. A partir disso, concluem que hackers, como objeto de pesquisa, e os ciclos de recuperação podem ser analisados a partir de três perspectivas temporais:

- Incorporação de uma única tecnologia ou comunidade: como tecnologias desenvolvidas por hackers encontram espaço em aplicações comerciais ou são desenvolvidos em conjunto com a indústria, a recuperação toma forma de cooptação tecnológica e a unidade de tempo corresponde ao ciclo de vida de um projeto ou comunidade. Os conflitos normalmente ocorrem porque a tecnologia sofre transformações para se adequar ao mercado e se afasta dos valores e objetivos atribuídos a elas pelos hackers. Uma das formas com que hackers resistem à recuperação é através da recusa em adotar versões atualizadas de tecnologias ou serviços (MAXIGAS, 2017);
- Evolução dos hackers como movimento: relaciona aspectos do desenvolvimento de culturas hackers com momentos históricos específicos ou a coevolução entre o movimento hacker e uma indústria ou instituição

como o Estado ou Exército. Neste último caso, a unidade de tempo equivale à expansão da indústria ou instituição em decorrência da interação com os hackers até o momento em que a resistência à incorporação ou obrigações recíprocas se tornam um limite ao crescimento. Exemplos seriam a trajetória política dos *hackerspaces* e as narrativas desenvolvidas em Levy (1984), que relaciona especificidades de gêneros hackers com o contexto das décadas de 1960, 1970 e 1980, e;

- Evolução do espírito do capitalismo: partindo da ideia de que o capitalismo se alimenta de culturas críticas ao seu funcionamento, a unidade temporal equivale ao capitalismo como um todo em sua relação com os hackers. Nesse sentido, o capitalismo não só absorve práticas hackers, como as utiliza para reinventar sua própria infraestrutura, principalmente em relação ao trabalho e produção. É o caso de práticas organizacionais e formas abertas de acumulação, como *open innovation*, trabalho colaborativo e plataformas para produção distribuída e compartilhamento.

Delfanti & Söderberg (2018) recuperam o conceito de público recursivo para afirmar que hackers lutam contra a recuperação – entrando em conflito com corporações e instituições sobre propriedade, significado e uso de tecnologias que desenvolveram ou estratégias corporativas integradoras – para proteger as pré-condições de sua existência, como sua autonomia e autodeterminação.

A questão da cooptação das práticas e dinâmicas hackers foi amplamente discutida na Escola Doutoral, mas de formas diferentes em espaços diferentes. Quando a questão era levantada por palestrantes como Gabriella Coleman e Maxigas, discutia-se a cooptação do trabalho hacker pelo capitalismo, principalmente porque hackear dificilmente é uma ocupação em si, mas uma atividade secundária feita nos intervalos dos empregos formais dos hackers. Se não há tempo para hackear ou se o trabalho hacker é incorporado ao sistema produtivo, resistência e subversão desaparecem.

Porém, quando a questão era levantada pelos alunos e técnicos ali presentes, a preocupação se voltava à cooptação do trabalho hacker pelo governo. Após o escândalo dos instrumentos de vigilância massiva da NSA, instituições governamentais começaram a empregar mais hackers tanto para descobrir falhas nos sistemas governamentais quanto para encontrar novas ferramentas para hackear a sociedade civil. Um dos principais assuntos foi o Hacking Team, empresa de tecnologia da informação com base na Itália que vende

ferramentas de invasão e vigilância (para monitoramento de conversas e e-mails, de-encriptação, filmagem e gravação) para governos, forças policiais e corporações. O interessante das discussões era o confronto com as definições existentes sobre hackers: as práticas eram de hacking, mas o comportamento não era subversivo. Esses hackers, para os alunos e especialistas, vendiam-se para o maior dos inimigos, o Estado, ajudando a reforçar o autoritarismo contemporâneo na forma da vigilância e assédio à privacidade. Portanto, por essa perspectiva, foi possível notar que na Escola Doutoral prevalecia uma percepção de hacker semelhante àquela do início desta pesquisa – de indivíduos subversivos e focados em defender a liberdade e a autonomia, representantes de um movimento de não-aceitação da condição de caixa-preta das tecnologias –, mas essa percepção estava entrando em choque a partir da observação deste ciclo específico de recuperação: a cooptação do trabalho hacker pelo Estado, agências de segurança e grandes corporações.

A cooptação do trabalho e das ferramentas hackers para opressão e violência não é uma questão tratada no artigo de Delfanti & Söderberg (2018), que se foca principalmente em questões de trabalho e produção[33].

2.5 *Hacklabs*, *hackerspaces*, política e socialização hacker

Trazer o exemplo dos *hacklabs* e *hackerspaces* se torna interessante porque o ciclo de recuperação dessas manifestações hackers tem sido explorado pela literatura dos estudos hackers de diferentes formas através da crítica ao processo de despolitização dos *hacklabs* e a exaltação do potencial inovativo dos *hackerspaces*. A disputa entre *hacklabs* e os *hackerspaces* ajuda a exemplificar não só um movimento de recuperação de práticas e tecnologias hackers, mas também uma das formas como a antiga disputa entre ideais do *software* livre e do código aberto se dá na prática (SÖDERBERG, 2013), além de levantar questionamentos sobre outros tipos de políticas que permeiam os debates entre hackers e evidenciar como pesquisadores estão abordando essa temática. Essa literatura foi explorada principalmente no início da trajetória de pesquisa e se conformou como um caso interessante para retratar e entender arcabouço analítico proposto pelos autores do segundo momento dos estudos hackers.

[33] No momento da Escola Doutoral, as controvérsias sobre o envolvimento de hackers na campanha das eleições presidenciais de 2016 nos Estados Unidos ainda não estavam em discussão. As conversas informais sobre hackers trabalhando para governos poderiam ter dominado as discussões caso a Escola Doutoral tivesse acontecido alguns meses depois.

Os hackers, além de compartilhar das práticas de outros artesãos de promover reuniões para aprender, ensinar e estabelecer diretrizes para colaboração e criação, também construíram espaços de socialização análogo às oficinas. Listas de e-mail, repositórios de códigos, projetos de *software* livre, *hackerspaces*, e *makerspaces* e chats de Internet são espaços onde as comunidades se conformam para discutir valores essenciais às suas práticas e os hackers podem forjar suas identidades e trabalhar de forma semiautônoma (SCHROCK, 2014) e independente das instituições nas quais trabalham por salários (COLEMAN, 2016).

Coleman (2016) enfatiza, porém, que a existência de espaços de socialização não é condição suficiente para que os hackers se engajem politicamente. Ao contrário, o ativismo político de hackers estaria relacionado às escolhas individuais e à história do surgimento desses espaços em diferentes regiões. Ainda que mesmo dentro do mesmo território os espaços de socialização possam ter posicionamentos conflitantes, normalmente considera-se que as atividades e espaços hackers europeus sejam baseados em posicionamentos políticos explícitos e ativismo, enquanto os estadunidenses costumam ser associados à cultura do empreendedorismo de mercado (FONSECA, 2014; COLEMAN, 2016).

Ainda assim, os espaços de socialização de hackers são múltiplos em seus objetivos e formas de organização e *hacklabs* e *hackerspaces* são duas dessas formas. A importância de falar de *hacklabs* ao tratar de *hackerspaces* está no fato de que atualmente os termos são muitas vezes usados como sinônimos. Partindo do contexto europeu, Maxigas (2012) esclarece que apesar de compartilharem a mesma herança cultural, alguns de seus condicionantes ideológicos e históricos são diferentes.

As descrições aqui apresentadas partem de uma literatura europeia e estadunidense, tendo como base os autores considerados referências no tema. Dessa forma, ainda que *hacklabs* e *hackerspaces* tenham elementos que os caracterizem e diferenciem, as experiências das quais os autores partem são específicas dessas regiões, onde esses espaços apareceram pela primeira vez.

Os *hacklabs* começam a aparecer no cenário europeu na década de 1990 num contexto em que as pessoas tinham pouco ou nenhum acesso à Internet e aos computadores pessoais e em que o uso de computadores e *softwares* livres não eram triviais.

> *"Hacklabs are, mostly, voluntary-run spaces providing free public access to computers and internet. They generally make use of reclaimed and recycled machines running GNU/Linux, and alongside providing computer access, most hacklabs run workshops in a range of topics from basic computer use and installing GNU/Linux software, to programming, electronics, and independent (or pirate) radio broadcast."* (MAXIGAS, 2012)

De forma geral, seu surgimento foi marcado pela interconexão entre duas tendências. De um lado, das ocupações autônomas e anarquistas (*squats*, no original em inglês), incorporadas no cotidiano urbano, que demandavam infraestruturas de comunicação como acesso à Internet e acesso público a terminais. Do outro, dos ativistas de mídia enraizados em comunidades locais que demandavam espaços para reunião, produção, ensino e aprendizado e frequentemente se organizavam em torno de tecnologias como rádios piratas ou comunitárias, de publicações independentes e do computador pessoal. Associados aos movimentos europeus mais amplos contra o capitalismo neoliberal e buscando alternativas à falta de acesso às infraestruturas de comunicação mais modernas, os *hacklabs* adotaram redes de computadores e tecnologias midiáticas para uso comunitário e fins políticos e contribuíram muito para a área de acesso e tecnologias de rede.

Os *hackerspaces* se diferenciam dos *hacklabs* em termos de concepção, organização, materialidade e visão de mundo. Os *hackerspaces* são espaços organizados por hackers para hackers com o objetivo de dar suporte à atividade hacker (MAXIGAS, 2012): são coordenados por uma comunidade onde pessoas se encontram para compartilhar seus interesses e conhecimentos sobre mexer e transformar tecnologias e trabalhar em seus projetos.

Com origem no fim da década de 1990, os *hackerspaces* começaram a se proliferar em 2007, quando hackers estadunidenses, através do projeto *Hackers on a Plane*, foram para o Congresso do *Chaos Computer Club*, *hackerspace* alemão e uma das maiores associações de hackers no mundo. No congresso, frequentadores locais apresentaram um documento com diretrizes para criação e organização do que seria um *hackerspace* (FONSECA, 2014; MATTOS, 2014). Para Maxigas (2012), o conceito de *hackerspaces* foi difundido a partir dessa experiência, que colocou a criação de novos *hackerspaces* na agenda do movimento hacker por todo mundo.

Os *hackerspaces* normalmente são organizados por um sistema de associação, muitas vezes paga e dependente de convite de membros internos, e pela manutenção de um ambiente de trabalho comum para socialização, produção e aprendizado. Os membros do *hackerspace* podem realizar projetos individuais ou coletivos, com ou sem a colaboração de outros para resolução de problemas. Nessa manifestação do movimento hacker, as práticas são bastante consistentes entre diferentes espaços e estão ligadas ao material e ao compartilhamento de espaço físico:

> *"The technologies used can be described as layers of sedimentation: newer technologies take their place alongside older ones without it becoming entirely obsolete. First of all, the fact that hackers collaborate in a physical space meant a resurgence of work on electronics, which conjoined with the established trend of tinkering with physical computers. A rough outline of connected research areas could be (in order of appearance): free software development, computer recycling, wireless mesh networking, microelectronics, open hardware, 3D printing, machine workshops and cooking."* (MAXIGAS, 2012)

Muitas vezes, os *hackerspaces* são os únicos lugares abertos em que esses dispositivos eletrônicos estão disponíveis para manuseio e utilização de um público mais amplo. Além desses elementos, a exploração da área teórica da computação física através do Arduino e a proliferação de mídias voltadas para difusão de projetos e resultados reforçaram os aspectos em comum da materialidade dos *hackerspaces*.

De acordo com Maxigas (2012), o foco das discussões nos *hackerspaces* costuma ser a forma de organização da comunidade, e não seu conteúdo político, em consequência de sua inclinação libertária. A escolha dos *hackerspaces* em não se posicionar politicamente tem duas consequências. Primeiro, os projetos e colaborações são difundidos e aceitos pelos mais diferentes atores (grupos da sociedade civil, corporações capitalistas, entre outros). Segundo, a falta de um posicionamento político muitas vezes leva à reprodução das estruturas de poder dominantes na sociedade dentro dos *hackerspaces*, centralizando suas atividades aos interesses de homens brancos de classe média e entusiastas de tecnologias.

Maxigas (2014) avalia que a conexão dos *hacklabs* com movimentos sociais e sua importância no movimento anarquista e autonomista para a expansão do acesso às tecnologias de informação e comunicação atrelou sua imagem a um momento histórico específico, dificultando sua expansão para contextos diferentes. Os *hackerspaces*, portanto, foram além dos limites históricos dos *hacklabs* e impactar de forma mais duradoura na criação, transformação e aprendizados em torno das tecnologias com as quais trabalham porque são mais abertos às dinâmicas externas e se articulam com um grupo mais amplo de atores.

> *"Arguably, hackers occupied such an ambiguous position since the beginning of hackerdom, but shared machine shops represent a new configuration. They appear as embodied communities organised in research and production units of physical and logical goods; they even appear to escape the subcultural ghetto as they expand their collaborations to educational institutions, museums, and libraries. They are eminent laboratories in both their practices and products: as experimental forms of social institutions, and as the developers of technological prototypes projecting new visions of the future. Industry actors, state authorities and policy makers have recognised such milieus as prolific grounds for recruitment and new organisational models, which in itself warrants critical attention."* (TROXLER & MAXIGAS, 2014)

Hackerspaces são espaços em que pessoas com diferentes interesses e motivações se encontram para compartilhar conhecimentos, ferramentas, recursos e práticas em lugares fixos ou não. Nesses espaços, as pessoas podem trabalhar em seus próprios projetos ou de forma colaborativa, aprendendo e ensinando uns aos outros e as experiências de manusear, desmontar, remontar e dar novas funções e significados para as tecnologias são uma forma de transformar o conhecimento tecnológico e a relação dos indivíduos com as tecnologias existentes.

Alguns debates mais recentes sobre *hacklabs* e *hackerspaces* envolvem sua capacidade de serem, de fato, um lugar aberto e seguro onde alternativas às dinâmicas sociotécnicas existentes têm espaço. De acordo com Nascimento (2014), *hackerspaces* engendram oportunidades concretas para interações descentralizadas e colaborativas com tecnologias não só nos experimentos em nível material e técnico, mas com potenciais consequências econômicas, culturais, sociais e políticas. Essa potencialidade, segundo a autora, deriva da racionalidade presente nesses espaços de suporte à abertura e liberdade ao pensar e fazer tecnologia:

> "*This powerful and captivating rationale expresses that any user, consumer, or citizen should be ultimately able to produce, use, share, copy and improve technologies, with little to no help or backup from traditional technological experts, organizations or institutions. And from this standpoint, derives a multiplicity of potential pathways for empowerment through technology and democratization of technology for broader social groups*." (NASCIMENTO, 2014)

A partir dessa perspectiva, cogitou-se que os *hackerspaces* abririam caminho para uma série de potenciais formas de empoderamento de parcelas da sociedade normalmente ignoradas ou excluídas das decisões e do processo de desenvolvimento tecnológico através da democratização da criação, transformação e apropriação da tecnologia.

Porém, os estudos sobre *hackerspaces* têm mostrado que esses espaços não são, em sua maioria, inclusivos ou diversos. Para Grenzfurthner & Schneider (2009), o argumento de que os espaços são abertos, ou seja, que todos poderiam participar das atividades dos *hackerspaces* desde que tenham as habilidades adequadas para comunicação e colaboração, tem fundo meritocrático e normalmente é usado como desculpa para exclusão de vários grupos étnicos e sociais.

Toupin (2014), em consonância com Grenzfurthner & Schneider (2009), aponta que dessa ideia de abertura, que ignora questões de gênero, raça, orientação sexual, classe social e habilidades tecnológicas, surgem diversos problemas intrinsecamente ligados à

hesitação dos *hackerspaces* em reconhecer e tratar de questões de privilégio e meritocracia. O principal deles seria que um espaço aberto (sem delimitações) normalmente favorece os indivíduos que já usufruem de privilégios de gênero, classe e raça e reproduz estruturas de dominação e poder existentes na sociedade. Os ambientes dos *hackerspaces* sob a bandeira da abertura estão predominantemente associados às necessidades e interesses de homens brancos, de classe média, heterossexuais e com afinidades tecnológicas.

A não identificação com esses espaços têm levado feministas hackers e entusiastas de tecnologia a pensar em espaços intersecionais concebidos com suas próprias delimitações, onde criação e colaboração possam acontecer em lugares seguros em que mulheres não estejam subrepresentadas ou invisibilizadas. "*They [the feminists] envisage a different role for their hackerspace, one in which boundaries offer both safety and a platform for political resistance.*" (TOUPIN, 2014). Ao criar seus próprios *hackerspaces*, as mulheres estão contestando a ideia de que espaços abertos são necessariamente inclusivos e igualitários e moldando a organização e as práticas que as fazem hackers, ressignificando e expandindo o conceito de *hackerspace*.

Um dos fatores condicionantes da característica não inclusiva ou democrática dos *hackerspaces* teria sido a progressiva perda de consciência política desses espaços ao longo do seu processo de proliferação, que foi concomitante ao desaparecimento dos *hacklabs* e do esquecimento de suas diferentes histórias e concepções (MAXIGAS, 2012). A fusão dos artigos da Wikipédia sobre *hacklabs* e *hackerspaces* em 2010 sob alegação de que não haveria diferenças entre eles teria sido um sintoma do esquecimento de que *hacklabs* e *hackerspaces* são ideologicamente diferentes: os primeiros explicitamente políticos, ligados aos movimentos anarquistas e autonomistas europeus; os segundos sem posicionamento político aberto, mas cercados de valores libertários.

Grenzfurthner & Schneider (2009) são mais críticos em relação ao que chamam de processo de despolitização dos espaços e suas consequências:

> *"The political agenda was mushroomed by individual problems that techno nerds tried to solve in nice fearless atmospheres, non-aggressive states where the aggressiveness of the market was suspended; where one could discuss technical and creative problems and challenges politely with likeminded people. As such, the political approach faded away on en route into tiny geeky workshop paradises. The micro-politics failed on the same scale and to the same extent as older macro-political projects got pulverized through the irreversibility of capitalism. The idea of having a revolution (of whatever kind) was domesticated into good clean reformism, and the only revolutions that lay ahead were the technological semi-revolutions of the internet and its social web sprouts."* (GRENZFURTHNER & SCHNEIDER, 2009)

Os atores avaliam que sem articulação política os *hackerspaces* podem ser comparados com as ocupações europeias após sua legalização, agora reformadas, transformadas e ocupadas pela burguesia.

Ainda que Maxigas (2012) concorde que exista uma gentrificação dos espaços e das tecnologias dos *hackerspaces*, o autor reforça que seus frequentadores consideram suas atividades uma forma de repensar o consumo de tecnologias e de permitir que o desenvolvimento do conhecimento tecnológico e as práticas relacionadas sejam livres. A questão principal, então, seria o que esses frequentadores entenderiam como liberdade e os meios necessários para alcançá-la. Na maioria dos *hackerspaces*, em consequência de sua inclinação libertária, as liberdades são as individuais de expressão, acesso, associação e apropriação do próprio trabalho.

Nascimento (2014) discute, porém, que capacidades e escolhas individuais em relação a meios de produção normalmente não levam ao empoderamento, criatividade e transformação social por meio da tecnologia. A percepção de que os *hackerspaces* teriam capacidade de alterar as estruturas e relações do modelo sociotécnico existente apenas por permitir o acesso e diferentes formas de interação com tecnologia sob a premissa de abertura apresentada anteriormente é tecnologicamente determinista, mas corrobora com as análise de Söderberg (2013) de que argumentos dessa natureza fazem parte das ações políticas dos hackers e não necessariamente indicam um comportamento acrítico e antidemocrático em relação à tecnologia.

Defrontando-se com o potencial dos *hackerspaces* em democratizar o espaço de criação, aprendizado e vivência de tecnologias, torna-se necessário identificar e entender como as dinâmicas dos *hackerspaces* com o capitalismo têm se manifestado, portanto, como tem se desenrolado o movimento de recuperação. Nos estudos sobre *hackerspaces* predomina a percepção de que o movimento é ainda recente para ser avaliado nesse aspecto, embora alguns autores já estejam se questionando se os *hackerspaces* não seriam apenas mais uma forma de organização da produção dentro do sistema capitalista.

Ainda que os *hackerspaces* e os espaços de produção capitalistas se diferenciem quanto às técnicas e organização da produção e da apropriação de bens, serviços e conhecimento, Troxler & Maxigas (2014) apontam que uma evidência de que compartilhariam da mesma lógica seria a característica em comum de convergência do trabalho, socialização e vida pessoal em um mesmo ambiente.

De acordo com Lund (2017), existiriam diversos elementos na configuração dos *hackerspaces* que facilitariam sua cooptação pelo capitalismo, como a necessidade de

financiamento das atividades, as interações entre a proteção intelectual dos comuns e a proteção intelectual privada e o fato dos trabalhos nos *hackerspaces* normalmente não serem remunerados, mas sim atividades secundárias de seus frequentadores, de forma que a apropriação do conhecimento gerado nesses espaços poderia se configurar como apropriação de trabalho criativo gratuito pelo capitalismo.

Nesse sentido, Grenzfurthner & Schneider (2009) expressam preocupação com a capacidade do capitalismo, em sua qualidade de sistema altamente adaptável, de incorporar os frutos do conhecimento gerado nos movimentos de resistência que surgem ao longo do tempo. Espaços e vivências alternativas, dentro do sistema capitalista, costumam prover ideias que eventualmente são apropriadas e reproduzidas em organizações e ambientes capitalistas emuladas daquelas alternativas visando lucro.

CAPÍTULO 3 – Panorama dos estudos de caso sobre hackers na América Latina

A proposta deste capítulo é apresentar um panorama dos estudos de caso sobre hackers na América Latina a partir das publicações encontradas, selecionadas e sistematizadas por meio da Revisão Sistemática de Bibliografia (RSB) como parte da síntese de literatura proposta pelo método. O quadro gerado pela sistematização dos achados foi base para a criação de categorias e agrupamentos analisados. As referências dos artigos e capítulos de livros selecionados podem ser consultadas no Anexo A e uma versão resumida das categorias e agrupamentos criados para análise compõem o Anexo B.

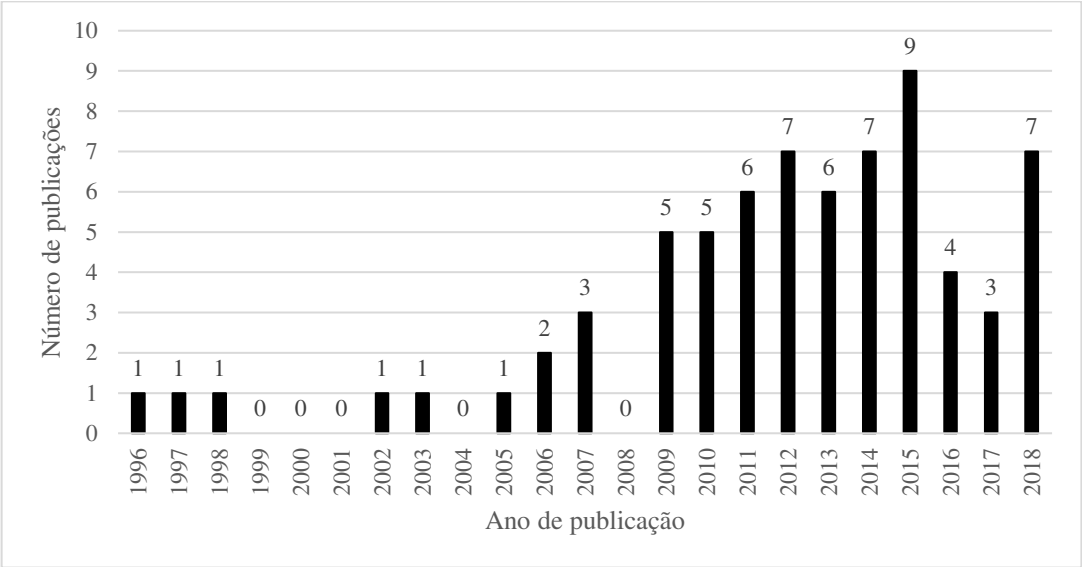
Assim como propõe a RSB, a síntese aqui construída traz para análise outras informações além do conteúdo. Primeiro, são apresentadas informações sobre a publicação, tais como ano e país de publicação da revista ou livro, para em seguida apresentar informações sobre os autores. Em relação ao conteúdo, dentre as questões abordadas encontram-se os objetos de pesquisa, palavras-chave, método de obtenção de dados, abordagem, definição de hackers e hackerismos e políticas hackers identificadas. Para tratar do conteúdo, especificamente, foram criadas categorias de análise com o objetivo de organizar o conjunto de publicações selecionadas e permitir alguns cruzamentos de informações.

É importante reiterar que as setenta publicações selecionadas para análise atenderam a todos os critérios de inclusão mencionados no primeiro capítulo, portanto, são estudos de caso sobre grupos, espaços, atividades, práticas ou eventos ligados aos hackers de computador geograficamente localizados na América Latina.

3.1 Informações sobre publicação

Este item apresenta informações gerais sobre a publicação dos estudos encontrados. O conjunto de publicações selecionadas é formado por 62 artigos e 8 capítulos de livros, totalizando setenta publicações. A partir da Figura 1, que ilustra o número de publicações por ano, é possível identificar um aumento do número de publicações após 2009, sendo 2015 o ano com o maior número de publicações. A exceção do intervalo de 2009-2018 foi o ano de 2017, em que apenas três publicações atenderam os critérios de inclusão propostos.

Figura 1 - Número de publicações por ano



Fonte: elaboração própria com base no conjunto de publicações selecionadas.

Dentre a seleção, as primeiras publicações sobre hackers na América Latina datam o final dos anos 1990: "*Maya Hackers and the Cyberspatialized Nation-State: Modernity, Ethnostalgia, and a Lizard Queen in Guatemala*" (NELSON, 1996), que trata da apropriação tecnológica e resistência de ativistas culturais do povo maia na Guatemala contra a absorção pela cultura hegemônica, e "*A comment on the zapatista 'netwar'*" (RONFELDT & MARTÍNEZ, 1997) e "*The Zapatistas and the Eletronic Fabric of Struggle*" (CLEAVER, 1998), que tratam de aspectos da *netwar* transcorrida ao longo do levante zapatista no México: especificidades do conflito e da ação coletiva e as inter-relações, mobilizações e resistências do movimento zapatista, respectivamente. Os primeiros estudos de caso sobre a América Latina, portanto, são de manifestações hackers politicamente engajadas.

Dentro do conjunto de publicações selecionadas, estas três publicações são citadas constantemente por serem compreendidas como histórias originárias das representações hackers na América Latina tanto em relação às formas de apropriação de tecnologias da informação na luta de povos tradicionais e movimentos sociais quanto, no caso dos zapatistas, por ser o primeiro grande exemplo da força de mobilização dos hackers em nível global, trazendo para a discussão o ciberativismo, suas táticas e o papel das tecnologias da informação para a promoção da democracia (PITMAN, 2007). É interessante notar que tanto o artigo de Nelson (1996) quanto os capítulos de livros de Ronfeldt & Martínez (1997) e Cleaver (1998) foram escritos em língua inglesa e não publicados originalmente por editoras ou revistas latino-americanas, sendo os dois primeiros publicados nos Estados Unidos e o

terceiro no Reino Unido. Em relação à língua em que o artigo ou capítulo foi publicado, cerca de metade deles estão em língua espanhola. O Quadro 4 resume as informações:

Quadro 4 - Número de publicações por linguagem de publicação

Língua de publicação	Número de publicações	% do total
Espanhol	36	51,4
Português (Brasil)	19	27,1
Inglês	15	21,4
Total	**70**	**100,0**

Fonte: elaboração própria com base no conjunto de publicações selecionadas.

Para o conjunto de publicações, o Quadro 5 resume as informações sobre país de publicação das revistas e livros.

Quadro 5 - Número de publicações por país da revista/livro

País	Número de publicações	% do total
Países latino-americanos	**47**	**67,1**
Brasil	22	31,4
Equador	5	7,1
México	5	7,1
Colômbia	4	5,7
Argentina	3	4,3
Chile	2	2,9
Peru	2	2,9
Venezuela	2	2,9
Costa Rica	1	1,4
Paraguai	1	1,4
Outros países	**22**	**31,4**
Estados Unidos	13	18,6
Espanha	5	7,1
Reino Unido	2	2,9
Alemanha	1	1,4
Índia	1	1,4
Sem informação	1	1,4
Total	**70**	**100,0**

Fonte: elaboração própria com base no conjunto de publicações selecionadas.

O Quadro 5 evidencia que cerca de um terço do conjunto de artigos e capítulos selecionados foram publicados por editoras e revistas de países não pertencentes à América Latina. Dentre eles, treze foram publicados nos Estados Unidos, o que equivale a 59% das publicações em outros países e 18,6% do total de setenta publicações. Em termos de total de publicações, os Estados Unidos ficam abaixo apenas do Brasil, cujas editoras e revistas foram responsáveis por 31,4% do total de publicações sobre hackers na América Latina.

O único meio de publicação sem informação sobre país de publicação é o *Journal of Peer Production*, que agrega contribuições sobre produção por pares e trabalhos colaborativos e é acessado por meio do próprio site[34]. O *Journal of Peer Production* tem em seu corpo editorial alguns dos autores citados no segundo capítulo, como Maxigas, Gabriella Coleman, Peter Troxler, Sophie Toupin, Johan Söderberg e Alessandro Delfanti.

Algumas revistas apareceram mais de uma vez nos resultados do conjunto selecionado, são elas:

- *Chasqui: Revista Latinoamericana de Comunicación* (VASQUÉZ, 2013; GARCÍA, 2015): revista equatoriana do campo da comunicação latino-americana com foco em políticas e estrutura da comunicação, jornalismo, comunicação popular e comunitária, economia política da comunicação e outras temáticas[35];
- *Razón y Palabra* (ISLAS, ARRIBAS & MINERA, 2009; PINO, 2014): revista de origem mexicana e agora publicada no Equador voltada aos estudos de comunicação[36];
- *Revista Iberoamericana* (MAGUIRE, 2009; GARCÍA, 2012): revista estadunidense interessada em artigos, resenhas e notas sobre literatura e teoria e crítica literária em espanhol ou português[37];
- *Science Fiction Studies* (REDONDO, 2005; ENTEEN, 2007): revista estadunidense com focos em artigos, ensaios, resenhas e documentos históricos sobre ficção científica[38], e;

[34] http://peerproduction.net (último acesso em 17 de julho de 2017).
[35] https://revistachasqui.org/index.php/chasqui (último acesso em 17 de julho de 2017).
[36] http://www.revistarazonypalabra.org/index.php/ryp (último acesso em 17 de julho de 2017).
[37] https://revista-iberoamericana.pitt.edu/ojs/index.php/Iberoamericana/index (último acesso em 17 de julho de 2017).
[38] https://www.depauw.edu/sfs/index.htm (último acesso em 17 de julho de 2017).

- *Sociedade e Cultura* (GRAVANTE, 2012; PARRA, 2012): revista brasileira, voltada para publicações em Antropologia Social, Ciência Política e Sociologia[39].

Pensando em tecer comparações, são apresentadas a seguir informações sobre os autores do conjunto de publicações selecionado.

3.2 Sobre os autores e coautorias

Das setenta publicações selecionadas, vinte delas foram elaboradas em coautoria, o que corresponde a 28,6% das publicações. É importante observar que seis autores foram contabilizados duas vezes porque são autores de dois artigos diferentes do conjunto e apresentaram informações diferentes sobre vínculo institucional, formação acadêmica ou grupo/projeto de pesquisa vinculado. São eles: Agustín Zanotti (ZANOTTI, 2011; 2014), Bárbara Maria Farias Mota (MOTA & FIGUEIREDO FILHO, 2015; MOTA, HAYASHI & FERNANDES; 2016), Graciela Natansohn (NATANSOHN, 2018; NATANSOHN & PAZ, 2018), Luz Marina Suaza (SUAZA & ORTIZ, 2011; SUAZA, 2013), Mônica Paz (PAZ, 2013; NATANSOHN & PAZ, 2018) e Tania Pérez-Bustos (PÉREZ-BUSTOS, 2010a; 2010b).

O Quadro 6 resume as informações sobre coautoria:

Quadro 6 - Coautorias

Coautorias	**Número de publicações**	**% do total de publicações**	**Número de autores(as)**	**% do total de autores**
Sem coautoria	50	71,4	50	50,0
2	12	17,1	24	24,0
3	6	8,6	18	18,0
4	2	2,9	8	8,0
Total	**70**	**100,0**	**100**	**100,0**

Fonte: elaboração própria com base no conjunto de publicações selecionadas.

[39] https://www.revistas.ufg.br/fchf (último acesso em 17 de julho de 2017).

Mais de dois terços das publicações foram escritas apenas por um autor, o equivalente a cinquenta publicações. Dos setenta autores que encabeçam as publicações, 29 (41,4%) são do gênero feminino e 41 (58,6%) do gênero masculino, números que passam para 44 (44%) e 56 (56%), respectivamente, quando se considera o total de cem autores. No conjunto de publicações selecionadas não houve coautoria entre pesquisadores de instituições de países diferentes.

Dos vinte artigos escritos em coautoria, quatro foram publicados por autores pertencentes ao mesmo grupo ou projeto de pesquisa como resultado das atividades desenvolvidas. São eles:

- *Grupo de Pesquisa Educación y Cultura Política* da Universidad Pedagógica Nacional de Bogotá, Colômbia (SUAZA & ORTIZ, 2011);
- *Laboratório de Educação, Mediações Tecnológicas e Transdisciplinaridade em Saúde* (Lemtes) da Escola Fiocruz de Governo, Brasil (GUIZARDI et al., 2018);
- *Seguridad Informática y Delitos Informáticos* da Universidad Santo Tomás de Aquino, Colômbia (OJEDA-PÉREZ et al, 2010), e;
- *Proyecto Internet-Cátedra de Comunicaciones Estratégicas y Cibercultura* do Tecnológico de Monterrey, México (ISLAS, ARRIBAS & MINERA, 2009).

Além destes três grupos e um projeto, as autoras de dois outros artigos (PAZ, 2013; NATANSOHN, 2018) mencionaram compor o Gig@: Grupo de Pesquisa em Gênero, Tecnologias Digitais e Cultura da Universidade Federal da Bahia (UFBA). Especificamente, Natansohn (2018) aponta que seu trabalho é uma reflexão inicial do projeto de pesquisa "Ciberfeminismos 3.0 na América Latina, apropriações feministas da cultura digital", vinculado ao Programa de Pós-graduação em Comunicação e Cultura Contemporâneas da UFBA.

Apenas 39 dos autores informaram nas publicações sua formação acadêmica. Como indica o Quadro 7, 11% do total de autores são formados em áreas das Ciências Sociais, 9% em Estudos da Linguagem e 7% em Direito.

Quadro 7 - Formação acadêmica informada pelos autores

Área do conhecimento	Área de formação	Número de autores	% do total
Ciências Sociais	Ciências Sociais, Ciências Políticas, Antropologia, Sociologia	11	11,0
Estudos da Linguagem	Comunicação, Comunicação Social, Jornalismo, Literatura	9	9,0
Direito	Criminologia, Direito	7	7,0
Educação		5	5,0
Outras humanidades	Administração, Economia, Ciências Humanas	4	4,0
Engenharia	Engenharia de Sistemas, Engenharia Industrial	2	2,0
Estatística		1	1,0
Sem informação		61	61,0
Total		**100**	**100,0**

Fonte: elaboração própria com base no conjunto de publicações selecionadas.

Reiterando o comentário feito no primeiro capítulo, como há uma disparidade de qualidade de informações entre pesquisadores brasileiros e de outros países devido à existência da Plataforma Lattes e as informações encontradas utilizando a ferramenta de busca do Google foram imprecisas e pouco confiáveis, a escolha foi manter apenas as informações contidas nas publicações. O interesse em extrair informações sobre formação acadêmica e grupos/projetos de pesquisa era de retratar os autores no momento da escrita ou publicação do artigo ou capítulo de livro, mas as informações contidas nas publicações foram escassas e incompletas, o que dificulta qualquer generalização sobre o conjunto de autores. O vínculo institucional foi a única informação mais consistente. O Quadro 8 resume os achados:

Quadro 8 - Número de autores e publicações por país do vínculo institucional informado

País do vínculo institucional	Número de autores	% do total de autores	Número de publicações	% do total de publicações
Países latino-americanos	**72**	**72,0**	**45**	**64,3**
Brasil	30	30,0	20	28,6
Colômbia	14	14,0	8	11,4
México	11	11,0	6	8,6
Argentina	5	5,0	4	5,7
Venezuela	4	4,0	2	2,9
Equador	3	3,0	1	1,4
Peru	3	3,0	2	2,9
Chile	1	1,0	1	1,4
Costa Rica	1	1,0	1	1,4
Outros países	**12**	**12,0**	**12**	**17,1**
Estados Unidos	8	8,0	8	11,4
Espanha	4	4,0	4	5,7
Sem informação	16	16,0	13*	18,6
Total	**100**	**100,0**	**70**	**100,0**

Fonte: elaboração própria com base no conjunto de publicações selecionadas. *Dentre as publicações escritas em coautoria, em uma delas um dos autores informou vínculo institucional enquanto outro não. Neste caso (HERRERA & GARRIDO, 2011), considerou-se o vínculo institucional do primeiro autor (México).

Considerando o total de cem autores, 72% deles informaram vínculo em instituições de países latino-americanos. Portanto, considerando o conjunto de publicações selecionado, é possível afirmar que a maior parte do conhecimento sobre hackers na América Latina foi gerada por pesquisadores em instituições latino-americanas.

Dos vinte países que compõem a América Latina, apenas nove foram mencionados nas publicações, sendo que apenas três países concentraram mais de 50% dos autores: Brasil (30%), Colômbia (14%) e México (11%). Com exceção dos países latino-americanos, apenas outros dois foram identificados: Estados Unidos e Espanha, com 8% e 4% dos autores, respectivamente.

Dadas essas informações, é possível tecer comparações entre o número de publicações do país de vínculo institucional informação (origem do estudo) e o país de publicação dos artigos e capítulos. O Quadro 9 resume os cruzamentos realizados e o Quadro 10 expande os resultados do Quadro 9.

Quadro 9 - Número de publicações por país do meio de publicação e país de vínculo institucional informado (resumido)

	Número de publicações por país do meio de publicação	% do total	Número de publicações por vínculo institucional dos autores	% do total
Países latino-americanos	**47**	**67,1**	**45**	**64,3**
Brasil	22	31,4	20	28,6
Equador	5	7,1	1	1,4
México	5	7,1	6	8,6
Colômbia	4	5,7	8	11,4
Argentina	3	4,3	4	5,7
Chile	2	2,9	1	1,4
Peru	2	2,9	2	2,9
Venezuela	2	2,9	2	2,9
Costa Rica	1	1,4	1	1,4
Paraguai	1	1,4	0	0,0
Outros países	**22**	**31,4**	**12**	**17,1**
Estados Unidos	13	18,6	8	11,4
Espanha	5	7,1	4	5,7
Reino Unido	2	2,9	0	0,0
Alemanha	1	1,4	0	0,0
Índia	1	1,4	0	0,0
Não informado	1	1,4	13*	18,6
Total	**70**	**100,0**	**70**	**100,0**

Fonte: elaboração própria com base no conjunto de publicações selecionadas. *Dentre as publicações escritas em coautoria, em uma delas um dos autores informou vínculo institucional enquanto outro não. Neste caso (HERRERA & GARRIDO, 2011), considerou-se o vínculo institucional do primeiro autor (México).

Quadro 10 - Número de publicações por país do meio de publicação e país de vínculo institucional informado (expandido)

	País de publicação																
País de vínculo institucional dos autores	Argentina	Brasil	Chile	Colômbia	Costa Rica	Equador	México	Paraguai	Peru	Venezuela	Alemanha	Espanha	Estados Unidos	Índia	Reino Unido	Não informado	**Total de publicações**
Argentina	1	0	1	0	0	0	1	0	0	0	0	1	0	0	0	0	**4**
Brasil	2	17	0	0	0	0	0	0	0	0	0	1	0	0	0	0	**20**
Chile	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**
Colômbia	0	2	0	4	0	0	0	0	0	0	0	1	0	1	0	0	**8**
Costa Rica	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	**1**
Equador	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	**1**
México	0	0	0	0	0	1	4	0	1	0	0	0	0	0	0	0	**6**
Peru	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	**2**
Venezuela	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	**2**
Espanha	0	1	0	0	0	1	0	1	0	1	0	0	0	0	0	0	**4**
Estados Unidos	0	0	0	0	0	1	0	0	0	0	0	0	6	0	1	0	**8**
Sem informação	0	2	0	0	0	0	0	0	0	0	1	2	6	0	1	1	**13***
Total	**3**	**22**	**2**	**4**	**1**	**5**	**5**	**1**	**2**	**2**	**1**	**5**	**13**	**1**	**2**	**1**	**70**

Fonte: elaboração própria com base no conjunto de publicações selecionadas. *Dentre as publicações escritas em coautoria, em uma delas um dos autores informou vínculo institucional enquanto outro não. Neste caso (HERRERA & GARRIDO, 2011), considerou-se o vínculo institucional do primeiro autor (México).

Os quadros 9 e 10 evidenciam que 50% dos artigos ou capítulos de livros foram publicados por revistas e editoras do mesmo país de vínculo institucional informado. A Colômbia se destaca do grupo de países latino-americanos tanto por ser um dos países com mais vínculos institucionais informados (14% do total de autores) quanto pelo número de publicações por revistas e editoras de outros países: quatro no total, equivalente à metade da produção colombiana. Autores com vínculo em instituições argentinas, equatorianas e venezuelanas também publicaram mais em outros países.

De forma geral, há uma equivalência entre o número de artigos e capítulos de livros publicados por cada país e o número de publicações por autor com vínculo em instituições do mesmo país. As maiores discrepâncias em relação ao conjunto de países são Colômbia, Equador e Estados Unidos. Enquanto apenas quatro (5,7%) artigos ou capítulos de livro foram publicados na Colômbia, os autores com vínculos em instituições colombianas foram responsáveis por oito (11,4%) do total de publicações, sendo quatro em outros países (Brasil, Espanha e Índia), além das outras quatro publicações na Colômbia. No caso do Equador e dos Estados Unidos, o movimento é contrário. Os meios de publicação do Equador foram responsáveis por 7,1% do total de publicações do conjunto selecionado, enquanto os autores com vínculo em instituições equatorianas contribuíram com apenas um artigo, correspondente a 1,4% do total de publicações. Para os Estados Unidos, esses números passam para 18,6% e 11,4% respectivamente.

3.3 Sobre o conteúdo das publicações

Para a análise do conteúdo das publicações foram criadas categorias que facilitassem a construção de um panorama dos estudos de caso sobre hackers na América Latina a partir das leituras dos artigos. As categorias criadas buscaram identificar aspectos metodológicos das publicações, perspectivas pelas quais hackers e hackerismos são estudados, formas com que hackers e hackerismos são definidos e como emergem as políticas hackers no conjunto de publicações selecionadas.

Aspectos metodológicos

Considerando os parâmetros propostos por Selltiz et al. (1975) para classificação de estudos em descritivos ou exploratórios, principalmente em relação à função do estudo e os métodos utilizados, o conjunto de publicações pôde ser dividido em:

- 5 estudos descritivos, correspondente a 7,1% do total de publicações;
- 63 estudos exploratórios, correspondente a 90% do total de publicações, e;
- 2 estudos descritivos e exploratórios, corresponde a 2,9% do total de publicações. Neste caso, as publicações apresentaram funções e métodos dos dois tipos de estudos proposto por Selltiz et al. (1975), sem prevalência de um ou outro.

A quantidade de publicações de caráter exploratório em relação ao conjunto de publicações significa que 90% dos estudos de caso foram realizados para aumentar o conhecimento existente sobre situações e fenômenos, esclarecer conceitos ou ajudar na criação de hipóteses. Portanto, parece existir uma percepção entre os autores de que hackers e hackerismos na América Latina são assuntos ainda pouco explorados. Söderberg (2013) sugere, ao falar das primeiras literaturas sobre hackers, que essa abordagem mais exploratória indicaria uma percepção dos autores de que hackers e hackerismos são exóticos e fechados em si mesmos. Porém, esse não é o caso das publicações sobre estudos de caso de hackers de computador na América Latina. Como será apresentado adiante, há muitos estudos de caso que pensam as práticas e o ser hacker como intrínsecos ao social, econômico e político contemporâneos, portanto, apresentam uma visão mais próxima àquela de Coleman (2017).

As formas de obtenção de dados para a análise dos estudos de caso foram múltiplas. Na maior parte das publicações foram identificadas duas fontes de dados: i) notícias, relatórios, wikis, manifestos, artes e outros materiais disponíveis na Internet, uma vez que, sendo um dos espaços de socialização hacker e parte essencial do seu público recursivo, a Internet torna-se um lócus de informação, e; ii) literatura existente sobre hackers ou sobre outros objetos, mas com nova compreensão a partir da perspectiva de grupos, espaços, atividades, práticas ou eventos ligados aos hackers. Essa conclusão foi corroborada pela varredura realizada nas referências bibliográficas para identificar se foram utilizados quaisquer outros estudos acadêmicos sobre hackers, independente se incluídos ou não no estudo de escopo. O resultado foi dividido: das setenta publicações 38 não citaram outros estudos sobre hackers, o que equivale a 54,3% do total. Exceto pelos estudos descritivos, a consulta à literatura existente foi o principal método de obtenção de dados do conjunto de publicações.

Dentre as publicações que utilizaram de outros métodos de obtenção de dados, foi possível identificar uma preferência por entrevistas semiestruturadas e etnografia participante ou em redes sociais. Também foi comum a combinação entre esses dois métodos e a revisão de literatura.

Campos de conhecimento

A identificação dos campos de conhecimento foi realizada de três formas: através da indicação de utilização de conceitos, da contribuição evidenciada pelos autores ao longo do estudo e da varredura das referências bibliográficas. Considerando o total de publicações, 28 delas (40,0%) identificaram mais de um campo de conhecimento e 42 delas (60,0%) apenas um. Essa medida não necessariamente indica um caráter interdisciplinar dos estudos de caso sobre hackers na América Latina, mas reforça a percepção de que pesquisadores estão dando nova compreensão a certas abordagens ou contribuindo para diferentes campos de conhecimento a partir da inclusão e perspectiva de grupos, espaços, atividades, práticas ou eventos ligados aos hackers.

Os campos de conhecimento mais mencionados e com maior contribuição para o conjunto de publicações selecionadas foram os estudos hackers, seguidos pelos Estudos Sociais da Ciência e da Tecnologia. Um achado importante desta pesquisa envolve a contribuição de três campos do conhecimento: teorias feministas, teoria dos movimentos sociais e estudos literários.

Nesse sentido, é interessante que, no conjunto de publicações sobre hackers na América Latina, um dos principais campos do conhecimento explorados sejam as teorias feministas porque isso não se refletiu na literatura consultada para o estudo de escopo. Particularmente, os primeiros contatos que tive com temas hackers abordavam questões de gênero, de forma que a percepção construída no início da pesquisa foi de que esse tema era extensivamente estudado. Porém, durante a Escola Doutoral de Estudos Digitais, ao final de um dos painéis de técnicos, pude perguntar para Gabriella Coleman por indicações de leitura dos estudos hackers em intersecção com gênero e, após responder que não conhecia ninguém que tratasse disso especificamente, indicou um texto de Christine Dumbar-Hester, que abarca gênero, geeks e tecnologia, principalmente nas rádios amadoras estadunidenses, não necessariamente hackers de computador. Posteriormente, entrei em contato com o *Journal of Peer Production*, que conta com alguns artigos com incursões em questões de gênero, como o de Sophie Toupin (2014). Em termos do conjunto de publicações selecionadas, também é interessante que a maioria das autoras que tratam de questões de gênero em seus estudos estejam vinculadas a instituições brasileiras e colombianas.

O destaque das teorias dos movimentos sociais, por sua vez, tem como uma das principais causas o impacto das mobilizações do levante zapatista nas Chiapas e a insurreição de Oaxaca na percepção dos pesquisadores sobre o lugar dos hackers na política local e global

e da força do hacktivismo e, de forma mais geral, do ciberativismo como instrumento de resistência e transformação social.

Por fim, os estudos literários, junto dos estudos de ficção científica, estão relacionados com a produção extensa do gênero cyberpunk da América Latina. Os autores que escrevem sobre o cyberpunk latino-americano tratam não só do conteúdo das obras, mas de como as representações hackers, contidas nas obras, são reflexo dos hackers e sua relação com o contexto latino-americano. Os quadros 11 e 12 evidenciam os campos de conhecimento e suas intersecções.

Quadro 11 - Número de publicações com menção a apenas um campo de conhecimento

	Número de publicações
Estudos hacker	9
Teorias feministas	4
Estudos Sociais da Ciência e da Tecnologia	3
Teoria dos movimentos sociais	3
Teorias e tecnologias da comunicação	3
Estudos de ficção científica	2
Estudos literários	2
Teoria da arte	2
Abordagem de redes	1
Análise de políticas públicas	1
Ciência política	1
Conhecimentos tradicionais	1
Estudos da Juventude	1
Estudos de cibercrimes	1
Estudos do Direito da Informática	1
Estudos sobre a violência	1
Segurança da informação	1
Teoria da Atividade Histórico-Cultural	1
Teoria do crime	1
Teorias da educação	1
Teorias das organizações	1
Teorias de guerra	1
Total	**42**

Fonte: elaboração própria com base no conjunto de publicações selecionadas.

As autoras que conversam com as teorias feministas, por exemplo, o fazem em conjunto com os estudos hackers e Estudos Sociais da Ciência e da Tecnologia. Além da observação já realizada sobre estudos literários e estudos de ficção científica, outros dois

campos que aparecem em conjunto são os estudos de direito da informática e direito penal, utilizados nas publicações que tratam do aspecto violento e ilegal de certas práticas hackers.

Quadro 12 - Número de publicações com menção a mais de um campo de conhecimento

	Número de publicações
Estudos Sociais da Ciência e da Tecnologia	
Análise de políticas públicas	2
Teoria da ação política	1
Teorias feministas	4
Estudos literários	
Estudos do *software*	1
Estudos culturais	
Avaliação de políticas públicas	1
Estudos do Direito da Informática	
Direito Penal	3
Estudos hacker	
Estudos do Direito da Informática	1
Revisão sistemática	1
Teoria da dádiva	1
Teoria dos movimentos sociais	1
Teorias feministas	2
Estudos literários	
Ciência Política	1
Estudo dos ciborgues	1
Estudos de ficção científica	3
Teoria dos movimentos sociais	1
Teorias dos movimentos sociais	
Estudos do ciberespaço	1
Psicologia	1
Urbanismo	1
Estudos da guerra	1
Total	**28**

Fonte: elaboração própria com base no conjunto de publicações selecionadas.

Perspectivas sobre os estudos de caso

Neste item são apresentadas as perspectivas pelas quais os autores olharam para os hackers e hackerismos na América Latina. Para a análise aqui desenvolvida, foram criadas categorias para agrupar objetos de estudo, palavras-chave e foco da análise. Além disso, buscou-se aplicar as categorias de análise do processo de recuperação propostas por Delfanti

& Söderberg (2018) como uma aproximação da percepção dos autores sobre o lugar dos hackers e hackerismos no mundo contemporâneo.

O Quadro 13 resume as informações sobre localização do caso explorado:

Quadro 13 - Países ou região do caso explorado

País ou região	**Número de publicações**	**% do total**
América Latina	14	20,0
e outros países não latino-americanos	2	2,9
Argentina	4	5,7
Bolívia	1	1,4
Brasil	19	27,1
e outros países não latino-americanos	2	2,9
Chile	1	1,4
Colômbia	7	10,0
e outros países não latino-americanos	1	1,4
Costa Rica	1	1,4
Cuba	3	4,3
Guatemala	1	1,4
México	10	14,3
e outros países não latino-americanos	1	1,4
Peru	2	2,9
Venezuela	1	1,4
Total	**70**	**100,0**

Fonte: elaboração própria com base no conjunto de publicações selecionadas.

Os estudos que apontaram como lócus dos casos explorados a América Latina, 20% do total de setenta publicações, são, em sua maioria, estudos exploratórios que utilizaram da consulta à literatura existente como forma de obtenção de dados. Mais especificamente, essas publicações tratam de hackear outros meios, como arte e literatura, de representações hackers e da relação dos hackers com seu contexto e são ou uma primeira abordagem sobre o tema ou uma discussão mais ampla do lugar dos hackers no mundo contemporâneo.

O Brasil foi, dentre os países, o maior lócus de casos do conjunto de publicações, agregando 27,1% do total, seguido pelo México e a Colômbia, com 14,3% e 10% do total de publicações, respectivamente.

Considerando o conjunto de publicações selecionadas, foi possível identificar que a maior parte dos autores situou os casos de hackers e hackerismos na América latina, de forma abrangente, no contexto do capitalismo informacional, cujas reflexões são retiradas, em sua maioria, do primeiro volume do livro “A Era da Informação: Economia, Sociedade e

Cultura" de Manuel Castells, publicado em 1996. Castells se configura como um autor importante para o conjunto de publicações selecionadas não só por suas contribuições sobre o informacionalismo, mas também porque dialoga com outro autor importante para os estudos hackers: Pekka Himanen.

Manuel Castells escreve o posfácio do livro de Himanen (2001) trazendo descrições e reflexões sobre o informacionalismo como paradigma tecnológico[40] e a sociedade em rede como nova estrutura social, que – como foi apontado no segundo capítulo – é utilizado pelo segundo autor para discutir o trabalho hacker como alternativa à ética protestante do capitalismo industrial no contexto do pós-industrialismo. Castells, em Himanen (2001), constrói a contextualização da seguinte forma:

> "Sobre os fundamentos do informacionalismo, a sociedade em rede emerge e se expande pelo planeta como a forma dominante de organização social de nosso tempo. A sociedade em rede é uma estrutura social formada por redes de informação movidas pelas tecnologias de informação características do paradigma informacionalista. Por *estrutura social*, eu quero dizer os arranjos organizacionais dos seres humanos em relações de produção, consumo, experiência e poder, como expressos na interação significativa estruturada pela cultura. Uma rede é um conjunto de nós interconectados. Um nó é o ponto onde a curva encontra a si mesma. Redes sociais são tão antigas quanto a humanidade. Mas elas ganharam outra vida sob o informacionalismo porque as novas tecnologias aumentam a flexibilidade inerente às redes enquanto solucionam os problemas de coordenação e condução que, historicamente, dificultaram as redes na sua competição com as organizações hierárquicas." (CASTELLS, 2001, pp. 145-146)

Neste contexto – em que a economia é construída sobre redes colaborativas de produção e conhecimento (como as multinacionais) e mercados financeiros globais, cujos processos de investimento e valorização são construídos e suportados com base em redes eletrônicas – o trabalho também se transformaria. Segundo Castells (2001), assim como o sistema é conduzido pela inovação tecnológica, o trabalho – que se torna individualizado – passa a ser avaliado a partir da capacidade de trabalhadores e gerentes em se reprogramar constantemente para conseguir realizar novas tarefas.

A perspectiva na qual Manuel Castells baseia seu enfoque – de que a tecnologia incorpora a sociedade e a sociedade utiliza a tecnologia, de modo que não existiriam revoluções tecnológicas sem transformação cultural e social, ao mesmo tempo em que a

[40] O informacionalismo como novo paradigma tecnológico teria sido desencadeado pela revolução das tecnologias da informação e estaria apoiado em três características: a autoexpansão da capacidade de processamento em relação ao volume, complexidade e velocidade, a habilidade de realizar novas combinações e a flexibilidade em termos de distribuição. Segundo Castells (2001), a novidade deste paradigma é a tecnologia de processamento da informação e seu impacto na geração e na aplicação de conhecimento.

tecnologia criada e difundida numa sociedade configura sua materialidade e desdobramento – acaba atribuindo aos hackers papel central no capitalismo informacional:

> "O informacionalismo foi parcialmente inventado e decisivamente moldado por uma nova cultura que foi essencial no desenvolvimento das redes de computadores, na distribuição da capacidade de processamento e no aumento da potencial inovação através da cooperação e do compartilhamento. O entendimento teórico dessa cultura [hacker] e de seu papel como fonte de inovação e criatividade no informacionalismo é a pedra fundamental para a nossa compreensão da gênese da sociedade em rede [...] É por isso que a teoria da cultura hacker, de Pekka Himanen, como o espírito do informacionalismo é um avanço fundamental na descoberta do desdobramento do mundo neste incerto alvorecer do Terceiro Milênio." (CASTELLS, 2001, p. 154)

Mesmo nas definições mais abrangentes de hackers, como a utilizada nesta pesquisa (aqueles que constroem, trabalham e habitam tecnologias da informação, que são parte essencial de suas experiências, políticas, éticas e formas de interagir e ser no mundo), fica entendido que hackers se diferenciam de outros indivíduos na sociedade pelas formas com que vivenciam as tecnologias da informação. De forma geral, como ficará evidente no quarto capítulo com a análise do conteúdo das publicações, hackers são vistos não só como intrínsecos ao paradigma tecnológico do informacionalismo, mas muitas vezes como exemplos de como a incorporação das tecnologias da informação por indivíduos, grupos ou comunidades deveria ocorrer para que seus benefícios sejam mais bem explorados.

Como os objetos de pesquisa identificados entre as publicações selecionadas para análise foram múltiplos, foi necessário criar grandes agrupamentos, cujo parâmetro para criação foi o cruzamento entre o objeto da pesquisa e o foco da análise. Seis grandes agrupamentos foram criados:

- **Comunidade/grupo/coletivo:** o objeto de estudo é uma comunidade, grupo ou coletivo e o foco da análise são práticas e dinâmicas internas;
- **Hacking em outros meios:** o objeto de estudo são as influências e impactos do ser e fazer hacker em outros meios usualmente não relacionados aos hackers (arte, música e literatura);
- **Relações entre hackers e contexto:** o objeto de estudo é o lugar dos hackers nas dinâmicas de um contexto específico (política, espaços urbanos, Internet, neoliberalismo e globalização, patriarcalismo, movimentos de resistência);
- **Relações entre hackers e outros atores:** o objeto de estudo são dinâmicas ou conflitos entre hackers e outros atores e/ou a influência dos

hackers nas ações e práticas desses outros atores (Estado, setor público, mídia, indústria, movimentos sociais, partidos políticos, sociedade civil);

- **Potencialidades:** o objeto de estudo são as potencialidades de aspectos identificados como característicos ou surgidos dos hackers (práticas, ferramentas de subversão e empoderamento, trabalho e organização) caso sejam difundidos, e;
- **Representações hackers:** o objeto de estudo são as características de manifestações hackers específicas.

O Quadro 14 apresenta o número de publicações por agrupamento de objeto de estudo:

Quadro 14 - Grandes agrupamentos de objetos de estudo

Objetos de estudo	Número de publicações	% do total
Relações entre hackers e outros atores	21	30,0
Comunidade, grupo ou coletivo	15	21,4
Relações entre hackers e contexto	10	14,3
Hacking em outros meios	8	11,4
Potencialidades	8	11,4
Representações hackers	8	11,4
Total	**70**	**100,0**

Fonte: elaboração própria com base no conjunto de publicações selecionadas.

Dois terços das publicações selecionadas se concentraram em apenas três dos seis grandes agrupamentos, mais especificamente, "relações entre hackers e outros atores", "comunidade, grupo ou coletivo" e "relações entre hackers e contexto".

No grupo "relações entre hackers e outros atores", dezesseis dos 21 artigos trataram da relação entre hackers e Estado. Neste caso, as publicações se focaram em discussões sobre legislação e marco regulatório do hacking (OJEDA-PÉREZ ET AL., 2010; AROCENA, 2012; CERQUEIRA & ROCHA, 2013; MOTA HAYASHI & FERNANDES, 2016; ALCÍVAR, BLANC & CALDERÓN, 2018; HERNÁNDEZ, BAQUERO & GIL, 2018), diferentes formas com que se dá a relação entre hackers e Estado, seja de fiscalização (TAVARES, 2001), conflito (CLEAVER, 1998; BUNKER, 2011; VON WERDER, 2016) ou influência nos desdobramentos das ações do Estado (ISLAS, ARRIBAS & MINERA, 2011; GUTIÉRREZ, 2015) e as relações entre práticas e dinâmicas hackers na implementação de

políticas públicas e mudanças na legislação (DONAS, 2007; VILLANUEVA & OLIVERTA, 2012; ALMEIDA, 2014; CHAN, 2014).

Em “comunidade, grupo ou coletivo”, foi possível agrupar doze das quinze publicações em três principais focos de análise: ação política de grupos hackers (LIMA, 2015; MACHADO, 2015; MOTA & FIGUEIREDO FILHO, 2015), características e dinâmicas de comunidades (SOLÓRZANO, 2009, COLEMAN, 2010; ZANOTTI, 2011, 2014; EVANGELISTA, 2014) e questões de gênero em comunidades/coletivos e suas relações com a tecnologia (ROCHA, 2006; PÉREZ-BUSTOS, 2010a; PAZ, 2013; ARAUJO & GITAHY, 2017).

Por fim, em “relações entre hackers e contexto”, as publicações trataram de diferentes formas com que hackers se tornam mediadores ou intermediários entre tecnologia e economia, política e sociedade (OVIEDO, 2003; SUAZA & ORTIZ, 2011; GARCÍA, 2012; JORZA, 2012; PARRA, 2012; SUAZA, 2013; VASQUÉZ, 2013; PINO, 2014; GARCÍA, 2015; NATANSOHN & PAZ, 2018).

Junto dos objetos de estudo e focos de análise, foi possível identificar alguns agrupamentos de palavras-chave com maior incidência no conjunto de publicações selecionada. De setenta publicações, apenas 45 apresentaram palavras-chave, totalizando duzentos termos. O Quadro 15 apresenta os principais agrupamentos:

Quadro 15 - Palavras-chave de maior incidência no conjunto de publicações

Termo chave	Palavras-chave relacionadas
Cibercrime	análise forense; assédio online; cibercrime; cibercriminalidade; *cracking*; crime político; crime por computador; crime por computador - Brasil; crimes cibernéticos; delito informático; delitos informáticos; fraude informática; investigação criminal; violência; vitimização
Hacker	ativismo hacker; cultura hacker; ética hacker; hackaton; hacker; hackerismo; hackers; hacking; hacking ético; hacktivismo; motivações dos hackers
Feminismo/ Gênero	ciberfeminismo; etnografia feminista; feminismo; gênero; movimentos sociais de mulheres; mulheres; mulheres e tecnologia; subjetividade feminista; tecnofeminismo; tecnologia de gênero
Tecnologias da informação e comunicação	apropriação das NTIC; apropriação de TICs; NTIC; informática; Internet; tecnologias da comunicação; TIC
Movimentos sociais	ação coletiva; movimentos sociais; movimentos sociais de mulheres; teoria dos movimentos sociais
Ciber-	ciberativismo; cibercultura; ciberespaço; ciberfeminismo; cibercrime; cibersegurança; ciberpolítica
Tecno-	tecnociência; tecnocultura; tecnofeminismo; tecnopolítica
Segurança da informação	criptografia; cuidados digitais; direito à privacidade; segurança; segurança informática
Software livre	comunidade de *software* livre; *software* livre
Arte	arte; arte e tecnologia; artes digitais; artesanato

Fonte: elaboração própria com base no conjunto de publicações selecionadas.

Ainda que a maior diversidade de palavras-chave tenha sido identificada em relação a cibercrime, a maior incidência foi em relação a "hacker" e "feminismo/gênero", seguidos por "tecnologias da informação e comunicação" e "*software* livre". As palavras-chave expressam, de alguma forma, os principais temas que os atores relacionam com seus objetos de estudo e as discussões desenvolvidas. Especificamente, esse conjunto de palavras-chave conecta hackers e hackerismos a materialidades (tecnologia da informação, *software* livre), espaços (ciberespaço e Internet) e políticas (feminismo, movimentos sociais, segurança da informação).

Por fim, foi realizado o exercício de utilizar as categorias de análise de ciclos de recuperação, propostas por Delfanti & Söderberg (2018), em uma tentativa de verificar se as categorias propostas se aplicavam às publicações selecionadas e, em caso afirmativo, identificar sob qual perspectiva temporal hackers na América Latina estão sendo estudados.

Como desenvolvido no segundo capítulo, as categorias propostas por Delfanti & Söderberg (2018) são:

- Incorporação de uma única tecnologia ou comunidade;

- Evolução dos hackers como movimento ou em relação ao contexto ou outros autores, e;
- Evolução do espírito do capitalismo.

Algumas conclusões puderam ser tiradas deste exercício. Primeiro, as categorias de Delfanti & Söderberg (2018), em termos de perspectiva temporal, são aplicáveis às publicações selecionadas, mas as escolhas não são óbvias e imediatas. Para enquadrar as publicações nas categorias, foi necessário analisar não só o objeto de estudo das publicações, mas a forma com que a análise foi desenvolvida e o teor das conclusões. Um caso exemplar é o artigo de Evangelista (2014), cujo objeto de estudo se encaixa em "comunidade, grupo ou coletivo" e, ainda que seu interesse seja o movimento de *Software* Livre no Brasil a partir das observações em uma edição do Fórum Internacional de *Software* Livre, a análise se foca tanto nas dinâmicas internas do movimento quanto nas externas de cooptação do trabalho hacker por corporações e, portanto, no direcionamento do movimento ao longo dos anos. Pelo foco da análise, o artigo foi incluído na categoria de evolução dos "hackers como movimento ou em relação ao contexto ou outros autores".

A proposição de categorias sobre ciclo de recuperação de Delfanti & Söderberg (2018) leva em consideração uma crítica recorrente nos trabalhos de Johan Söderberg sobre a dificuldade dos estudos hackers em se desprender da promessa emancipatória vinculada ao hacking. Estudar hackers e hackerismos em relação a outros autores e intervalos maiores de tempo seriam um caminho para ver esse objeto de estudo de forma crítica e entender os impactos a médio e longo prazo das práticas e dinâmicas consideradas inovativas e subversivas em seu surgimento.

Ainda que os estudos de caso do conjunto de publicações selecionadas envolvam relações com outros atores, discutam a evolução do movimento e os impactos das inovações e subversões hackers para o capitalismo, não foi notado, necessariamente, um desprendimento da promessa emancipatória do hacking. Algumas hipóteses surgem nesse aspecto. Primeiro, as publicações são um retrato de um momento específico do caso estudado e da pesquisa desenvolvida. Como poucos autores têm mais de uma publicação no conjunto selecionado, não foi possível determinar movimentos de continuidade da pesquisa realizada. Segundo, muitos dos casos estudados são recentes e, ainda que evidências de recuperação tenham sido identificadas pelos autores, os processos ainda não têm caminho determinado e não há como saber se de fato o movimento percebido se configura como recuperação – a exceção sendo o artigo de Evangelista (2014). Terceiro, mesmo em casos em que o movimento de recuperação

tenha sido identificado e amplamente estudado, existem ondas de resistência que retardam o processo ou surgem novas formas de subversão, como é o caso dos *hacklabs* e *hackerspaces*.

O Quadro 16 mostra a classificação do conjunto de publicações selecionadas nas categorias propostas.

Quadro 16 - Agrupamentos de objetos de estudo por perspectiva temporal de análise (DELFANTI & SÖDERBERG, 2018)

	Comunidade ou tecnologia	**Hackers como movimento/ outros atores**	**Espírito do capitalismo**	**Total**
Relações entre hackers e outros atores	5	13	3	**21**
Comunidade, grupo ou coletivo	12	2	1	**15**
Relações entre hackers e contexto	0	10	0	**10**
Hackear outros meios	0	8	0	**8**
Potencialidades	2	4	2	**8**
Representações hackers	3	5	0	**8**
Total	**22**	**42**	**6**	**70**

Fonte: elaboração própria com base no conjunto de publicações selecionadas.

De forma geral, a maior parte das publicações selecionadas – 42 do total de setenta publicações – trataram seus casos de uma perspectiva temporal da evolução dos "hackers como movimento ou em relação ao contexto ou outros autores". A análise menos realizada foi das relações entre hackers, suas práticas e dinâmicas com a evolução do espírito do capitalismo.

Os resultados para os agrupamentos de objetos em "relações entre hackers e outros atores", "relações entre hackers e contexto" e "comunidade, grupo ou coletivo" foram esperados: os primeiros foram melhor enquadrados no ciclo de recuperação de "hackers como movimento ou em relação a outros atores e contexto" e o último em ciclo de recuperação de uma "comunidade ou tecnologia". No caso do agrupamento de objeto "comunidade, grupo e coletivo", a exceção foi Zanotti (2011) e sua discussão sobre formas de desenvolvimento coletivo e apropriação de comunidades de *software* livre na Argentina no contexto do capitalismo informacional e as trocas que existem entre as comunidades e esse contexto. Por esse motivo, o artigo pareceu se encaixar no ciclo de recuperação sobre evolução do espírito do capitalismo.

O agrupamento de objetos "potencialidades" também apresentou resultados interessantes e oferece exemplos do exercício com as categorias de Delfanti & Söderberg

(2018). As duas publicações pertencentes à perspectiva de recuperação de "comunidade ou tecnologia" trataram de formas de organização e dinâmicas de trabalho hackers e seus impactos nas atividades e gestão da Casa de Cultural Digital de Porto Alegre (CHIESA & CABEDON, 2016) e em um grupo de profissionais brasileiros dedicados ao jornalismo *data-driven* (TRÄSEL, 2018). As quatro publicações em evolução dos "hackers como movimento ou em relação a outros atores e contexto" discorreram sobre as potencialidades de maratonas hackers para solução de problemas e criação de aplicativos no campo da saúde (GUIZARDI et al., 2018), o potencial subversivo dos métodos aplicados em *hackerspaces* para a educação (RENNO, 2015) e as potencialidades de práticas hackers e do uso da Internet para a implementação do e-México (MENDOZA, 2002) e para a formação de professores (PRETTO, 2010). Por fim, as duas publicações em evolução do "espírito do capitalismo" trataram de como os meios digitais e práticas hackers influenciam nos processos de empoderamento na sociedade contemporânea (GRAVANTE, 2012) e de como as características do trabalho hacker têm potencial de transformar como é organizado o trabalho no capitalismo (FRANÇA FILHO & AGUIAR, 2014).

É interessante que, ao explicar a categoria evolução do espírito do capitalismo, Delfanti & Söderberg (2018) utilizam como principal exemplo questões do trabalho e produção como práticas organizacionais e formas abertas de acumulação, como *open innovation*, trabalho colaborativo e plataformas para produção distribuída e compartilhamento. Porém, no caso deste conjunto de publicações, cujo foco são os hackers na América Latina, a maior parte das discussões sobre evolução do espírito do capitalismo trataram de como hackers, suas práticas e dinâmicas têm impacto nas formas de resistir às forças do capitalismo em nível global, focando-se em ciberativismo e ciberprotestos. Nestes casos existe a percepção de que essas formas de resistência são algo com que o capitalismo deve aprender a lidar. Essas análises partem de estudos sobre o levante zapatista (CLEAVER, 1998; PITMAN, 2007), a insurreição de Oaxaca (GRAVANTE, 2012) ou de discussões mais amplas sobre opressão sistêmica (VON WERDER, 2016).

Definições

O propósito em extrair e categorizar as definições sobre hackers das publicações selecionadas foi tentar identificar quais foram os parâmetros para a definição do conceito em cada caso, uma vez que, assim como na literatura consultada dos estudos hackers, as definições se mostraram múltiplas e variadas. Identificar de onde emergem as definições de

hacker permitiu, também, compará-las com aqueles existentes na literatura consultada e identificar semelhanças.

Diversos termos foram trabalhados pelos autores: hacker, hackear, hacking, hackerismo, *hackerspace*, hacktivismo, trabalho hacker, práticas hackers, aprendizado hacker. Ainda assim, foi possível identificar cinco principais origens das definições utilizadas pelos autores:

- **Entusiasmo com tecnologias da informação:** hackers são definidos como indivíduos aficionados por ou especialistas em tecnologias da informação;
- **Relação com ferramentas e tecnologias da informação:** indivíduos são definidos como hackers quando suas relações com as tecnologias da informação se dão de formas diferentes em comparação com outros indivíduos na sociedade. A ideia que perpassa as definições que se enquadram nesta categoria é de que hackers se aproximam de híbridos humanos-máquinas e sua agência e existência estão interconectadas com àquelas das tecnologias da informação;
- **Práticas – características do trabalho hacker:** indivíduos são identificados como hackers quando as especificidades e dinâmicas do trabalho que desenvolvem se assemelham àquelas identificadas como características do trabalho hacker (colaboração, compartilhamento, trabalho como algo lúdico, entre outros);
- **Práticas – características do ser hacker:** indivíduos são considerados hackers quando suas formas de ver e interagir com o mundo se assemelham àquelas identificadas como características dos hackers (subversão, resistência, transformação e apropriação de tecnologias, entre outros), e;
- **Práticas – cibercrime:** hackers como indivíduos que se aproveitam de vulnerabilidades para cometer crimes e outras formas de violência online.

Todas as definições encontradas e, em decorrência, as categorias criadas, relacionam hackers a uma materialidade específica – as tecnologias da informação. Para o conjunto de publicações selecionadas, de uma forma ou outra, esse seria o elemento em comum entre os hackers e o que os separa de outros grupos de indivíduos e objetos de pesquisa.

Além disso, as definições sobre hackers foram apresentadas de duas principais formas: utilizando referências da literatura existente ou a partir da análise dos casos estudados. O Quadro 17 exibe os resultados do cruzamento entre as duas categorias:

Quadro 17 - Parâmetros das definições de hackers por origem

	Definições existentes	**A partir do caso**	**Total**
Relação com ferramentas e tecnologias da informação	11	11	22
Práticas – características do trabalho hacker	10	10	20
Práticas – características do ser hacker	4	11	15
Práticas – cibercrime	4	3	7
Entusiasmo com tecnologias da informação	3	3	6
Total	**32**	**38**	**70**

Fonte: elaboração própria com base no conjunto de publicações selecionadas.

O Quadro 17 explicita algumas questões. A definição da maior parte das publicações (81,4% do total de setenta publicações) pôde ser enquadrada nas categorias "relação com ferramentas e tecnologias da informação", "práticas – características do trabalho hacker" e "práticas – características do ser hacker". Esses resultados também são verificados quando se analisa a literatura consultada e discutida no segundo capítulo. Em retrospecto, e considerando os parâmetros aqui criados, as definições de Eric Raymond e Pekka Himanen, por exemplo, se enquadrariam em "práticas – características do trabalho hacker", as de Gabriella Coleman, Alex Golub e Steven Levy em "práticas – características do ser hacker" e, por fim, as de Christopher Kelty, Alessandro Delfanti, Johan Söderberg e Maxigas em "relação com ferramentas e tecnologias da informação".

Quanto à origem da definição, foi verificado um equilíbrio entre a utilização de definições já existentes na literatura e definições propostas a partir dos casos estudados. A única categoria discrepante foi "práticas – características do ser hacker", em que o maior número de publicações definiu hackers a partir dos casos. Esses resultados fazem sentido em relação aos parâmetros. Se hackers são definidos por sua forma de ver e interagir com o mundo, são as especificidades de cada caso que determinam o que faz dos indivíduos ou práticas hackers.

Além da divisão entre origens a partir da literatura existente e dos casos, as definições identificadas no conjunto de publicações foram comparadas com aquelas apresentadas no segundo capítulo. No caso de definições existentes, considerou-se aquelas

citadas pelos autores, mas para as definições a partir dos casos, buscou-se observar semelhanças ou não com a literatura consultada.

A comparação entre definições rendeu dois resultados interessantes. Primeiro, dentro do grupo de definições existentes, as mais utilizadas foram as de Eric Raymond, Pekka Himanen – que retira parte da sua definição do *Jargon File*, compêndio de gírias e termos sobre tradição, folclore e humor hacker organizado por Eric Raymond – e, em menor grau, a de Manuel Castells, que também cita os outros dois autores, mas reforça a inserção dos hackers no contexto da Internet e das inovações tecnológicas. Mais especificamente em relação a Pekka Himanen:

> "Os hackers não são celebridades da TV cujos nomes são amplamente reconhecidos, mas todos já ouviram falar de suas façanhas, que constituem grande parte da base tecnológica da sociedade: a Internet e a Web (que juntas podem ser chamadas de Rede), o PC e uma parcela importante dos *softwares* utilizados nele. O arquivo de jargões dos hackers, compilado na Net, os define como 'indivíduos que se dedicam com entusiasmo à programação' que acreditam que 'o compartilhamento de informações é um bem poderoso e positivo, e que é dever ético dos hackers compartilhar suas experiências elaborando *softwares* gratuitos e facilitar o acesso a informações e a recursos de computação sempre que possível'. Assim se apresenta a ética dos hackers desde que um grupo de programadores fanáticos do MIT passaram a chamar a si próprios de hackers no início da década de 1960. (Posteriormente, em meados da década de 1980, a mídia começou a aplicar o termo para designar criminosos da informática. Para evitar essa confusão com os criadores de vírus e invasores de sistemas de computação, os hackers começaram a chamar esses usuários destruidores de *crackers*. Neste livro, observa-se esta distinção entre hackers e *crackers*)." (HIMANEN, 2001, p. 7)

Neste trecho, especificamente, Himanen (2001) retoma diversos pontos levantados por Eric Raymond – acesso e compartilhamento de conhecimento, colaboração para criação, hacker como um entusiasta e especialista em tecnologia da informação – e reforça o que considera como características centrais do trabalho hacker: seu caráter aparentemente voluntário e a existência de uma relação prazerosa e desafiadora entre hacker e hacking.

Dessa forma, também não foi inesperado que a maior parte das publicações que utilizou dos conceitos de Raymond, Castells e Himanen ou cuja definição a partir dos casos apresentou semelhanças com esses três autores estavam nas categorias "práticas – características do trabalho hacker" e "entusiasmo com tecnologias da informação". Particularmente na primeira categoria, as definições de hackers trouxeram questões como trabalho como um processo criativo, desafiador e prazeroso; trabalho hacker como voluntário e colaborativo; centralidade do compartilhamento; conhecimento técnico profundo em tecnologias da informação; meritocracia, e; foco em encontrar soluções técnicas.

Um segundo resultado interessante foram as semelhanças encontradas entre as definições a partir dos casos com os preceitos da ética hacker observados por Levy (1984). Esses preceitos, de forma geral, estão mais relacionados com o ser hacker que emergia das práticas e dinâmicas nos laboratórios do MIT nos anos 1950 e menos com as especificidades do trabalho hacker, depois restringido nos textos de Eric Raymond. Seguidos dos preceitos estão os elementos semelhantes que foram utilizados para definir hackers no conjunto de publicações selecionadas:

- *Access to computers – and anything which might teach you something about the way the world works – should be unlimited and total. Always yield to the Hands-On Imperative!*: curiosidade e exploração como meios de aprendizado, criar tecnologias para que sejam adaptadas, modificadas, consertadas pelos usuários, garantir processos próprios de aprendizagem, intervir, afetar, apropriar, integrar de forma criativa os recursos livres na rede, encontrar solução para problemas técnicos de forma astuta;
- *All information should be free*: informação livre e tecnologias livres, posicionamento transgressivo direcionado à liberdade e disseminação de informação através do desenvolvimento de código, defesa da livre distribuição e acesso a tecnologias da informação alternativas aos monopólios e à arte e ciência;
- *Mistrust authority – promote decentralization*: compartilhar, acolher a participação, não controlar e devolver controle, auto-organização cooperativa, e;
- *Computers can change your life for the better [...] like Aladdin's lamp, you could get it to do your bidding*: explorar novas formas de vida, promover sociedade mais democrática e aberta, tecnologias da informação como formas de sobrevivência e expansão de modos de vida.

Dentro do grupo de definições a partir do caso, semelhanças com a ética hacker de Levy (1984) foram encontradas em publicações enquadradas em "relação com ferramentas e tecnologias da informação" e "práticas – características do ser hacker" tiveram. Em apenas dez publicações do grupo de definições a partir do caso não foram encontradas semelhanças com a literatura existente, sendo cinco deles em "relação com ferramentas e tecnologias da informação" (CLEAVER, 1998; HERRERA & GARRIDO, 2011; VASQUÉZ, 2013; GUTIÉRREZ, 2015; NATANSOHN, 2018), quatro em "práticas – características do ser

hacker" (RONFELDT & MARTÍNEZ, 1997; BUNKER, 2011; GARCÍA, 2012; LIMA; 2015) e um em "práticas – a características do trabalho hacker" (JOLÍAS & PRINCE, 2013).

Considerando outras categorias de análise, foi possível identificar algumas correspondências entre três agrupamentos de objetos de estudo e as definições sobre hackers. Das quinze publicações do agrupamento "comunidade, grupo ou coletivo", em dez delas hackers foram definidos a partir das práticas, sendo quatro em "práticas – características do ser hacker" (PÉREZ-BUSTOS, 2010a; 2010b; EVANGELISTA, 2014; LIMA, 2015) e seis em "práticas – características do trabalho hacker" (SOLÓRZANO, 2009; ZANOTTI, 2011; 2014; DÍAS & SEGURA, 2013; ARAUJO & GITAHY, 2017; NÚNEZ, 2017); das oito publicações em "hacking em outros meios", em cinco delas hackers foram definidos em "relação com ferramentas e tecnologias da informação" (FERNÁNDEZ, 2011; HERRERA & GARRIDO, 2011; MILLS, 2012; GAINZA C., 2016; PEDERSON, 2016), e; das oito publicações em "potencialidades", em cinco hackers foram definidos a partir das "práticas – a características do trabalho hacker" (MENDOZA, 2002; FRANÇA FILHO & AGUIAR, 2014; RENNO, 2015; GUIZARDI et al., 2018; TRÄSEL, 2018).

Essas correspondências fazem sentido ao pensar nos parâmetros para cada categoria. Se o objeto de estudo é uma comunidade, grupo ou coletivo e o foco da análise são práticas e dinâmicas principalmente internas, as manifestações de hackers e hackerismos podem emergir do funcionamento e organização daquele meio, sejam das especificidades do trabalho ali desenvolvido ou pela forma com que aquele grupo de indivíduos vê e interage com o mundo ao redor. Da mesma forma, em "hacking em outros meios", os objetos de estudo são as influências e impactos do fazer ou ser hacker para outros meios, de forma que hackers não necessariamente são o cerne da análise, mas são as características consideradas hackers que atravessam esses outros meios e transformam suas práticas e atividades. Uma das principais características, e o que faz com que seja possível essa transposição, é a relação diferenciada dos indivíduos com as ferramentas e tecnologias da informação. Por fim, o trabalho é uma das questões relacionadas ao hackerismo mais discutidas tanto pelo impacto dos textos de Eric Raymond e Pekka Himanen quanto por ser uma inovação em termos de organização e motivações para engajamento em atividades produtivas, o que o torna de grande interesse às grandes corporações. Dessa forma, não é surpreendente que, ao discutir potencialidades, a maior parte das definições para hackers partam das "práticas – características do trabalho hacker".

As políticas hackers

Assim como para os objetos de estudo e as definições de hackers, foram criadas categorias de análise para as políticas hackers identificadas no conjunto de publicações. O exercício para a criação dessas categorias não foi apenas de extração de conteúdo porque as políticas hackers não necessariamente são o objeto das publicações. Além disso, como tratado anteriormente, políticas hackers não se manifestam apenas como ativismo ou ação direta, mas estão entremeadas às práticas, tecnologias e dinâmicas das comunidades.

Partindo da análise realizada pelos autores, para a tentativa de identificação das políticas hackers buscou-se recuperar o conceito apresentado anteriormente – formas de disputar o ordenamento o mundo através do reordenamento de tecnologias da informação e suas infraestruturas – e a questão de pesquisa sobre quais seriam características das políticas hackers na América Latina. As categorias foram criadas com base nas análises realizadas pelos autores, principalmente em relação às relações, conflitos e disputas identificadas. Isto posto, as categorias criadas foram:

- **Outras formas de fazer política pública, influenciar tomada de decisões ou se expressar politicamente:** as políticas emergem da interação entre práticas, dinâmicas, táticas e ferramentas hackers e as arenas políticas tradicionais (tomada de decisão, formulação de políticas públicas, disputas, conflitos, lutas por direitos, intersecções com movimentos sociais);
- **Políticas do dia-a-dia:** as políticas emergem das práticas e dinâmicas dos hackers em suas atividades cotidianas e em espaços de socialização e dos fatores e características que os tornam hackers e garantem sua existência como tal;
- **Resistências:** as políticas emergem nos e dos atos de resistência contra apropriações, opressões, violência, controle, entre outros;
- **Transposição do ser hacker para outros meios:** as políticas emergem da transferência/apropriação de elementos considerados característicos do ser e fazer hacker para/em outros meios (arte, literatura, música, corporações, meios urbanos), e;
- **Violência e ilegalidade:** as políticas emergem dos atos ilegais e violentos e das controvérsias relacionadas à criminalização de práticas hackers.

Em todas as formas de emergência das políticas hackers, as tecnologias da informação estiveram presentes, seja como parte das táticas de engajamento político, como facilitadoras da organização e empoderamento ou como intrínsecas a tudo o que é hacker.

O Quadro 18 apresenta os resultados:

Quadro 18 - Emergência das políticas hackers

	Número de publicações	**% do total**
Políticas do dia-a-dia	21	30,0
Resistências	15	21,4
Transposição do ser hacker para outros meios	15	21,4
Outras formas de fazer política pública, influenciar tomada de decisões ou se expressar politicamente	11	15,7
Violência e ilegalidade	8	11,4
Total	**70**	**100,0**

Fonte: elaboração própria com base no conjunto de publicações selecionadas.

A decisão por definir as categorias com base na análise realizada pelos autores está alinhada com as perguntas de pesquisa – como os estudos de casos sobre hackers da América Latina contribuem com o conhecimento sobre políticas hackers e como os pesquisadores estão olhando para essa temática – porque permite identificá-las pela perspectiva dos pesquisadores. O Quadro 18, portanto, começa a apresentar algumas especificidades do conhecimento gerado sobre hackers na América Latina.

Quando hackers e aspectos relacionados são objetos de estudo, é coerente que as análises se foquem em práticas e dinâmicas dos hackers em suas atividades cotidianas, particularmente, nos fatores e características que os tornam hackers e garantem sua existência como tal, como em "políticas do dia-a-dia". Análises como a de Kelty (2005), Coleman & Golub (2008) e Maxigas (2017), por exemplo, se encaixariam nesta categoria. Isso não implica que os hackers ainda sejam vistos como especialistas exóticos fechados em si mesmos pelos pesquisadores, mas mostra que o comportamento apolítico dentro das comunidades, grupos e coletivos não deve ser generalizado e que justificativas como autossatisfação e diversão não são suficientes para entender por que hackers engajam em suas atividades ou politicamente. Ao mesmo tempo, também abre a possibilidade de que as políticas hackers não sejam apenas aquelas de grupos que usam de táticas de desobediência civil eletrônica, como os Anonymous.

Particularmente para essa categoria, foi possível identificar três fatores que influenciaram nas práticas e dinâmicas dos hackers estudados: questões de gênero, outros modos de vida e dinâmicas internas das comunidades. No primeiro caso, ficou evidente nas publicações que no ser hacker está considerado o ser mulher: as práticas e dinâmicas hackers são construídas junto da percepção do ser mulher no mundo. Aqui, as políticas tomam forma de cuidados digitais, construção de espaços seguros, proteção na rede e de coletivos ativistas, construção de tecnologias feministas, entre outras. Portanto, neste caso, gênero e questões relacionadas estão na essência do público recursivo (ROCHA, 2006; PÉREZ-BUSTOS, 2010a; 2010b; SUAZA & ORTIZ, 2011; PAZ, 2013; SUAZA, 2013; ARAUJO & GITAHY, 2017; NATANSOHN, 2018; NATANSOHN & PAZ, 2018). No segundo caso, os autores pareceram compreender que as atividades cotidianas dos hackers como outros modos de vida, em outras palavras, formas de vivenciar o hackerismo de forma diferente (COLEMAN, 2010; ALMEIDA, 2014; FRANÇA FILHO & AGUIAR, 2014; GARCÍA, 2015; BORGES, 2018). Outras publicações se focaram nas políticas que emergem dentro das comunidades (SOLÓRZANO, 2009; ZANOTTI, 2011, 2014; BARON, 2014; EVANGELISTA, 2014; RENNO, 2015; NÚÑEZ, 2017).

Outra divisão interessante foi observada na categoria “resistências”. No segundo capítulo foram apresentadas várias formas em que o ser e fazer hacker se configuram como formas de resistência contra censura e outras formas de bloqueio à livre circulação de informações, além da centralidade do antiautoritarismo para a subjetividade política dos hackers. Para o conjunto de publicações sobre hackers na América Latina, as resistências foram contra apropriação por culturas dominantes, opressões e agressividade do capitalismo informacional, violência estatal e formas de controle e vigilância massiva do Estado e corporações. Porém, o mais interessante foi que as resistências não partiram apenas da perspectiva do indivíduo (OVIEDO, 2003; REDONDO, 2005; BROWN, 2006; MAGUIRE, 2009; JORZA, 2012; PINO, 2014; MACHADO, 2015; MOTA & FIGUEIREDO FILHO, 2015; VON WERDER, 2016), como é o caso das discutidas na literatura consultada, mas da perspectiva da soberania nacional (GUTIÉRREZ, 2015) e de povos tradicionais e indígenas (NELSON, 1996; RONFELDT & MARTÍNEZ, 1997; CLEAVER, 1998; PITMAN, 2007; GRAVANTE, 2012), conectando essas resistências, muitas vezes, aos movimentos antiglobalização.

Em “transposição do ser hacker para outros meios”, os autores trataram de como a transposição e absorção de elementos do ser e fazer hacker tornaram-se essenciais para a transformação de outros meios (arte, literatura, música, corporações, meios urbanos). Os

elementos identificados como transpostos foram a apropriação, experimentação, subversão, redes de colaboração e comunicação e organização não hierárquica (ENTEEN, 2007; PRETTO, 2010; FERNÁNDEZ, 2011; HERRERA & GARRIDO, 2011; GARCÍA, 2012; MILLS, 2012; DÍAZ & SEGURA, 2013; LEDESMA, 2015; LIMA, 2015; SCHÄFER, 2015; CHIESA & CAVEDON, 2016; GAINZA C., 2016; PEDERSON, 2016; GUIZARDI et al., 2018; TRÄSEL, 2018)

A categoria "outras formas de fazer política pública, influenciar tomada de decisões ou se expressar politicamente" surgiu principalmente como uma segunda forma de emergência de políticas hackers em conexão com a categoria "resistência". Porém, nos casos em que foi identificada como a forma primária das políticas, as discussões realizadas giraram em torno dos usos de ferramentas de tecnologia da informação para fomentar governo aberto como forma de participação cidadã, além de outras sobre a utilização elementos considerados característicos dos hackers como racionalidade de políticas públicas (MENDOZA, 2002; DONAS, 2007; ISLAS, ARRIBAS & MINERA, 2009; BUNKER, 2011; TAVARES, 2011; PARRA, 2012; VILLANUEVA & OLIVERA, 2012; JOLÍAS & PRINCE, 2013; VAZQUÉZ, 2013; CHAN, 2014; MOTA, HAYASHI & FERNANDES, 2016).

Em "violência e ilegalidade", as políticas hackers foram restringidas a cibercrimes, ódio e violência online e os hackers reduzidos a criminosos. Em sua maioria, as análises realizadas buscaram demonstrar que o comportamento malicioso desses atores é ampliado por mediação das tecnologias da informação, dificultando a responsabilização pelos crimes e causando danos a indivíduos, corporações e governos. Em algumas publicações também foram discutidas as controvérsias trazidas pelas práticas hackers e como as tecnologias da informação apresentam à legislação novos desafios em relação à regulamentação de crimes cibernéticos (GACHARNÁ G., 2009; RUIZ, SEGURA & QUESADA, 2009; OJEDA-PÉREZ et al, 2010; AROCENA, 2012; CERQUEIRA & ROCHA, 2013; RODRÍGUEZ, ODUBER & MORA, 2017; ALCÍVAR, BLANC & CALDERÓN, 2018; HERNÁNDEZ, BAQUERO & GIL, 2018).

Não foi possível encontrar correlações relevantes entre as três categorias criadas (objeto de estudo, definições e emergência das políticas hackers), considerando-as juntas. Novamente, é preciso lembrar que tanto as definições quanto as políticas são múltiplas, mesmo dentro de uma mesma categoria. Ainda assim, entre definições e políticas foram identificados alguns agrupamentos.

Dez das quinze publicações em "resistências" definiram hackers e hackerismos a partir da "relação com ferramentas e tecnologias da informação". Essa correspondência faz

sentido quando se entende que as políticas hackers emergem nos e dos atos de resistência contra apropriações, opressões, violência, controle, de forma que conhecimento e apropriação das tecnologias da informação se tornam ferramentas de luta. As definições de Nelson (1996) e Machado (2015) exemplificam essa correspondência.

> "*Hacking is about the understanding and control of information technologies and, most importantly, the ability to form networks for communication and information sharing. When I joke about the Maya hacker, I am thinking about the vital importance of information and networking to the political strategies of the indigenous cultural rights movement.*" (NELSON, 1996, p. 291)

> "Enquanto as primeiras gerações de hackers estavam centradas nas políticas relacionadas a *softwares* e *hardwares*, os hacktivistas transpuseram mais claramente esse caráter político ao plano social, realizando ações diretas de desobediência civil. Assim, o ativismo hacker pode ser definido como o uso de ferramentas digitais tendo em vista fins exclusivamente políticos, que não raro são logrados de maneiras transgressivas e/ou disruptivas. De forma mais ampla, trata-se da junção das ferramentas e conhecimentos técnicos encontrados no hacking e de uma forma especial de ativismo político – realizado por meio das redes digitais." (MACHADO, 2015, p. 1533)

Onze das 21 publicações em "políticas do dia-a-dia" definiram hackers e hackerismos a partir das "práticas – características do trabalho hacker". Se as políticas emergem das práticas e dinâmicas dos hackers em suas atividades cotidianas e do que os tornam hackers e garantem sua existência como tal, é razoável que hackers sejam vistos a partir da forma com que realizam o trabalho. Um exemplo interessante vem de França Filho & Aguiar (2014), que discutem o trabalho hacker em uma comunidade brasileira para desenvolvimento de um sistema:

> "a dinâmica de trabalho adotada pelos hackers estaria, de forma geral, fundada numa espécie de engajamento eminentemente voluntário e não-contratual. Este trabalho voluntário, segundo tal pressuposto, não estaria sendo empreendido conforme princípios instrumentais e individualistas, mas sim sob princípios de liberdade e obrigação intimamente imbricados, por meio dos quais se realiza um objetivo comum: o desenvolvimento e a distribuição de um sistema computacional livre." (FRANÇA FILHO & AGUIAR, 2014, p. 108).

Uma correspondência óbvia entre as categorias de definições e política se deu entre "violência e ilegalidade" e "práticas-cibercrime". Nas publicações da primeira categoria, em que as análises se focaram em comportamentos maliciosos mediados por tecnologias da informação e as controvérsias e desafios que os delitos informáticos trazem para a legislação, a maior parte delas entendeu hackers e hackerismos pelo conceito de *cracker*, semelhante ao de Eric Raymond.

Por fim, exceto por uma, todas as publicações em que as políticas hackers emergem da "transposição do ser hacker para outros meios" dividiram-se principalmente entre as definições a partir de "práticas – características do ser hacker", "práticas – características do trabalho hacker" e "relação com ferramentas e tecnologias da informação". Esta categoria é bastante interessante e as três formas de definição são coerentes, uma vez que os meios em questão, inicialmente, não são hackers em si, mas tornam-se hackers pela adoção de práticas e características vinculados a eles. Fernández (2011) ajuda a exemplificar essa correspondência em relação a um estilo de *netart*, a arte hacker:

> *"Otra de las características del arte hacker es la práctica del entorpecimiento, se rebelan contra las utilidades de las aplicaciones de la red haciéndolas más lentas, programando fallos, llevándolas a caminos sin salida, manifestando con ello la diferencia entre un artista y un programador creativo que tiene su horizonte en una funcionalidad más o menos estética."* (FERNÁNDEZ, 2011, p. 93).

As cinco categorias aqui criadas para políticas hackers deram base à análise realizada no quarto capítulo, onde o conteúdo das publicações foi explorado mais profundamente a fim de identificar as características das políticas hackers na América Latina.

CAPÍTULO 4 – As políticas hackers segundo os estudos de caso sobre a América Latina

Junto do terceiro capítulo, este se configura como parte da síntese proposta pela Revisão Sistemática de Bibliografia, porém, enquanto o primeiro compôs um panorama do conjunto das publicações, a proposta deste capítulo é explorar mais profundamente o conteúdo das publicações selecionadas e sistematizadas através de revisão e comparação. Nesse sentido, o objetivo foi acumular achados que ajudem na identificação das características das políticas dos hackers na América Latina a partir das análises desenvolvidas pelos autores do conjunto de publicações selecionadas e, assim, determinar quais são as contribuições dos estudos de caso sobre hackers na América Latina para os estudos hackers em geral.

Desta forma, as categorias de análise criadas para identificar como as políticas hackers emergem foram o ponto de partida para a análise desenvolvida aqui. Este capítulo está dividido em: i) resistências; ii) políticas do dia-a-dia; iii) transposição do ser hacker para outros meios; iv) outras formas de fazer política pública, influenciar tomada de decisões ou se expressar politicamente; e v) violência e ilegalidade[41]. As publicações selecionadas foram analisadas em relação às outras da mesma categoria e em relação à literatura utilizada no estudo de escopo. É interessante apontar que os casos apresentados e as análises voltaram-se principalmente para a identificação de dinâmicas, descrição de atividades, apontamento de tendências e possíveis direcionamentos e menos para a construção de teorias mais gerais sobre hackers e hackerismos a partir dos casos. Por esse motivo, muitos dos itens aqui construídos trazem exemplos dos casos estudados pelo conjunto de publicações selecionadas.

4.1 Resistências: ação coletiva, autonomia e o direito de existir

Em comparação com a literatura consultada para a elaboração do segundo capítulo, em que as resistências do ser e fazer hacker emergem contra censura e outras formas de bloqueio à livre circulação de informações, para o conjunto de publicações selecionadas sobre hackers na América Latina, as resistências foram contra a apropriação por culturas dominantes, opressões e agressividade do capitalismo informacional, violência estatal e formas de controle e vigilância massiva do Estado e corporações. O antiautoritarismo, um dos elementos da subjetividade política dos hackers (COLEMAN, 2017), foi identificado também

[41] Neste capítulo, optou-se por alternar as posições entre políticas do dia-a-dia e resistência porque, nesta última, são desenvolvidas discussões que apareceram em outros itens.

entre os diferentes casos e apareceu de formas diversas, relacionado com a perspectiva dos atores que conformam as resistências. Neste sentido, verificou-se duas grandes fontes de resistência: uma mais relacionada a movimentos populares e outra referente à resistência individual contra a sociedade de controle.

Movimentos populares e resistência de povos tradicionais

As publicações que tratam dos casos de resistência de povos tradicionais englobam três das mais antigas sobre hackers na América Latina "*Maya Hackers and the Cyberspatialized Nation-State: Modernity, Ethnostalgia, and a Lizard Queen in Guatemala*" (NELSON, 1996), "*A comment on the zapatista 'netwar'*" (RONFELDT & MARTÍNEZ, 1997) e "*The Zapatistas and the Eletronic Fabric of Struggle*" (CLEAVER, 1998). De alguma forma, essas publicações identificam algumas das origens dos hackers na América Latina que datam a segunda metade dos anos 1980 e o começo dos anos 1990: os maias hackers da Guatemala e o levante zapatista no México.

A análise realizada por Diane Nelson identificou que as características do modo de existir no mundo do povo maia e a forma com que são vistos pelo restante da sociedade guatemalteca se apresentam através de binarismos entre elementos pré-modernos e modernos. Nesse sentido, ao mesmo tempo em que o povo maia é visto como atrasado, avesso ao progresso, uma representação daquilo que a nação não quer ser, também há estranhamento e sentimento de impropriedade quando incorporam tecnologias da informação em seu dia-a-dia.

> *"In fact, the binary semiotics of identity in Guatemala mean you cannot be both Indian and modern. Ladino (nonindigenous) identity is defined as modern in terms of technology, lifeways, and so on. Because centuries of mestizaje have made it difficult to tell an indigenous person from a non-Indian, the categories are marked culturally. Thus, any indigenous person who speaks Spanish, has earned an academic degree, or holds a desk job has historically been redefined as ladino."* (NELSON, 1996, p. 288)

Nelson (1996) parte sua análise da pesquisa etnográfica que realizou na metade dos anos 1980 em Nebaj, na Guatemala, enquanto investigava os efeitos da guerra civil em populações indígenas. O que a autora chama de maias hackers são ativistas dos direitos culturais maias que se recusam a sofrer ladinização (apropriação cultural pela cultura dominante não-indígena). Isso porque, como hackers de computador que desenvolvem conhecimentos profundos sobre tecnologias e códigos enquanto trabalham com um sistema que não lhes pertencem ou podem controlar, os maias se apropriaram de tecnologias da

informação e conhecimentos modernos como forma de recusar a apropriação pela nação ladina. Por estarem conectados a elementos considerados tradicionais e atrasados, quando os maias hackers apropriam e usam tecnologias da informação, que são símbolos da modernidade e do progresso, há uma invasão, um sentimento de impropriedade, de que esses povos e movimentos não pertencem ao urbano, ao moderno, ao futuro.

> *"[..] as Maya hackers, by contrast, and reprogramming such familiar binary oppositions as those between past and future, between being rooted in geography and being mobile, between being traditional and being modern, between manual labor and white-collar technology/information manipulation, between mountain shrines and mini malls, and between unpaved roads and the information superhighway. Thinking of the site of this reprogramming work as the cyberspatialized nation-state foregrounds the importance of information and representation in the work of the Mayan activists and in the production of an imagined community like the Guatemalan nation."* (NELSON, 1996, p. 289)

Os maias hackers, portanto, usam das tecnologias da informação para hackear binarismos. Quando Nelson (1996) coloca os ativismos nesses termos, busca evidenciar a importância da informação e da formação de redes de colaboração e compartilhamento para as estratégias políticas dos movimentos ativistas de direitos culturais[42].

Como parte do movimento de resistência à ladinização observado por Nelson (1996), os maias hackers combinam ciência e tecnologia modernas com conhecimento maia tradicional, usando da linguagem (alfabetização, recuperação de línguas indígenas e informação), publicações, educação, bibliotecas, rádio e computadores para garantir sobrevivência cultural, educar a população maia e disputar opressões raciais, econômicas e políticas. Nelson (1996) deixa claro que os maias hackers não querem tomar o poder do Estado, mas "*like hackers who work in the interstices of computer networks, the Maya hackers are creating spaces for themselves inside the state*." (NELSON, 1996, p. 294).

É bastante interessante que Nelson (1996) também aponta que os maias hackers compartilham de outros elementos observados entre hackers, mais notadamente as políticas de gênero. Segundo a autora, assim como entre hackers, mulheres estão pouco presentes entre os ativistas de direitos culturais maias.

Quanto aos zapatistas, Ronfeldt & Martínez (1997) e Cleaver (1998) descrevem alguns dos eventos que transcorreram durante o levante em 1994, mas focam-se em elementos diferentes: enquanto os primeiros tratam de especificidades do conflito e dos seus significados

[42] O próprio termo "maia", de acordo com Nelson (1996), foi reprogramado pelos ativistas para representar uma tentativa de formar uma identidade pan-indígena em nível nacional.

para a governabilidade do Estado mexicano, Cleaver (1998) reforça a centralidade das tecnologias da informação para o levante. Segundo Ronfeldt & Martínez (1997):

> *"On New Year's Day 1994, some two to four thousand insurgents of the Zapatista National Liberation Army (EZLN) occupied six towns in Chiapas, declared war on the Mexican government, proclaimed radical demands, and mounted a global media campaign for support and sympathy. Through its star-quality spokesman 'Subcomandante Marcos', the EZLN broadcast its declarations through press releases, conferences, and interviews, and invited foreign observers and monitors to Chiapas. The Mexican government's initial reaction was quite traditional. It ordered army and police forces to suppress the insurrection, and downplayed its size, scope, and sources, in keeping with official denials in 1993 that guerrillas existed in Chiapas."* (RONFELDT & MARTÍNEZ, 1997, p. 369)

Com a ocupação das cidades, de acordo com Ronfeldt & Martínez, o Exército Zapatista de Liberação Nacional (EZLN) chamou uma reunião coletiva de imprensa para esclarecer que suas raízes eram os povos tradicionais do México e não tinham conexão com os revolucionários da América Central. Dentre as demandas do movimento estavam: respeito pelos povos tradicionais, renúncia do presidente mexicano como caminho para alcançar uma verdadeira democracia, a instalação de uma transição governamental multipartidária, eleições justas e legítimas e realização de reformas sociais e econômicas, incluindo a revogação de um artigo sobre regularização da propriedade sobre a terra criado no espírito do Tratado Norte-Americano de Livre Comércio (NAFTA) que buscava privatizar as terras, criando um mercado competitivo em nome da atração de investimento na agricultura. Nesta oportunidade, os zapatistas também convidaram a sociedade civil a se juntar na luta a favor de reformas econômicas, políticas e sociais e organizações internacionais de direitos humanos a monitorarem o conflito nas Chiapas. Em resposta, Cleaver (1998) assinala que o Estado mexicano tentou restringir o levante às Chiapas através da repressão militar, resultando em centenas de mortes, torturas, estupros e outras violências, da limitação da cobertura jornalística, uma vez que o monopólio midiático era controlado pelo Estado, e do impedimento da entrada de ativistas de direitos humanos.

O levante zapatista e a resposta violenta do Estado mexicano causou a mobilização de diversas organizações não governamentais (ONGs) internacionais pró-direitos humanos e direitos indígenas. Esses atores, utilizando táticas não violentas, invadiram massivamente o México com ocupações virtuais (em sites institucionais) e físicas (nos prédios e outras estruturas governamentais), mostrando solidariedade às demandas do EZLN e pressionando pelo cessar-fogo, pela retirada das forças militares das Chiapas e pelo início das negociações com os zapatistas e reformas democráticas, além de exigir a entrada das ONGs

para monitoramento das condições de direitos humanos durante o conflito (RONFELDT & MARTÍNEZ, 1997).

Ronfeldt & Martínez (1997) têm duas contribuições interessantes: o enquadramento do levante zapatista e seus desdobramentos como uma *social netwar* e a discussão sobre o papel das ONGs internacionais, que consideram a grande novidade do conflito.

Quanto ao primeiro, Ronfeldt & Martínez (1997) trazem o termo *social netwar* para analisar os eventos ocorridos na Chiapas:

> *"The term netwar refers to conflict (and crime) at societal levels where the protagonists rely on network forms of organization, and related doctrines, strategies, and technologies. The term was coined (Arquilla & Ronfeldt, 1993) to focus attention on the likelihood that network-based social conflict and crime, involving measures short of war, would increase and become a major, widespread phenomenon in the decades ahead. Thus the term is both a tool and a prediction. It reflects assessments that the information revolution is about organizational design as well as technological prowess, and that this revolution favors whoever can master the network form."* (RONFELDT & MARTÍNEZ, 1997, p. 372)

Portanto, *social netwars* seriam uma nova forma de protesto de grupos que já se organizam de forma não-hierárquica e acabam utilizando a rede e outras tecnologias da informação como ferramentas para comunicação, organização e outras instrumentalidades. Nesse sentido, no caso das *social netwars,* os conflitos pré-datam a utilização das tecnologias da informação, e não são decorrência delas[43]. Em termos de táticas, Pitman (2007) comenta que alguns aspectos das *social netwars* vinculados ao ciberespaço compartilham táticas vinculadas ao hacktivismo, como aquelas de desobediência civil eletrônica (ocupações virtuais, bombardeamento de e-mails, desfiguração de sites e formas de *netart*), além de outros usos como formação de redes de colaboração. O levante zapatista se caracterizaria como exemplo de políticas hackers pelas características do conflito e as táticas utilizadas em seu desdobramento.

Para Ronfeldt & Martínez (1997), a participação massiva das ONGs internacionais e suas táticas de desobediência civil eletrônica, a ponto de rivalizar o Estado mexicano, teriam sido as novidades do conflito nas Chiapas. Os autores apontam que a infraestrutura para ação das ONGs já estava presente no México depois das ondas de ativismo

[43] O conceito de *social netwar*, portanto, é diferente daquele de *cyberwar* também cunhado por David Ronfeldt e John Arquilla em 1993 para se referir à guerra militar orientada à informação, em que táticas incluem a utilização da rede para divulgar propaganda e desinformação, assim como hackear os sistemas dos inimigos no contexto de guerra declarada entre Estados (PITMAN, 2007). Pitman (2007) reforça que, uma vez que Ronfeldt e Arquilla são estrategistas militares, as discussões que levantam sobre *cyberwars* e *social netwars* têm como objetivo entender o funcionamento dos conflitos e encontrar forma de suprimi-los.

anti-NAFTA no começo dos anos 1990. Quando do levante zapatista, dois tipos de ONGs foram essenciais para seus desdobramentos. Primeiro, as ONGs orientadas especificamente para problemas relacionados às causas do conflito, como aquelas de direitos humanos e indígenas, ambientalistas e voltadas ao desenvolvimento humano. Segundo, aquelas que constroem e proveem infraestrutura, assim como qualquer outro suporte, para ONGs e ativistas e são especializadas em facilitar a formação de redes de comunicação, a organização interna e de eventos, entre outros. Dentre elas, a principal teria sido a *Association for Progressive Communications* (APC), que conecta várias redes de comunicação de ONGs ativistas pelo acesso à Internet e garante a comunicação e coordenação entre essas redes e suas atividades, potencializando o volume de participantes envolvidos em táticas de desobediência civil eletrônica e outras formas de protesto.

> *"In short, the NGOs' activism altered the dynamics of the confrontation in Chiapas and helped convert a military confrontation into a political one. It assured that what might once have remained a provincial event became a national and international event. It affected the context for decisionmaking in Mexico City; it helped impel the government to dialogue and negotiate with the EZLN; it helped keep the military at bay; and it put unusual pressures on the political system to become more democratic."* (RONFELDT & MARTÍNEZ, 1998, pp. 381-382)

Cleaver (1998), por sua vez, traz a discussão para o papel das tecnologias da informação na luta do EZLN e seus aliados. Ao contrário de Ronfeldt & Martínez (1998), Harry Cleaver não trata das táticas características da *social netwar*, que são próximas àquelas da desobediência civil eletrônica, mas das redes, que permitem compartilhamento de informações e facilitam a organização dos movimentos sociais.

> *"In the narrow terms of traditional military conflict, the Zapatista uprising has been confined to a limited zone in Chiapas. However, through their ability to extend their political reach via modern computer networks the Zapatistas have woven a new electronic fabric of struggle to carry their Revolution throughout Mexico and around the world [...] Despite its initial defeat, a key aspect of the state's war against the Zapatistas (both in Mexico and elsewhere) has been its on-going efforts to isolate them, so that they can be destroyed or forced to accept co-optation. In turn, the Zapatistas and their supporters have fought to maintain and elaborate their political connections throughout the world. This has been a war of words, images, imagination and organization in which the Zapatistas have had surprising success."* (CLEAVER, 1998, p. 1)

Quando Cleaver (1998) destaca que a guerra dos zapatistas é de palavras, imagens, imaginação e organização, a informação é colocada no centro do conflito e, com ela, as tecnologias que permitem sua criação e difusão. Nesse sentido, o uso das tecnologias da informação parece ser condição para o levante do EZLN ao invés de um dos seus

desdobramentos, como argumentam Ronfeldt & Martínez (1997), para quem as tecnologias se configuram como infraestrutura de um conflito existente e não seu centro.

Ainda que sejam mencionadas outras táticas comuns a movimentos sociais como a realização de palestras, a publicação de artigos em imprensa alternativa, demonstrações e ocupações, faz sentido que o foco de Cleaver (1998) seja as tecnologias da informação, uma vez que o autor está interessado em apresentar o exemplo zapatista como o modelo de uma nova forma de luta que acontece no ciberespaço, ainda que às vezes o faça em detrimento do conflito *in loco*. Os ativistas e movimentos sociais estariam se apropriando de tecnologias comumente utilizadas pela coordenação de operações produtivas e financeiras de corporações transnacionais para compartilhar experiências, difundir informações, discutir sobre suas lutas e táticas alternativas, além de coordenar estratégias de ação.

No caso do levante zapatista, para Cleaver (1998), o papel das tecnologias da informação, por intermédio dos apoiadores do movimento, foi garantir a livre circulação e discussão de posicionamentos políticos e alternativas, fazendo com que os comunicados, cartas, manifestos e toda informação originada pelo EZLN fossem difundidos pelo México e internacionalmente.

> *"What they did was very simple: they typed or scanned the communiques and letters into e-text form and sent them out over The Net to potentially receptive audiences around the world [...] Again and again, friendly and receptive readers spontaneously re-posted the messages in new places while sometimes translating the Spanish documents into English and other languages. In this way, the words of the Zapatistas and messages of their communities have been diffused from a few gateways throughout much of cyberspace."* (CLEAVER, 1998, p. 7)

Cleaver (1998) conclui que a experiência nas Chiapas traz novos elementos para as lutas dos movimentos sociais. A mobilização e organização não-hierárquica permitida pelo uso de redes alternativas e pela Internet, que Cleaver (1998) chama de *electronic fabric of struggle*, aumentaria a complexidade dos conflitos, que graças a livre circulação de ideias passaria a ter impactos políticos, econômicos e sociais mais abrangentes. Seria por esse motivo que as reflexões sobre o levante Zapatista, de acordo com o autor, também trouxeram novas estratégias aos Estado e corporações nas tentativas de evitar outros levantes, dentre elas a censura e o controle do fluxo de informações através da privatização e comercialização da Internet.

Dez anos depois das publicações de David Ronfeldt[44] e Harry Cleaver, Thea Pitman buscou em "*Latin American Cyberprotest: before and after the Zapatistas*" tratar de questões que foram negligenciadas ou mal compreendidas com o passar dos anos, mas desenvolvidas por outros estudos etnográficos e entrevistas realizadas posteriormente. As questões de Pitman (2007) sobre o levante zapatista parecem estar conectadas com dois desdobramentos das publicações de David Ronfeldt e Harry Cleaver (1998). Primeiro, com o fato de a opinião pública ter confundido, desde o início, os conceitos de *cyberwar* e *social netwar*, generalizando-os para "guerra conduzida pela Internet", de forma que o entendimento foi de que o conflito aconteceu na rede e os próprios zapatistas foram responsáveis pelo ativismo na Internet. Segundo, com o fato de que esses autores – junto de Manuel Castells – foram responsáveis pela consolidação de imaginários sobre o levante zapatista, principalmente em relação às ideias de que os zapatistas foram o primeiro movimento de guerrilha informacional e de que o *electronic fabric of struggle* foi o fator definidor do levante e o motivo do movimento ter ganhado apoio internacional e avançado em sua causa. Especificamente, Pitman (2007, p. 90) desenvolve as seguintes questões, retomando vários elementos de Ronfeldt & Martínez (1997):

1) Os zapatistas não começaram a "guerra da Internet", ainda que tenham a capitalizado posteriormente: o denominado *electronic fabric of struggle* foi organizado por simpatizantes do levante e não pelos próprios zapatistas. Nesse sentido, os aspectos eletrônicos do conflito são consequência de o levante ter conseguido apoio de indivíduos e organizações adeptos às tecnologias da informação. Ainda assim, a Internet foi ferramenta importante para a promoção da causa zapatista;
2) Existiam outras razões além da presença na Internet que explicam a enorme popularidade dos zapatistas, principalmente em nível internacional: a utilização de tecnologias da informação não se configurou como fonte da popularidade dos zapatistas, mas algo secundário. A razão para a popularidade teria sido as escolhas de local, data e agenda. Nesse sentido, Pitman (2007) aponta que o município de San Cristóbal de las Casas, um dos ocupados pelo EZLN, era um destino turístico para aqueles interessados em cultura indígena e de fácil acesso aos jornalistas. Além

[44] O capítulo escrito por Ronfeldt & Martínez (1998) é parte do livro "*In Athena's Camp: Preparing for Conflict in the Information Age*" editado por David Ronfeld e John Arquilla. O primeiro autor, em particular, escreveu uma série de livros e artigos sobre *cyberwars* e outras questões do ciberespaço que são citados por outros autores.

disso, o levante aconteceu no mesmo dia em que seriam implementadas novas regras comerciais devido à entrada do México no NAFTA, de forma que suas demandas estavam conectadas com as correntes internacionais anti-neoliberais e antiglobalização e com os movimentos de direitos humanos e indígenas;

3) A luta dos zapatistas não foi apenas online: o uso de tecnologias da informação não excluiu outras formas de comunicação e ação coletiva: também foram utilizadas mídias impressas, palestras, rádios e o turismo para as Chiapas;
4) Em termos de inovação, a "guerra da Internet" foi, pelo menos no início, mais sobre a disseminação tradicional de informação/desinformação e sobre redes eletrônicas de colaboração e menos sobre formas específicas de ativismo na Internet: Pitman (2007) afirma que Cleaver (1998) foi um dos principais responsáveis em tecer o *electronic fabric of struggle*, uma vez que veio dele a percepção de que o uso de tecnologias da informação pelos zapatista foi algo inovativo em meio aos movimentos sociais. Os zapatistas e seus simpatizantes teriam apenas passado velhas formas de ativismo para um novo meio, a Internet, através do compartilhamento de textos e imagens. O aspecto inovativo teria vindo posteriormente com a exploração crescente da Internet como meio para mobilização, organização horizontal e ação conjunta em nível internacional que se tornaram características do ativismo na Internet. Este seria, para Pitman (2007), uma das principais contribuições da América Latina para a cibercultura, e;
5) Outros grupos ativistas latino-americanos, inclusive de luta armada, já haviam criado precedentes do ativismo na Internet: as primeiras configurações de redes ativistas na América Latina pré-datam os zapatistas[45].

Pitman (2007) corrobora Ronfeldt & Martínez (1998) sobre a existência de redes de ativistas, ONGs e organizações comunitárias na região das Chiapas anteriores ao conflito. O que torna a quinta questão levantada por Pitman (2007) interessante é a recuperação de outros movimentos populares na América Latina que também fizeram uso das redes, mas que

[45] Além da APC, também mencionada por Ronfeldt & Martínez (1997), Pitman (2007) se refere constantemente à Laneta, rede alternativa de computadores para comunicação do México anterior aos zapatistas que teria dado suporte às necessidades de formação de redes eletrônicas durante o levante.

não tiveram tanto impacto no imaginário dos ciberativistas: os maias hackers e a circulação massiva de informações por redes alternativas de comunicação conectadas com outras internacionais quando ocorreu o assassinato do seringueiro e ativista político brasileiro Chico Mendes em 1991.

Ainda que as análises realizadas sobre o levante zapatista sejam diferentes, Ronfeldt & Martínez (1997), Cleaver (1998) e Pitman (2007) concordam sobre a influência do que ficou conhecido por zapatismo digital para outros movimentos de povos tradicionais e para o ciberativismo como um todo[46]. Particularmente, Pitman (2007) cita a insurreição de Oaxaca, objeto do artigo de Tommaso Gravante "*Ciberactivismo y apropiación social. Un estudio de caso: la insurgencia popular de Oaxaca*" (2012), também parte do conjunto de publicações selecionadas.

> "*El 14 de junio de 2006 hay el estadillo de la insurrección popular. Bajo los ordenes del Gobernador Ulises Ruiz, que quiere acabar con toda forma de disenso en Oaxaca, la policía desalojó de violentamente una acampada del sindicado de maestros (SNTE) de en la plaza principal de la ciudad. Las protestas de la ciudadanía en contra de la política autoritaria del gobernador cobró en pocos días la dimensión de una amplia y profunda insurrección popular, con un alto sentido antiautoritario."* (GRAVANTE, 2012, p. 54)

O que se seguiu, de acordo com Gravante (2012), foi a ocupação de cidades pela população, que se organizou para a construção de barricadas de defesa e espaços de discussão e comunicação. Em termos gerais, a insurreição de Oaxaca apresentou muitas semelhanças com o levante zapatista: o envolvimento de ONGs e ativistas internacionais em atos de desobediência civil eletrônica, a utilização de meios alternativos para comunicação e organização, a violência desmedida do Estado mexicano, assim como censura e isolamento da mídia tradicional.

Os meios de comunicação alternativos foram essenciais para o movimento: cidadãos comuns apropriaram e usaram tecnologia da informação, tomando para si emissoras de rádios e televisão, para organização e construção de uma identidade do movimento popular que se constituía. Esses meios de comunicação, para Gravante (2012), tornaram-se a voz do movimento. Ao contrário do levante zapatista, a análise de Gravante (2012) parece evidenciar

[46] Sobre a influência do zapatismo para o ciberativismo, Sancho (2018, p. 358) escreve que "O espaço comum que emergiu da defesa global do levante zapatista permitiu que se pensasse de outra forma e que se atraíssem novas potências: foi o primeiro germe do movimento antiglobalização, sob o lema 'Outro mundo é possível' e que eclodiu em 30 de novembro de 1999, em Seattle, contra a reunião da Organização Mundial do Comércio. Essa mobilização massiva se tornou um 'evento midiático global' que deu origem ao 'movimento altermundista', 'antiglobalização' ou 'movimento pela justiça global' que se especializou em bloquear massivamente as reuniões de instituições econômicas internacionais, em organizar contracimeiras, jornadas de luta descentralizadas contra o capital e os Fóruns Sociais Mundiais".

que o movimento popular de Oaxaca já nasce conectado às tecnologias da informação como parte de um modo de vida alternativo e democrático e seus desdobramentos mostram que o movimento se preocupava também com a governança dessas tecnologias.

Nessa perspectiva, as entrevistas realizadas por Tommaso Gravante com membros do movimento popular de Oaxaca mostraram que a criação de meios alternativos de comunicação e informação decorreu da indignação com o tratamento dado pelo Estado e a imprensa tradicional à insurreição. Portanto, a apropriação das tecnologias da informação partiu do próprio movimento. Duas principais dificuldades foram encontradas: falta de conhecimentos técnicos sobre sites, redes, Internet e rádios e falta de recursos financeiros para a manutenção de domínios e servidores.

> *"Analizando la dimensión técnica, se observa que la falta de conocimientos técnicos es del todo influyente en la apropiación y uso del medio. Los diferentes problemas surgidos en este ámbito a lo largo de la experiencia mediática (tanto digital como analógica) se resolvieron compartiendo el conocimiento con personas externas pero afnes al proyecto. Asimismo en las experiencias de ciberactivismo se manifesta una relación entre la falta de recursos y de conocimiento y el software libre y su flosofía. La relación entre software libre y práctica de mediactivismo no se limita solamente al uso de aplicaciones no propietarias, sino que implica considerar el conocimiento y la comunicación como un bien común y, por ello, sujeto a ser compartido sin restricciones."* (GRAVANTE, 2012, p. 58)

Como o trecho sugere, a solução encontrada pelo movimento foi a adoção de *softwares* livres. O que surgiu como uma opção para as restrições financeiras foi ganhando força e espaço no movimento popular pelas práticas e filosofia de compartilhamento, que teria ajudado na construção do conhecimento técnico necessário para os objetivos do movimento. Um dos resultados da articulação deste movimento popular com o movimento do *software* livre foi a formação de uma comunidade hacker ativa em Oaxaca, interessada em participar em eventos e hacker *meetings* no México.

Controle, violência e o indivíduo

As publicações desta subcategoria, de forma geral, entendem o hacktivismo como uma forma de resistência política do indivíduo em relação ao contexto em que vive. Como apresenta Machado (2015):

> "Se o hacking sempre foi uma atividade carregada de traços políticos, também é possível afirmar que o hacktivismo dá um passo além. Enquanto as primeiras gerações de hackers estavam centradas nas políticas relacionadas a *softwares* e *hardwares*, os hacktivistas transpuseram mais claramente esse caráter político ao plano social, realizando ações diretas de desobediência civil. Assim, o ativismo

> hacker pode ser definido como o uso de ferramentas digitais tendo em vista fins exclusivamente políticos, que não raro são logrados de maneiras transgressivas e/ou disruptivas. De forma mais ampla, trata-se da junção das ferramentas e conhecimentos técnicos encontrados no hacking e de uma forma especial de ativismo político – realizado por meio das redes digitais." (MACHADO, 2015, p. 1533)

Machado (2015) e Mota & Figueiredo Filho (2015)[47] recuperam como uma das origens do hacktivismo o levante zapatista – e sua denominação de primeiro movimento de guerrilha internacional da história – e partem para discutir a ação política da expressão brasileira e hacktivista dos Anonymous. Aqui, o contexto em resposta ao qual surge a resistência é a sociedade de controle.

> "À medida que as sociedades contemporâneas constroem e adotam tecnologias digitais de comunicação, despontam formas de comando cada vez mais precisas e sofisticadas que, por meio da vigilância e das biopolíticas de modulação, exercem um controle jamais visto. Contudo, as mesmas tecnologias que controlam também são capazes de oferecer oportunidades de resistência." (MACHADO, 2015, p. 1534)

As formas com que se dão o controle – que é disperso, distribuído e pervasivo assim como as tecnologias da informação – seriam a implementação de programas de cibervigilância através dos rastros de navegação e o bloqueio do acesso a conteúdo, que engloba desde segredos de Estado até código-fonte de *softwares* e protocolos necessários para navegar em redes. Nesse contexto, hackers se tornam atores políticos importantes devido seu conhecimento avançado de linguagem computacional e tecnologias da informação (MOTA & FIGUEIREDO FILHO, 2015).

> "Nesse cenário, o ativismo hacker desponta como uma resposta à sociedade de controle. Dia após dia, hacktivistas se unem para, entre inúmeras outras ações: furar bloqueios indesejáveis; libertar informações de interesse público; promover a proteção da privacidade dos internautas; criptografar comunicações; desenvolver *softwares* inclusivos, cujo uso independa de empresas; e, mais especificamente no caso dos Anonymous, empreender ações digitais diretas em protesto a atos de governos e/ou corporações. Desde que se tornou um movimento de ações de massa, os Anons – como muitos Anonymous se chamam entre si – fizeram investidas contra o controle cibernético, hipertrofiando-o." (MACHADO, 2015, p. 1536)

Machado (2015) argumenta que a ação política dos Anonymous Brasil se configura como resistência por seu caráter heterogêneo, difuso e distribuído. A promoção do anonimato garante que exista um compartilhamento de identidade coletiva que conquista

[47] Machado (2015) e Mota & Figueiredo Filho (2015) usam literatura semelhante sobre o tema dos Anonymous. Mota & Figueiredo Filho (2015), em particular, citam como fonte a dissertação de mestrado de Murilo Machado, que deu base ao artigo de 2015.

colaboradores de diferentes origens e garante que os ativistas tenham sua identidade preservada para escapar das ferramentas de controle presentes na rede. Tanto Machado (2015) quanto Mota & Figueiredo Filho (2015) qualificam o anonimato como estratégia característica dos Anonymous na resistência ao contexto de controle e vigilância.

O anonimato conversaria diretamente com um dos preceitos da ética hacker observado por Levy (1984, p. 31): "*hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position*" e se oporia ao caráter identitário dos novos movimentos sociais (MACHADO, 2015). Ainda assim, de acordo com Machado (2015), as individualidades não seriam suprimidas, uma vez que também fazem parte dos Anonymous comunidades isoladas que mostram preferência por um tipo ou outro de tática de protesto[48]. A multiplicidade e dispersão também funcionam como um mecanismo de proteção, uma vez que torna difícil identificar e extinguir as todas atividades do coletivo. Machado (2015) avalia que essas características conformam novas formas de ação política que ainda fogem do controle de Estados e corporações.

A partir da contextualização, Machado (2015) entra nos pormenores da ação política dos Anonymous no Brasil[49], cujas operações deflagradas são descritas como espontâneas e iniciadas por indivíduos independentes. O único pré-requisito para as operações seriam a adesão de outros membros, sendo as redes formadas durante as operações rapidamente desfeitas. Assim como as experiencias internacionais, a organização do coletivo acontece por canais de IRC e existem diversos subgrupos, reflexo do caráter descentralizado do movimento. Uma das consequências da descentralização e falta de liderança características do Anonymous são as dissidências internas: não há unanimidade sobre a realização de operações. Machado (2015) discute dois exemplos interessantes: a #OpWeeksPayment, em que uma vertente específica do Anonymous Brasil comandou ataques de DDoS aos sites de bancos na semana do pagamento, e a #OpGlobo, em que outras vertentes atacaram sites da Fundação Roberto Marinho. No primeiro caso, a operação foi criticada por outras vertentes dos Anonymous antes mesmo de ser realizada porque prejudicaria apenas cidadãos comuns e os poria contra o Anonymous ao invés de gerar adesões e atingir governos e corporações, como esperado. A resposta da vertente responsável pela operação foi que os cidadãos se uniriam à causa por amor ou pela dor. No segundo, a dissidência girou em torno da regra

[48] O Anonymous se configura como uma identidade coletiva. Machado (2015), ao falar sobre a preservação das individualidades, parece se referir às preferências pessoais em relação às táticas hackers e às demandas/valores específicos dos indivíduos e comunidades que se identificam como Anonymous.

[49] De acordo com Machado (2015), as primeiras atividades dos Anonymous no Brasil começam com a *Operation: Payback* em resposta ao boicote da Mastercard, Amazon e PayPal ao Wikileaks em 2010. A faceta brasileira do coletivo participou esclarecendo dúvidas e recebendo novos participantes.

tácita entre os Anonymous em nível internacional de não atacar meios de comunicação em prol da liberdade de informação. Foram atacadas, então, apenas as páginas comerciais, mas também sem unanimidade e cercada de críticas.

De acordo com Mota & Figueiredo Filho (2015), a maior mobilização dos Anonymous no Brasil teria acontecido nas jornadas de junho de 2013, em que o coletivo ajudou na convocação de pessoas às ruas e foram relevantes na disseminação de informações sobre os protestos, que começaram com demandas contra o aumento das tarifas das passagens de ônibus. Após as ondas de protestos, 178 coletivos reivindicaram ser Anonymous no Brasil. Mota & Figueiredo (2015) apresentam uma última operação, a #OpHackingCup, em que foram tirados do ar diversos sites do governo, assim como de empresas patrocinadoras da Copa de 2014 no Brasil em protesto às violações de direitos básicos (como deslocamento de pessoas, barreiras financeiras à participação das festividades) e gastos exorbitantes em segurança para conter manifestações contrárias à realização da Copa.

Ainda em termos de resistência, uma das questões mais interessantes – comum às publicações enquadradas nesta subcategoria – foi a reflexão de que a sociedade de controle no caso latino-americano remete a memórias de um contexto específico – o passado colonial, os regimes ditatoriais violentos, as reformas neoliberais de privatização, desregulação e abertura favorecidas pelas tecnologias da informação e a modernização excludente. Um caminho para a discussão da história latino-americana encontrado por alguns dos autores foi trazer a análise do livro cyberpunk *El Delírio de Turing*, de Edmundo Paz Soldán (2003), que:

> "*follows several threads that converge on the life of one Miguel Saenz, a cryptographer who began his job under a dictatorial government and continues under the democratic version of that same government. Paz Soldán alludes here to the Bolivian governments of Hugo Banzer, the democratically elected former dictator, using the character of Montenegro, a bloody dictator who enjoys similar democratic success and who appears in many of Paz Soldán's novels. Saenz's job was to decode messages intercepted by the Camara Negra, an NSA-like organization charged with the surveillance of possible domestic threats. Under the dictatorship these threats were embodied by the so-called communist subversives; under the democratic govern ment the threat appears as a group of anti globalist hackers called the 'Resistencia'. The novel begins when Saenz receives an encrypted email that, when decrypted, reads 'ASESINO TIENES LAS MANOS MANCHADAS DE SANGRE', a message that leaves the man thoroughly nonplussed as he has never considered himself a part of the abuses of the dictatorship*." (BROWN, 2006, p. 116)

O livro de Paz Soldán é um exemplo da literatura cyberpunk latino-americana. Enquanto este subgênero da ficção científica é considerado apolítico e despolitizado no contexto de produção literária estadunidense (REDONDO, 2005), na América Latina as obras

cyberpunks mostraram-se politizadas por construírem utopias críticas, que Jorza (2012, p. 49) define como visões e práticas políticas compartilhadas por uma variedade de movimentos autônomos de oposição que rejeitam a dominação do sistema de corporações transnacionais e as estruturas produtivas ideológicas pós-industriais. Pela perspectiva de Jorza (2012), no contexto latino-americano, a Internet e outras redes se tornam espaços de resistência porque dão voz aos excluídos dos frutos da modernização sem a necessidade de passar pelo sistema político convencional. Aqui verifica-se outra característica comum às análises: a sensação de que os jovens sistemas democráticos latino-americanos são extremamente frágeis e que as ditaduras são latentes. Nesse sentido, "*el totalitarismo parece incluso inherente a la democracia contemporánea, porque las nuevas tecnologías refuerzan tanto las tentaciones, como también las posibilidades reales de control de los Estados y de sus servicios secretos*" (VON WERDER, 2016, pp. 57-58).

Quando Jorza (2012, p. 53) escreve que "e*l 'ciberhacktivismo' al cual se alude tantas veces en la novela de Paz Soldán se puede vincular, desde luego, con un amplio fenómeno contextual de oposición político-económica de los países del Tercer Mundo desde el espacio alternativo de la red*", refere-se especialmente às experiências do levante zapatista. Esses movimentos de resistência escancararam não só as consequências das reformas neoliberais – subordinação dos Estados às instituições financeiras internacionais, desemprego, pobreza, deslocamentos populacionais – mas também criticaram a forma com que ocorreram, apressadas e mal negociadas, por sentirem que os custos da globalização recaíram apenas sobre os países de terceiro mundo (OVIEDO, 2003).

Em se tratando de reflexões sobre o contexto, como apontado anteriormente, o surgimento das CryptoRaves está diretamente conectado à intensificação da vigilância massiva e do uso de tecnologias complexas pelos Estados e corporações. Os atos de denúncia de Snowden, como aponta Coleman (2017), tornaram-se um chamado para hackers e outros entusiastas da tecnologia se engajarem na agenda política da privacidade através do esforço conjunto em desenvolver ferramentas de criptografia. A criptografia e outras ferramentas de proteção à privacidade e segurança na Internet, assim como os *softwares* livres e as infraestruturas de rede, conformam a materialidade comum da prática e do interesse dos grupos presentes na CryptoRave. Nesse sentido, é principalmente nesta subcategoria das políticas hackers em que a maioria das discussões das quais participei nas edições da CryptoRave se enquadram. Nelas, foi possível identificar um consenso sobre a existência de

uma disparidade de poder entre os indivíduos e o Estado/grandes corporações[50] em se tratando da privacidade específica do contexto de vigilância em massa. Essa contextualização apareceu explícita ou implicitamente como justificativa em todas as atividades para se pensar privacidade e tentar reduzir a disparidade de poder, seja reconhecendo a situação (discussões), protegendo suas informações (criptografia, *software* livre e outras ferramentas) ou contra-atacando (hacking e vazamentos). No caso das discussões assistidas na CryptoRave, a contextualização se aproximou mais do conceito de capitalismo de vigilância, que Shoshana Zuboff (2015) define como uma nova forma do capitalismo informacional que intenta predizer e modificar o comportamento humano como forma de gerar receita e controle de mercado através da comoditização e monetização de dados de indivíduos. A coleta, comercialização e utilização de dados fazem parte de uma nova lógica de acumulação capitalista e a criptografia, assim como outras ferramentas de segurança da informação, transformam-se em resistência ao capitalismo de vigilância[51].

> *"Many of the practices associated with capitalizing on these newly perceived opportunities challenged social norms associated with privacy and are contested as violations of rights and laws. In result, Google and other actors learned to obscure their operations, choosing to invade undefended individual and social territory until opposition is encountered, at which point they can use their substantial resources to defend at low cost what had already been taken. In this way, surveillance assets are accumulated and attract significant surveillance capital while producing their own surprising new politics and social relations."* (ZUBOFF, 2015, p. 85)

Enquanto as relações entre indivíduos e contexto tratadas pelas mesas da CryptoRave e pelas publicações enquadradas nesta subcategoria apresentam semelhanças (vigilância, controle e violência), na CryptoRave foi possível identificar um sentimento de urgência, muito provavelmente por este ser um espaço para conscientização e denúncia que não passa pelos processos morosos da publicação acadêmica e é voltado para todos os públicos. Este sentimento foi transmitido de diferentes formas – desde a retomada constante sobre os perigos diários à privacidade e à liberdade dos indivíduos até a apresentação de casos em que populações vulneráveis e movimentos sociais sofreram com violências e abusos.

---

[50] No contexto da CryptoRave, "grandes corporações" muitas vezes é sinônimo das grandes quatro companhias de tecnologia – Facebook, Google, Amazon e Apple. Essas companhias, além de dominar grande parte do mercado de produtos e serviços de tecnologia da informação – inclusive de infraestrutura de rede – também se deparam com pouca ou nenhuma regulação, principalmente em relação às formas de coleta e comercialização de dados de usuários. Shoshana Zuboff, em "*Big other: surveillance capitalismo and the prospects of na information civilization*" (2015) discute, entre outras questões, a lógica de acumulação dessas grandes corporações.

[51] Zuboff (2015, p. 85) também apresenta sua definição de hacking no capitalismo de vigilância: "*Hacking intends to liberate affordances from the institutional logics in which they are frozen and redistribute them in alternativa configurations for new purposes*".

Um exemplo de como a relação entre contexto e criptografia é compreendida na CryptoRave foi a discussão realizada na mesa "Criptografia e agroecologia" (trilha política, 2017), onde foi reforçado que a criptografia surgiu como resistência à centralização e subordinação das relações à lógica do mercado capitalista em um momento em que a conectividade entre as pessoas é mediada por multinacionais de tecnologias da informação e comunicação, que armazenam e vendem os dados pessoais como fonte de receita. Nesse sentido, quando a circulação de informação sobre pessoas, protestos, ativismos e outras lutas é cerceada e fica centralizada e sob controle de empresas capitalistas e governos conservadores, a população se torna cada vez mais vulnerável, o que justifica o desenvolvimento e uso de tecnologias de criptografia. Palavras semelhantes para o contexto foram utilizadas por integrantes de outras mesas: vigilância em massa e mercantilização dos dados e da conectividade ("(Ciber)espaços seguros: redes autônomas feministas", trilha gênero, 2017); capitalismo de vigilância, economia de plataforma ("A economia psíquica dos algoritmos", trilha política, 2018).

Dois exemplos apresentados foram interessantes em relação a como os mecanismos de controle se expressam. O primeiro é próximo das análises de Oviedo (2003), Jorza (2012) e von Werder (2016) sobre o caráter totalitário das democracias latino-americanas, que irrompem em repressão e violência contra a dissidência. Em "*Whatsapp y comunidades vulnerables*", um representante da organização latino-americana independente e sem fins lucrativos *Derechos Digitales,* que busca desenvolver, defender e promover os direitos humanos no meio digital, narrou os fatos que levaram a sua criação: a Operación Huracán, em 2017, em que oito líderes mapuches foram presos pela polícia chilena sob pretexto de envolvimento de terrorismo captado em mensagens interceptadas de WhatsApp. Os líderes mapuches foram liberados em 2018 devido a contradições técnicas das evidências apresentadas, que eram compostas por arquivos de texto em .txt, datas e localizações que não corroboraram as ações e planos denunciados. De acordo com a investigação, foi utilizado um *software* proprietário forense (de recuperação e interpretação de dados) na obtenção das conversas entre os líderes mapuches, mas, em 2016 o WhatsApp já havia incorporado o Protocolo Signal de criptografia ponta-a-ponta em mensagens, o que dificultaria a obtenção de mensagens por terceiros. Depois de investigação do Ministério Público chileno, chegou-se à conclusão de que a polícia chilena havia criado as provas para incriminar os líderes mapuches.

O segundo exemplo, mais próximo do contexto apresentado por Machado (2015), foi discutido na mesa "Cidadão Quem? Usos e Abusos da Biometria no Brasil", em que as palestrantes do grupo de Informação, Comunicação, Tecnologia e Sociedade (ICTS) da

Unicamp apresentaram diversas formas com que dados biométricos são coletados e utilizados no Brasil pelo governo e pelo setor privado. Os principais argumentos (e exemplos) foram o convênio de troca de base de dados biométricos entre o Tribunal Superior Eleitoral e a Polícia Federal, o decreto assinado em São Paulo que criou o Sistema Estadual de Coleta e Identificação Biométrica Eletrônica para armazenamento de impressões digitais e comercialização do acesso aos dados por empresas credenciadas e a obrigatoriedade de identificação das palmas de recém-nascidos brasileiros e da biometria das mães. O alerta, e a discussão subsequente, foi sobre como esses órgãos e instituições se aproveitam de lacunas legislativas e utilizam dos argumentos da necessidade de garantir segurança e ordem para coletar e comercializar dados biométricos dos cidadãos sem conhecimento ou consentimento, isso quando estes dados não são utilizados como forma de controle de acesso e vigilância urbana. A participação e ocupação de muitos espaços públicos e privados já estão dependentes de identificação biométrica, o que potencializa a exclusão de grupos populacionais.

Dentro desta subcategoria de resistências, tanto as publicações selecionadas quanto as discussões da CryptoRave tratam de contradições e dualidades das tecnologias da informação quando o que está em disputa é a privacidade e a segurança dos indivíduos. As publicações, em particular, partem da ideia que as mesmas tecnologias utilizadas como ferramenta de controle, vigilância, repressão e levam a cabo as políticas neoliberais também oferecem caminhos para a resistência e são nesses caminhos que hackers se tornam importantes atores políticos. Portanto, mecanismos novos e mais intensos de repressão são encontrados com novas formas de subversão. As discussões na CryptoRave foram além e se mostraram preocupadas com questões de adoção e não-adoção de tecnologias de criptografia e segurança de informação, de forma que, dependendo da mesa, as especificidades técnicas das tecnologias também entravam em jogo.

Foi bastante comum sair de uma mesa, entrar em outra e ouvir posicionamentos completamente opostos sobre uma mesma tecnologia. Um dos principais exemplos é o próprio Protocolo Signal, considerado uma ferramenta de criptografia ponta-a-ponta para mensagem para escrita, voz e vídeo bastante segura. Os posicionamentos sobre o protocolo mudavam bastante dependendo do foco da mesa. Quando a discussão era mais ampla sobre proteção individual e das mensagens, com teor de divulgação da criptografia e conscientização de como cuidar da segurança individual, o uso Protocolo Signal era mandatório. Porém, nas mesas mais envolvidas com movimentos sociais, como "*Whatsapp y comunidades vulnerables*", o uso era recomendado com cautela porque, pelo menos até 2018,

os servidores para retransmissão de mensagens pertenciam a duas grandes corporações conhecidas por vender/disponibilizar dados. Mesmo a criptografia, como ferramenta, foi colocada em xeque repetidas vezes em debates relacionados a criptomoedas e anonimato, principalmente em relação aos usos imprevistos para mediação de tráfico humano, terrorismo e outras atividades criminosas ("Criptografia, privacidade e política", trilha política, 2018).

Quando Maxigas (2017) trata de escolhas de adoção ou não-adoção de tecnologias por hackers, argumenta que as preferências tecnológicas dependem de questões éticas e estéticas – relacionadas ao desenho, ao processo de desenvolvimento e outros aspectos relacionados à tecnologia que remetem a memórias de uma história compartilhada entre os hackers, assim como ao seu *ethos*. Essas escolhas seriam políticas porque a adoção ou rejeição de uma tecnologia por usuários sofisticados poderia levar à exploração de caminhos alternativos do desenvolvimento tecnológico que, por sua vez, conformam as realidades tecnopolíticas. Nas disputas e contradições em torno da adoção ou não-adoção de tecnologias na CryptoRave, ainda que também realizadas por usuários especialistas, as decisões parecem se configurar como reações às medidas governamentais, violências e intrusões que afligem os indivíduos, comunidades e movimentos sociais. Apesar do imediatismo das escolhas tecnológicas e das políticas que emergem delas, também estão em disputa alternativas tecnopolíticas menos ligadas à ideia de desenvolvimento e progresso tecnológico como em Maxigas (2017) e mais às formas de proteção e viver dos indivíduos, comunidades e movimentos sociais. Essas questões também aparecem nas políticas do dia-a-dia em intersecções com gênero, como é tratado no próximo item.

4.2 As políticas do dia-a-dia: trabalho, comunidades e gênero

Uma outra categoria de política hacker verificada na América Latina é aquela que emerge de práticas e dinâmicas das atividades cotidianas, particularmente, dos fatores e características que os tornam hackers e garantem sua existência como tal. Como apontado anteriormente, foi possível identificar três subdivisões: as políticas internas das comunidades de *software* livre, outros modos de vida e questões de gênero.

Comunidades e o movimento de software livre

De forma geral, nas publicações desta subcategoria as políticas as análises se focaram nas práticas e atividades cotidianas, assim como nas regras internas, em sua maioria

tácitas, e nas relações que se configuram tanto nas comunidades de *software* livre e código aberto quanto no movimento como um todo. Nesse sentido, as políticas emergem das práticas, atividades e regras, que estão em constante disputa e negociação nesses espaços. Estes, ora denominados comunidades de conhecimento (SOLÓRZANO, 2009) ora espaços comunitários (ZANOTTI, 2014), conformam-se tanto na rede, como em listas de e-mail e fóruns online de desenvolvedores, quanto offline, como em fóruns de *software* livre, conferências, festivais de instalação etc.

> "*Desde grupos de usuarios hasta organizaciones más complejas, estos se autodefinen en general como comunidades. Estas siguen en general una base horizontal de asociación y sirven para intercambiar recursos, trabajar en proyectos colectivos y promover el uso y la extensión del modelo libre. Allí se crean además vínculos, significados y experiencias compartidas. Las personas que conforman los espacios comunitarios lo hacen por una amplitud de motivaciones. Los mismos son valorados en términos de colaboración, solidaridad, apoyo mutuo, producción entre pares, socialización, acceso a recursos y redes, posibilidades de concretar iniciativas y la existencia de una cultura compartida."* (ZANOTTI, 2014, p. 58)

Ainda que os autores tratem de espaços diferentes – comunidades online da Costa Rica (SOLÓRZANO, 2009), comunidades da Argentina que se tornaram movimento (ZANOTTI, 2014) e movimento de *software* livre no Brasil (EVANGELISTA, 2014) – existem elementos em comum entre eles: i) grande parte da população é formada por indivíduos do sexo masculino que trabalham parcialmente ou completamente com desenvolvimento e gestão de *software*, e; ii) uma das fontes de conflito são as divisões internas, criadas explícita ou implicitamente a partir das relações entre os indivíduos-código/*software* livre e, portanto, o papel que têm dentro da comunidade/movimento.

Quando Solórzano (2009) analisa as comunidades online de *software* livre da Costa Rica, particularmente relacionadas com o sistema operacional GNU/Linux, conclui que são efêmeras e descontínuas. Os membros das comunidades relacionaram esse problema ao fato de só alguns deles participarem ativamente das comunidades, enquanto os outros são apáticos ou espectadores. Solórzano (2009) assinala, porém, que a baixa participação estaria relacionada com uma das lógicas das comunidades de *software* livre já mencionadas anteriormente em Levy (1984) e, principalmente, Raymond (1996, revisão 1.51 out. 2017), a tecnomeritocracia:

> *"La mayoría de las comunidades de software libre se caracterizan por la tecnomeritocracia, es decir, los usuarios son valorados por sus conocimientos y capacidad para resolver problemas. Por ello se espera que los usuarios traten de resolver los problemas por sí mismos, leyendo la documentación disponible*

> *primero, y luego formulando preguntas concretas y documentadas. Lo anterior ahuyenta a muchos novatos que formulan preguntas consideradas 'obvias'. De ahí que sea difícil que puedan participar fácilmente si esperan que la comunidad haga todo el trabajo por ellos.*" (SOLÓRZANO, 2009, p. 149)

Na prática, novos membros acabavam sendo expulsos ou simplesmente deixavam as comunidades e nunca mais voltavam. Para alguns membros já estabelecidos, essa atitude discriminatória e elitista era um dos motivos da morte lenta das comunidades, porém:

> *"para la mayoría de membros de GULCR* [uma das maiores comunidades]*, el ser considerados elitistas o excluyentes, lejos de ser un defecto, es una virtud, propia de la ética hacker y de las comunidades de software libre, especialmente aquellas en las que participan expertos programadores encargados del desarrollo de Linux."* (SOLÓRZANO, 2009, p. 150)

Portanto, ainda que essas comunidades fossem formadas a partir da busca desses indivíduos por valores comunitários como solidariedade, cooperativismo e trabalho coletivo, além de compartilhamento de conhecimentos técnicos sobre o GNU/Linux, a tecnomeritocracia, o elitismo, as regras restritas de interação as tornavam bastante fechadas e colocavam em discussão o conceito de abertura e horizontalidade, como apontado anteriormente por Toupin (2014).

Preocupado com as motivações que levam os membros de comunidades de *software* livre argentinas a se engajarem em projetos e outras atividades, Zanotti (2014) retoma uma série de valores e atitudes também identificadas em Levy (1984) e Raymond (1996, revisão 1.51 out. 2017): atendimento de buscas pessoais e necessidades cotidianas na solidariedade da comunidade (sentimento de pertencimento, suporte técnico, reputação etc.), acesso a recursos, compartilhamento de *softwares*, códigos e experiências, consequências da lógica de abertura, e a possibilidade de enriquecer a qualidade de seus trabalho a partir das trocas de conhecimento realizadas dentro da comunidade. A tecnomeritocracia também faz parte dessas comunidades: as capacidades e destrezas técnicas garantem autoridade e reputação dentro delas, uma vez que, em consonância a Raymond (1996, revisão 1.51 out. 2017), hackers respeitam bons hackers (ZANOTTI, 2014, p. 66). Ao contrário do observado por Solórzano (2009), porém, Zanotti (2014) evidencia que as comunidades argentinas estudadas são mais cuidadosas em relação à sua lógica de reprodução, estando mais abertas à inclusão de novos participantes e à socialização de conhecimentos técnicos.

Uma das questões mais interessantes trazidas por Zanotti (2014) foi o argumento de que, na Argentina, a ampliação dos espaços comunitários (comunidades e projetos) foram transformando o *software* livre em um movimento social em torno da disputa mais ampla

sobre relações entre tecnologias da informação, poder e controle sobre a informação e redes. Por trás da cooperação e reciprocidade estaria a racionalidade de que tecnologias da informação são centrais para as sociedades contemporâneas como um caminho para o fim das limitações tecnológicas dos indivíduos e nações (ZANOTTI, 2014).

Nesse sentido, a permanência de alguns membros nas comunidades esteve relacionada com o compromisso com as éticas e políticas vinculadas ao *software* livre e à conformação de uma agenda política interna. Esses membros são referidos por Zanotti (2014) como militantes. Ao contrário dos aderentes e participantes, que acompanham discussões nas listas de e-mail ou participam periodicamente de projetos, os militantes têm uma trajetória dentro das comunidades e são bastante ativos, liderando e garantindo recursos para os projetos, expondo seus posicionamentos sobre as políticas entorno do *software* livre e difundindo seus postulados.

> *"A partir de aquí, el software se construye como un objeto político y se incluye en un campo de disputas donde aparecen aliados y adversarios. La defensa y promoción del modelo libre conduce así a la interpelación de otros agentes sociales, favoreciendo por diferentes vías su difusión. De hecho las comunidades regionales parecen haber prestado una gran atención a los aspectos políticos del software libre."* (ZANOTTI, 2014, p. 67)

Neste ponto, a lógica das comunidades argentinas de *software* livre parece estar mais alinhada ao posicionamento de Richard Stallman que de Eric Raymond. A partir dos trechos das entrevistas destacados por Zanotti (2014), fica evidente que o posicionamento político não é algo exógeno às comunidades em questão e ao hackerismo nelas, mas intrínseco e parte do dia-a-dia, de forma que os relatos explicitam que falar de *software* livre é falar de política de patentes e da ideologia da livre circulação de informação ou apontam que a parte mais importante do *software* livre na América Latina sempre foi a política, de forma que o movimento político entorno do *software* livre seria maior que o técnico.

A militância pelo *software* livre não fica alheia a disputas. O fortalecimento do *software* livre como movimento nos anos 2000 e a incursão em políticas locais terai começado a gerar tensões principalmente relacionadas às políticas partidárias. Um dos exemplos seria a disputa entre os militantes que buscam se distanciar dos partidos políticos tradicionais, formando alianças estratégias quando necessário para o andamento de algum projeto, e aqueles que explicitamente associaram o *software* livre com o peronismo do passado:

> *"la vinculación entre el peronismo y el software libre comenzó a ser planteada a partir de blogs como Ubuntu peronista y Si Evita viviera sería linuxera [...] Aunque ambos blogs se planteaban en clave irónica y con un estilo jocoso, presentaban la conexión entre software libre y peronismo a partir de algunos temas como el impulso industrializador, la lucha contra sectores corporativos, la defensa de la soberanía nacional, la justicia social y la unidad del pueblo."* (ZANOTTI, 2014, pp. 69-70)

Um dos resultados da militância foi a formação de um coletivo que trabalhou para fortalecer o lugar do *software* livre nas políticas públicas, ajudando na formulação de projetos de lei e na difusão do *software* livre como forma de produzir conhecimento de forma soberana, independente e voltado para a sociedade fora do controle de grandes corporações.

A análise de Evangelista (2014) faz o movimento contrário ao de Zanotti (2014). Partindo das origens do movimento do *software* livre no Brasil, Evangelista (2014) discute as políticas identificadas durante edições do Fórum Internacional de *Software* Livre (FISL) que acontecem em Porto Alegre. O *software* livre como movimento no Brasil tem origens anteriores àquelas argentinas e progressivamente foi se tornando mais heterogêneo.

> "Desde meados da década de 1990, um grupo de pessoas vem atuando no Brasil no sentido de propor a adoção e contribuir para o uso do que se convencionou chamar de *softwares* livres. Esse grupo, nem sempre homogêneo em seus posicionamentos, intitula-se 'movimento *software* livre' e reúne técnicos, desenvolvedores, ativistas, usuários, organizações, empresas, empresários, artistas e intelectuais." (EVANGELISTA, 2014, p. 174).

O movimento de *software* livre no Brasil, segundo Evangelista (2014), é conhecido internacionalmente pelo tamanho dos eventos e pela influência junto aos governos municipais, estaduais e federal. O FISL, o principal desses eventos, acontece desde o ano 2000 e seus participantes são considerados a comunidade brasileira de *software* livre, de forma que as dinâmicas do evento se tornam representativas do movimento como um todo no contexto brasileiro.

Uma das grandes diferenças do movimento de *software* livre brasileiro em relação aos internacionais seria sua orientação política para a esquerda e a promoção pelo Estado das ideias do *software* livre, principalmente durante o governo Lula.

> "A ideia de cooperação, colaboração, solidariedade e construção de um conjunto de *softwares* que fosse uma alternativa para o enrijecimento das regras de propriedade intelectual ganhou outra força ao aportar em um país subdesenvolvido de industrialização parcial. Técnicos, muitos ligados ao serviço público, e com passado ligado aos movimentos de esquerda, entenderam o movimento *software* livre também como uma resposta ao domínio das grandes empresas de informática e ao saque de riquezas promovido pelos países desenvolvidos. No horizonte, enxergou-se o *software* livre até como fator de transformação e superação da economia

> capitalista. Foi assim que políticos de alguma forma identificados com a ideia de resistência à dominação e exploração externa incorporaram o *software* livre em seu repertório de propostas, somando-o a planos de independência nacional." (EVANGELISTA, 2014, p. 192)

O FISL, como exemplo desse movimento, tem sua origem entre funcionários públicos de tecnologia vinculados a sindicatos e movimentos de esquerda, ainda que tenha buscado seu apoio em estudantes e profissionais da computação vinculados a empresas privadas, atribuindo ao evento um caráter híbrido e heterogêneo pela necessidade de atender as demandas do público e conseguir recursos para sua realização. É dessa forma que conviveriam, no mesmo lugar, visões do *software* livre como meio de transformação social e como apenas um modelo econômico alternativo.

Ao tratar do movimento de *software* livre no Brasil, Evangelista (2014) mostra que apesar de ser possível identificar diferentes agendas, as discussões em fóruns virtuais e no FISL reproduzem a disputa entre os grupos do *software* livre e código aberto apresentadas no segundo capítulo. No evento, são notadas subdivisões entre o público: burocratas/ativistas e nerds/empresários, confundidos muitas vezes com pessoas com menos ou mais conhecimento técnico, respectivamente. Os primeiros, normalmente funcionários públicos ou formados em ciências humanas, estariam mais interessados em questões de inclusão digital e, de fato, têm pouco conhecimento técnico ou não estão envolvidos diretamente com desenvolvimento de *software*. Os últimos seriam estudantes de computação interessados em aprender sobre tecnologia e fazer contatos profissionais e os empresários que buscam recrutar profissionais e fazer contatos para prestação de serviço. Mesmo na organização do evento, segundo Evangelista (2014), é possível verificar uma classificação informal e hierárquica entre "hackers" e "políticos": os primeiros ocupam posição de prestígio, têm mais conhecimento técnico e postura pública austera, enquanto os segundos articulam apoio e convidados, além de serem os porta-vozes do FISL e sempre acusados por outros participantes de baixo envolvimento em desenvolver programas e de tentar se apropriar do *software* livre para causas políticas.

As divisões do público do FISL, especialmente empresários/nerds/hackers e burocratas/ativistas/políticos, na análise de Evangelista (2014), poderiam ser relacionadas com os grupos de código aberto e *software* livre, respectivamente, e marcaria a disputa de quem representa melhor o movimento de *software* livre no Brasil. Nos último anos, Evangelista (2014) aponta que o grupo do *software* livre foi progressivamente perdendo espaço para o grupo de código aberto, de forma que o FISL tem se tornado um lugar de

recrutamento de profissionais de tecnologias da informação onde a perspectiva da predominância da técnica e da competição sobre questões políticas e ativismos tem mais espaço .

Outros modos de vida

Esta subcategoria é conformada por publicações em que os autores trataram de formas diferentes de vivenciar o hackerismo. Essas formas são analisadas de uma perspectiva em que as atividades cotidianas as tornam únicas e permitem outros modos de vida, a partir dos quais emergem as políticas hackers, que são internas a essas formas. O ser hacker, aqui, é considerado intrínseco aos casos e não algo externo e apropriado. Três publicações trazem essas outras perspectivas e têm como objetos de estudo o trabalho hacker dentro do Projeto de Tradução do GNOME (GNU *Network Object Model Environment*) para o Português Brasileiro (FRANÇA FILHO & AGUIAR, 2014), as conferências hackers (COLEMAN, 2010)[52] e o tecnoxamanismo (BORGES, 2018). Os casos, assim como as características de cada um, são bastante específicos.

Ainda que o Projeto GNOME e as conferências hackers envolvam as atividades de um público semelhante (desenvolvedores de *software* e entusiastas de tecnologias da informação), as análises realizadas pelos autores trabalham com aspectos diferentes. Enquanto França Filho & Aguiar (2014) discutem o trabalho hacker em um projeto de longa duração sob a ótica da Teoria da Dádiva de Marcel Mauss, Coleman (2010) se interessa pelas inter-relações entre os hackers em um período curto, intenso e fora da rotina. Já Borges (2018) define e descreve o tecnoxamanismo como manifestação hacker devido às semelhanças fundamentais entre os movimentos. Um dos únicos elementos em comum entre as três publicações, além do fato das políticas emergentes sinalizarem outros modos de vida dentro do hackerismo, é a conexão com tecnologias livres, que são parte essencial dos casos apresentados.

Semelhante a Zanotti (2014), França Filho & Aguiar (2014) buscam compreender a natureza do engajamento dos hackers em processos de desenvolvimento e distribuição de *software* pela Internet. Analisando o caso do Projeto GNOME no Brasil, os autores apontam para as características do trabalho hacker como fator condicionante do engajamento. O

[52] Em seu artigo, Coleman (2010) analisa algumas edições da *Debian Conference* (Debconf). O Debian é um sistema operacional livre e, desde 2000, são realizadas conferências anuais dos seus desenvolvedores. Coleman (2010) discute particularidades e acontecimentos de algumas das edições do Debconf, inclusive a do ano de 2004 que aconteceu em Porto Alegre, no Brasil.

trabalho hacker, ao contrário do trabalho capitalista, seguiria outro conjunto de valores articulados com a reputação e o prazer em criar, posicionando-o à parte de instituições contratuais, vínculos institucionais e compensações financeiras.

> "Dentre esses valores, segundo Stallman (2002), Castells (2003) e Silveira (2005), a liberdade (de ter acesso, de usar, de contribuir e redistribuir todo o conhecimento possível) é o valor supremo dos hackers. Essa liberdade parece traduzir-se em um jogo de reputações e troca entre pares, quando a lógica social passa a ser determinada não pelo retorno monetário ou pela acumulação de bens, mas sim pela informação, conhecimento ou código (de programação) que é doado. Em outras palavras, a dinâmica empreendida no seio da cultura hacker estaria, assim, associada a uma regra de ouro fundada na tripla ação de dar, receber e retribuir que Apgaua (2004), Castells (2003), Kollock (1999), Raymond (1999) e Barbrook (1998) denominaram de prática da cultura do dom que induziria a manifestação de uma suposta economia da dádiva (*gift economy*)." (FRANÇA FILHO & AGUIAR, 2014).

França Filho & Aguiar (2014) expõem no início do artigo que a imersão no campo foi realizada já pressupondo as semelhanças entre trabalho hacker e dádiva. O comentário de Eric Raymond (1996, revisão 1.51 out. 2017) sobre a percepção dos antropólogos sobre o trabalho hacker parece ter sido um dos pontos de partida:

> *"Specifically, hackerdom is what anthropologists call a gift culture. You gain status and reputation in it not by dominating other people, nor by being beautiful, nor by having things other people want, but rather by giving things away. Specifically, by giving away your time, your creativity, and the results of your skill."* (RAYMOND, 1996, revisão 1.51 out. 2017).

Existe um objeto em comum – o desenvolvimento e distribuição de um *software* – e o trabalho tem caráter voluntário e não-contratual, normalmente realizado no tempo livre ou quando os hackers não estão engajados em seu trabalho formal. França Filho & Aguiar (2014, p. 127) querem evidenciar que, mesmo com essas características, o trabalho hacker pressupõe trocas, de forma que "o envolvimento social nesse trabalho coletivo (realizado junto com outros hackers) acaba proporcionando reconhecimento, prestígio, prazer, criatividade e, por conseguinte, poder (mérito) atribuído a cada importante contribuição técnica compartilhada". Por vezes generalizando, França Filho & Aguiar (2014) concluem que os hackers acabam configurando um outro modo possível de engajamento com o trabalho e característica das novas dinâmicas de vida e produção em uma sociedade em rede.

Ao reconhecer que hacking e desenvolvimento de *software* livre e código aberto acontecem em sua maioria por meio da Internet e que os estudos acadêmicos costumam se focar no trabalho e interações virtuais entre hackers, Coleman (2010) justifica que seu

interesse nas conferências hackers é mostrar que as interações virtuais não deslocam ou substituem as interações físicas. Em particular, essas interações acontecem nas conferências, a primeira delas tendo ocorrido em 1984 inspirada pelo livro de Levy (1984). O que faz das conferências uma outra forma de viver o hackerismo, de acordo com Coleman (2010), seria a reconfiguração entre tempo, espaço e pessoas. Todos os elementos já discutidos anteriormente sobre atividades relacionadas ao desenvolvimento e distribuição de *software* livre e hacking são identificadas pela autora: colaboração, compartilhamento, solução de problemas conjuntamente, brincadeiras, instalações, tecnologias livres.

> *"hacker conferences are rituals of confirmation, liberation, celebration, and especially re-enchantment where the quotidian affairs of life, work, labor, and social interactions are ritualized and thus experienced on fundamentally different terms. Through a celebratory condensation, hackers imbue their actions with new, revitalized, or ethically charged meanings. Lifting life 'out of its routine' (Bakhtin 1984:273) in its place, hackers erect a semi-structured but highly flexible environment, the kinetic energy being nothing short of irresistible and corporeal interactivity. These are profound moments of cultural re-enchantment whereby participants build and share a heightened experience of each other*." (COLEMAN, 2010, p. 53)

Nesse sentido, ainda que gerem exaustão física e mental depois de dias de congregação, trabalho, palestras, passeios e noites mal dormidas, as conferências são, para os hackers, formas de celebrar as práticas e sociabilidades do dia-a-dia e forma exarcebada e compartilhar com outros hackers espaços diferentes de trabalho e socialização.

O tecnoxamanismo apresentado por Borges (2018) traz ainda outra perspectiva, conectando as experiências dos hackers ao longo de sua história com aquelas do que chama de ontologias desperdiçadas.

> "Nessa transversalidade [das ontologias de comunidades sobreviventes que tiveram suas perspectivas de mundo devastadas por sistemas coloniais e industriais] surgem inúmeros grupos que veem sim na rede de computadores, na linguagem da programação, no uso de aparatos tecnológicos, formas de sobrevivência e expansão dos seus modos de vida. Esses índios, quilombolas, ciganos, beduínos, aborígenes, bárbaros contemporâneos podem com certeza serem hackers, e os sistemas que podem criar a partir disso sofrem toda a perseguição, anulação, silenciamento que os hackers ocidentalizados sofrem. O hackerismo a princípio pode ir para qualquer lado e servir a qualquer ideologia. Por isso é tão importante discutir a ética hacker e sua relação com essas ontologias desperdiçadas." (BORGES, 2018, p. 107)

Dentre as práticas e conhecimentos engajados pelo tecnoxamanismo estão tecnologias sobre plantas, sementes, água e cultivo, trocas de saberes e tecnologias livres, relação com comunidades tradicionais, apropriação, uso e desenvolvimento de *software* livre, código aberto, faça-você-mesmo e arte, tecnologias eletrônicas e subjetividade, entre outros.

Borges (2018) situa o reaparecimento da palavra tecnoxamanismo quando hackers, hacktivistas e desenvolvedores de *software* livre começaram a interagir com comunidades quilombolas, indígenas e ribeirinhas ou, como coloca Borges (2018, p. 106), "comunidades e modos de vida muito diferentes dos das capitais" no contexto da implementação dos Pontos de Cultura[53]. A ideia do tecnoxamanismo, como apresentada por Borges (2018), é justamente relacionar *software* livre com outros modos de vida, mais especificamente àqueles dos povos tradicionais, uma vez que da interação entre esse grupo heterogêneo de pessoas emergiu a percepção de que o movimento do *software* livre era mais que inclusão tecnológica (sob a perspectiva da política pública), mas de conexão entre culturas e saberes de tecnologias diversas.

A leitura sobre o tecnoxamanismo e a perspectiva apresentada por Borges (2018) remeteu às discussões realizadas por uma mulher integrante da Sempreviva Organização Feminista (SOF), organização não governamental que trabalha com a autodeterminação da mulher em movimentos de resistência contra hegemonia e com a articulação popular na construção de processos alternativos de desenvolvimento ("Criptografia e agroecologia: alternativas feministas em defesa dos comuns - nossas tecnologias, outras formas de vida. Como semear a resistência feminista?!", trilha política, 2017). De forma geral, o tema que perpassou todas as falas da mesa – também composta por mulheres integrantes da Marcha Mundial das Mulheres, movimento feminista internacional que busca construir e difundir perspectivas feministas através da afirmação do direito à autodeterminação e igualdade – foi a de resistências femininas ao sistema capitalista e ferramentas de defesa das mulheres contra sua lógica de dominação, partindo de comparações entre criptografia e a agroecologia (em especial o caso das mulheres agricultoras do Vale da Ribeira), entendidas como alternativas para solidariedade entre indivíduos e defesa contra contra a vigilância e o agronegócio/mineração, respectivamente, através de um modo de vida coletivo. Segundo as integrantes da mesa, a agroecologia e suas práticas são desenvolvidas por mulheres camponesas e ribeirinhas em contraposição à exploração, destruição e mercantilização dos campos e águas pelo agronegócio e a indústria da mineração. Essas mulheres, através de suas práticas, buscam desenvolver relação de harmonia entre o trabalho e a natureza.

A fala da integrante do SOF divergiu de outras discussões da CryptoRave por tirar o foco das tecnologias da informação. Grande parte do seu tempo de fala foi utilizado para

[53] Os Pontos de Cultura são projetos de grupos, coletivos e entidades que são financiados e apoiados institucionalmente pelo Ministério da Cultura (MinC) como parte da Política Nacional de Cultura Viva que teve início em 2004, no governo Lula, com o objetivo de realizar desenvolver e articular atividades culturais em comunidades e formar redes (disponível em <culturaviva.gov.br>, último acesso de 18 de julho de 2019).

justificar porque uma atividade como a agroecologia pertencia a um evento como a CryptoRave, junto dos debates sobre segurança de informação, privacidade e cultura hacker. A justificativa se baseou principalmente em três pontos. Primeiro, que os participantes da CryptoRave em seu determinismo tecnológico e fetiche pela tecnologia da informação acabam se esquecendo de que outras práticas também carregam conhecimento sobre tecnologias. A agroecologia seria um exemplo, uma vez que suas práticas são derivadas de conhecimentos tradicionais passados por gerações de mulheres. Segundo, que a agroecologia é uma atividade hacker tanto quanto invadir sistemas, encontrar vulnerabilidades, criar alternativas para proteção da privacidade e da liberdade na Internet como forma de proteger os indivíduos numa lógica colaborativa e solidária contra a concentração e mercantilização das informações e da conectividade. Isso porque parte da atividade das mulheres na agroecologia é encontrar formas de subverter a lógica de mercado do agronegócio, buscando espaços e utilizando técnicas e prática colaborativas e solidárias de plantio da subsistência por entre e em resposta à mercantilização dos campos por meio da monocultura. Aqui também se enquadra a identificação das sementes como portadoras de informação (material genético) e a luta para que sejam consideradas bem comum, o que as tornariam tecnologias livres. Terceiro, que a agroecologia é um movimento campesino que promove empoderamento das mulheres e é uma tecnologia feminista que se configura como resistência ao sistema capitalista. Desta perspectiva, a agroecologia deveria ser igualada ao movimento hacker, que existe para criar alternativas para proteção de dados e mediações de suas relações através da utilização da criptografia e *software* livre, desenvolvidos de forma diferente daquela capitalista, com base na liberdade, solidariedade e colaboração.

A mesa "Criptografia e agroecologia: alternativas feministas em defesa dos comuns - nossas tecnologias, outras formas de vida. Como semear a resistência feminista?!" (trilha política, 2017) é um exemplo de como as políticas hackers são múltiplas e as categorias de análise criadas se entrelaçam. As discussões sobre agroecologia poderiam facilmente ser enquadradas em "resistências", "políticas do dia-a-dia" em intersecção com gênero ou mesmo "transposição do ser hacker para outros meios", mas o entendimento da agroecologia como intrinsecamente hacker torna adequado seu enquadramento nesta subcategoria. Ao mesmo tempo, as políticas que emergem da agroecologia, considerando a definição de políticas hackers aqui utilizada – que se foca em hackers de computador e vincula hackerismos com tecnologias da informação –, não se enquadrariam como objeto desta pesquisa, o que torna a crítica ainda mais relevante. Os argumentos sobre a agroecologia conectam este movimento com manifestações hackers ao longo da história, como os *cypherpunks*, o movimento de

software livre e os zapatistas, mas a materialidade do movimento é outra que não as tecnologias da informação. A ideia de agroecologia como hackerismo, como apontado pela própria integrante do SOF, traz questões não só em relação à existência de um fetiche pela tecnologia da informação, mas também sobre as perspectivas tecnologicamente deterministas em se tratando dessas tecnologias.

Nesse sentido, o determinismo tecnológico se manifestou nas discussões assistidas na CryptoRave de duas formas. Primeiro, através da percepção de que as tecnologias da informação são pervasivas e ubíquas, as vezes manifestada na ideia de que é impossível fugir delas e de seus efeitos – considerando aqui a existência de disparidade de poder entre Estados/grandes corporações e indivíduos. Essa percepção também funciona como justificativa para o próprio evento e remete ao crescimento do engajamento político dos hackers observado por Coleman (2017), conectado ao sentimento de urgência frente à vigilância em massa e às ameaças à privacidade e autonomia dos cidadãos. Segundo, através do discurso de que apenas as próprias tecnologias da informação podem criar formas de resistência e subversão aos efeitos dessa ubiquidade – o que se assemelha às colocações dos autores que discutem formas de resistência do indivíduo (JORZA, 2012; MACHADO, 2015; VON WERDER, 2016) – e que se traduz em prática, com o desenho e desenvolvimento de criptografia e outras ferramentas de tecnologia da informação.

A fala da integrante do SOF também traz outra forma com que as políticas emergem na CryptoRave: a coexistência entre as manifestações de hackerismos, que entram em conflito quando precisam se reafirmar, combater ou reproduzir algumas características para ganhar espaço junto de outras que buscam delimitar o que pode ou não ser considerado hacker ou hackear. Nesse sentido, no caso da CryptoRave, ao analisar as falas e como foram feitas, outras formas do ser hacker tomaram como interlocutora, muitas vezes, aquela do "verdadeiro hacker", o indivíduo de grande conhecimento técnico-científico que programa, constrói e se diverte transformando tecnologias eletrônicas e digitais para sua satisfação, liberdade e seus pares (RAYMOND, 1996, revisão 1.51 out. 2017; EVANGELISTA, 2010).

Gênero, desigualdade, violência e cuidado

Todas as publicações desta subcategoria foram escritas por mulheres e, de modo geral, conversaram diretamente com a literatura do ciberfeminismo. Foi possível identificar duas principais temáticas: as desigualdades de gênero no ambiente de trabalho – junto da invisibilização do trabalho feminino em áreas de tecnologia da informação – e a violência de

gênero. As publicações partiram de estudos de caso sobre emprego e comunidades de *software* livre e das iniciativas de coletivos feministas, respectivamente. As discussões presenciadas na CryptoRave em intersecção de gênero apresentaram as mesmas temáticas e problematizações, manifestas nas falas de mulheres que atuam no mercado de trabalho das tecnologias da informação e integrantes de coletivos feministas.

Quanto ao ciberfeminismo, Natansohn (2018) e Natansohn & Paz (2018) tratam especificamente de discutir dois diferentes momentos e a possível emergência de um terceiro ainda vinculado ao anterior. Em resumo, num primeiro momento, o termo ciberfeminismo foi utilizado por Sadie Plant para identificar as problemáticas relacionadas às mulheres e tecnologias, particularmente sobre a percepção de que a liberação feminina das assimetrias de poder e valores tradicionais viria por meio da cooperação entre mulher, máquina e novas tecnologias. Outra origem teria sido junto ao grupo VNS Matrix, que buscava divertir-se com arte e teoria feminista e alguns dos primeiros trabalhos foram em homenagem à Donna Haraway e ao Manifesto Ciborgue (ROCHA 2006). Essa perspectiva inicial do ciberfeminismo, considerada utópica, tecnofílica, eurocêntrica e acrítica, foi reformulada por outras pesquisadoras e abriu espaço para enfoques construtivistas e de crítica feminista contemporânea (NATANSOHN, 2018). Um dos exemplos seria o tecnofeminismo de Judy Wajcman:

> "O tecnofeminismo (WAJCMAN, 2006), enquanto herança teórica crítica do ciberfeminismo, analisa como o gênero atua nos processos sociotécnicos: a materialidade da tecnologia propicia ou inibe a ação de sujeitos/as enredados/as nas relações de poder generizadas, assim como a agência desses/as sujeitos/as, nessas relações de poder, e afetam de diversas formas tanto o desenvolvimento como a circulação, distribuição, uso e apropriação de tecnologia." (NATANSOHN, 2018, p. 11)

Nesse sentido, a tecnologia seria simultaneamente causa e consequência das relações de gênero. Natansohn (2018) e Natansohn & Paz (2018) trabalham com a hipótese de que o ciberfeminismo está sendo atualizado com objetivos e táticas de luta diferentes ou "uma forma diferente de entender e praticar a comunicação digital, a geopolítica e a economia política de Internet, que coexiste com as formas dominantes" (NATANSOHN, 2018, p. 12). O caráter contestatório e contra-hegemônico caracterizaria esse novo momento, impulsionado por questões de segurança e vulnerabilidade e pelas experiências anteriores. Coletivismo, autonomia, controle, neutralidade e liberdade fazem parte do vocabulários das novas iniciativas, assim como infraestruturas distribuídas e tecnologias livres. O principal traço, para

Natansohn (2018, pp. 2-3), seria o "reivindicar o direito humano à comunicação e à internet, à vez que contestam e criticam os atuais direcionamentos da rede".

No caso das desigualdades de gênero no ambiente de trabalho e da invisibilização do trabalho feminino em áreas de tecnologia da informação, as autoras partem de alguns fatos. Primeiro, de que existe uma participação baixa e, muitas vezes, marginal de mulheres em comunidades, fóruns e eventos de *software* livre (ROCHA, 2006; PÉREZ-BUSTOS, 2010a; PAZ, 2013). Segundo, de que existe uma tendência a relegar às mulheres atividades de popularização (documentação, localização e ensino), consideradas subordinadas a outras atividades mais próximas do desenvolvimento tecnológico do *software* livre, como programação, vistas como mais especializadas (PÉREZ-BUSTOS, 2010a). De acordo com a análise de Pérez-Bustos (2010a):

> "*Esta relación jerárquica entre actividades más o menos especializadas se encuentra generizada en dos sentidos al menos. En primer lugar, las dinámicas de iniciación y socialización que consolidan la comunidad están soportadas sobre lógicas individualistas, solitarias, competitivas y elitistas que enfatizan en un quehacer tecnológico de carácter androcéntrico y que invisibilizan otros valores también relacionados, filosóficamente, con el Software Libre, como la diversidad, la democracia, la equidad y la mutualidad (Lin, 2006, 2007). En segundo lugar, estas dinámicas están relacionadas con una división sexual del trabajo, desde la cual el quehacer voluntario que realizan las pocas mujeres que hacen parte de estos colectivos está asociado a tareas que son consideradas como menos importantes y que se encuentran más cercanas al ejercicio de popularización hacia públicos no expertos."* (PÉREZ-BUSTOS, 2010a, p. 119)

É interessante notar que as mulheres entrevistadas para compor os estudos de caso de Pérez-Bustos (2010a), Suaza & Ortiz (2011) e Suaza (2013), em sua maioria, não se identificaram como feministas e, muitas vezes, apontaram a existência de situações de discriminação de gênero, mas nunca relativas a si mesmas. Pérez-Bustos (2010a, p. 128) identifica esse posicionamento como uma estratégia de sobrevivência, isso porque "*excluyendo no deliberadamente a otros y otras, desde un ejercicio de auto-inclusión, en tanto que su apuesta está en legitimar dentro de las comunidades de Software Libre um lugar para ellas mismas*". Da mesma forma, também no caso da comunidade de *software* livre colombiana Colibrí, as mulheres identificam a baixa participação feminina na comunidade, mas atribuem esse resultado a um problema considerado externo à comunidade: a baixa incursão feminina em cursos de ciência, tecnologia, engenharia e matemática (STEM, ou *Science, Technology, Engineering and Matemathics* em inglês). Para essas mulheres, a solução não seria responsabilidade das comunidades, mas das próprias mulheres, que deveriam mostrar mais interesse por essas áreas.

Além disso, Paz (2013) e Araujo & Gitahy (2017) apontam que muitas tentativas de organização e discussão feminina dentro das comunidades de *software* livre ou *hackerspaces* são encontradas com críticas sobre a relevância de se debater sobre questões de gênero, consideradas segregadoras e sexistas por membros do sexo masculino. Esse silenciamento não diz respeito apenas a essas discussões, mas também às práticas do dia-a-dia. Como explicitam Araujo & Gitahy (2017), o *hackerspace* majoritariamente frequentado por homens era dominado por um discurso de autoridade sobre conhecimento sobre tecnologias e as poucas mulheres que participavam de suas atividades sentiam-se inibidas em questionar ou opinar sobre. Em particular, esse discurso dominante tem base no mito da incapacidade das mulheres em criar tecnologias (SUAZA, 2013).

As questões de desigualdades de gênero e invisibilização feminina no ambiente de trabalho em áreas de tecnologia da informação, desenvolvidas na mesa "De volta ao ciberfeminismo: história e os desafios para o resgate e promoção da participação das mulheres na tecnologia" (trilha gênero, 2017), corroboraram as análises realizadas pelas autoras das publicações desta subcategoria. Foram notadas duas principais diferenças. Primeiro, as integrantes da mesa se identificaram prontamente como feministas e alvo de discriminação. Segundo, seus relatos e argumentações apresentaram traços de determinismo tecnológico, principalmente em relação ao potencial emancipatório do conhecimento em tecnologias da informação para mulheres.

A mesa apresentou três relatos sobre obstáculos que mulheres encontram na formação e no mercado de trabalho em TI e foi discutida a necessidade de resgatar a história e a contribuição das mulheres nessas áreas. Das integrantes, duas delas eram formadas em cursos de TI enquanto a terceira era socióloga, todas ativistas e envolvidas com iniciativas de emancipação e participação de mulheres em TI. Intercalando as falas, os relatos das três mulheres que compuseram a mesa tiveram como tema transversal a invisibilização do trabalho feminino e a desigualdade de oportunidades em relação ao gênero masculino na formação e nos empregos em TI. Duas das integrantes da mesa, que se identificaram como mulheres brancas e de classe média, apontaram que o papel das mulheres no desenvolvimento dos conhecimentos em TI foi marginalizado com a popularização dos computadores pessoais e a expansão do mercado de trabalho. Segundo as integrantes, algumas atividades, como a programação, chegaram a ser consideradas trabalho feminino.

Partindo do esquecimento da contribuição feminina para TI e do crescente esforço do ciberfeminismo em recuperar essa história, as duas integrantes focaram seus relatos, primeiro, em suas vivências sobre casos de misoginia durante a graduação e no ambiente de

trabalho e, segundo, em possíveis caminhos para garantir a presença feminina em todos os espaços de desenvolvimento de conhecimentos em TI.

O primeiro ponto foi marcado por relatos pessoais sobre o desestímulo por professores e superiores em procurar conhecimento e trabalhar em áreas mais técnicas de TI, principalmente as relacionadas a *softwares* e infraestruturas de rede, e ao estranhamento de clientes ao serem atendidos por mulheres para solucionar problemas nessas áreas. De acordo com as integrantes, as mulheres que se interessam por tecnologia da informação costumam ser incentivadas a trabalhar com programação e análise de sistemas, que são trabalhos pouco remunerados. Além disso, muitas empresas privadas contratam mulheres para cumprir cotas de contratação ou passar imagem de empresa inclusiva ao mercado consumidor, relegando posições secundárias e monetariamente desvalorizadas às mulheres.

Quanto ao segundo ponto, discutiram principalmente como desde cedo os papéis de gênero são reforçados para as mulheres, que não são estimuladas desenvolver interesse em áreas da STEM, consideradas intrinsecamente masculinas. Para as integrantes, o problema estaria na importância da tecnologia para a vida contemporânea, de forma que se mulheres não estão nessas áreas, acabam ficando excluídas dos avanços tecnológicos e do futuro. Uma das profissionais de TI, disse ter tido incentivo desde pequena a mexer em computadores e destruir e reconstruir coisas, o que a levou a procurar cursos de graduação na área. Para ambas as integrantes, a solução para o problema da falta de mulheres em STEM seria justamente incentivar o interesse de meninas nessas atividades – mesma solução encontradas pelas profissionais de TI entrevistadas por Pérez-Bustos (2010a).

A ideia de que participar dos avanços tecnológicos e do futuro perpassa necessariamente o conhecimento em tecnologias da informação é uma ideia tecnologicamente determinista também identificada nos estudos hackers (RAYMOND, 1996 revisão 1.51 out. 2017; SÖDERBERG, 2013). Ao mesmo tempo em que esse argumento atribui às tecnologias da informação potencial emancipatório para mulheres – trazendo, implicitamente, a ideia de que a solução para a discriminação, invisibilização e exclusão dos ganhos do avanço tecnológico repousa na incursão feminina em áreas de tecnologia de informação –, acaba relegando menor importância a outras tecnologias na participação das lutas por igualdade de gênero e autonomia feminina e da construção de futuros[54]. Por isso, foi interessante quando a

[54] A mesa "De volta ao ciberfeminismo: história e os desafios para o resgate e promoção da participação das mulheres na tecnologia" aconteceu logo antes – e no mesmo espaço – da "Criptografia e agroecologia: alternativas feministas em defesa dos comuns - nossas tecnologias, outras formas de vida. Como semear a resistência feminista?!", o que ofereceu um contraponto interessante em relação às tecnologias para emancipação e autonomia feminina e sobre quais tecnologias são construídas e trabalham para esse fim.

terceira integrante da mesa, que se identificou como mulher negra e periférica, trouxe um caráter interseccional para o debate. De acordo com ela, ser profissional da área de TI nunca foi uma escolha, uma questão de estímulo desde a infância, mas uma necessidade, pois era a área que mais estava empregando quando ela precisou decidir sobre qual graduação cursar e, sendo responsável pelo sustento de sua família, precisava ser empregada rapidamente.

Retomando as discussões realizadas na publicações, a segunda identificada foi a violência de gênero. Aqui, em particular, as análises retomaram o contexto de controle e vigilância massiva apresentado anteriormente. Sasha Costanza-Chock[55] – uma das palestrantes principais da edição de 2017 – trouxe para a CryptoRave que cada indivíduo vivencia a vigilância de forma diferente dependendo da sua relação e localização no que chamou de matriz da dominação, formada por forças de opressão da supremacia branca, capitalismo, heteropatriarcalismo e colonialismo. Nesse sentido, alguns corpos como os femininos, transgêneros, negros, periféricos, de colônias e ex-colônias europeias vivenciariam os efeitos da proliferação das tecnologias de vigilância mais intensamente porque são vítimas constantes de assédio, ameaça e violência na Internet. Em termos de violência contra a mulher, a ameaça não parte apenas do Estado ou das grandes corporações, mas companheiros, ex-companheiros, familiares e outros conhecidos.

> "Na internet, a violência contra as mulheres [...] se dá tanto sob a forma de assédio, extorsão, ameaças, roubo de identidade, *doxxing*, alteração e publicação de fotos e vídeos sem consentimento ou uso indevido, ofensas, *stalking*, invasão ou hacking de computadores, criação de perfis falsos criados para assediar; coerção para deletar perfis; dentre outras formas como também na forma de discurso de ódio: montagens racistas de fotos ou vídeos, criação e divulgação de memes ofensivos (gifs, etc.), comentários misóginos, transfóbicos e/ou racistas, criação de *hashtag* para promover discurso ofensivo, uso de *bots* para as ações anteriores." (NATANSOHN, 2018, pp. 4-5).

Os ataques acontecem também às páginas e perfis feministas, através de denúncias sobre o conteúdo, sobrecarregamento dos moderadores de plataformas e publicação de ameaças e insultos.

> "Os ataques públicos com ofensas e ameaças ou a derrubada de páginas e perfis feministas são estratégias de silenciamento, que acontecem por meio de censura, quando os canais de comunicação das ativistas fica impossibilitado de manter a comunicação, ou pela autocensura, que faz com que mulheres deixem de manifestar suas opiniões ou mesmo retirem seus perfis da Internet por medo de qualquer tipo de ataque pessoal. São táticas que atingem, dessa forma, o direito fundamental de liberdade de expressão." (ARAUJO & GITAHY, 2017, p. 4)

[55] Sasha Costanza-Chock é ativista e professora associada do Instituto de Tecnologia de Massachusetts (MIT) em mídia cívica. Pesquisa sobre movimentos sociais, mídia e tecnologias da computação.

As mulheres que sofrem ataques pela Internet têm suas vidas reais impactadas uma vez que, como apontam Araujo & Gitahy (2017) e Natansohn (2018), as tecnologias digitais fazem parte de quase todos os aspectos da vida contemporânea. Os ataques acabam levando a "danos à reputação e produzem isolamento, depressão, ansiedade, medo e até suicídio" (NATANSOHN, 2018, p. 5), além de abandonamento de emprego e mais assédio.

Tanto nas discussões sobre as desigualdades de gênero no ambiente de trabalho e invisibilização do trabalho feminino em áreas de tecnologia da informação, quanto em violência de gênero, as autoras apontam que uma das principais estratégias encontradas pelas mulheres tem sido a auto-organização, a ocupação de espaços tipicamente masculinos ou criação de outros exclusivos, semelhante ao descrito por Toupin (2014) ao tratar dos *hackerspaces* feministas, como apontado no segundo capítulo.

Dentre os espaços ocupados estão as mesas e atividades em eventos como a CryptoRave, o FISL, a Campus Party e o Fórum da Internet no Brasil (PAZ, 2013; ARAUJO & GITAHY, 2017), além de fóruns, listas de discussão e comunidades de desenvolvedores (PAZ, 2013), onde mulheres vão para discutir gênero, tecnologia, sub-representação, desigualdades, entre outros temas.

Considerando a criação de espaços exclusivos surgem exemplos interessantes. De forma geral, nesses espaços prevalecem outras lógicas daqueles das comunidades de *software* livre populadas principalmente por homens. Questionando o que é, de fato, abertura e heterogeneidade, esses novos espaços acabam reivindicando o compartilhamento, a acolhida, o não controle característicos do *software* livre como femininos (PÉREZ-BUSTOS, 2010a) e articulando redes de colaboração, construindo projetos e iniciativas em conjuntos uns com os outros (ARAUJO & GITAHY, 2017; NATANSOHN, 2018).

Dentre eles, primeiro, estão as comunidades de desenvolvedoras. Uma delas é a Chicas Linux, grupo de jovens colombianas desenvolvedoras pesquisado por Suaza (2013) que nasceu do Linux Colibrí, comunidade de *software* livre estudada por Pérez-Bustos (2010a). Ainda que não apresentassem interesse em se identificar como feministas, as jovens começaram a entender a relação entre mulheres e tecnologia como algo que deve ser disputado depois que a pesquisa etnográfica de Tania Pérez-Bustos tornou visível as percepções que já tinham sobre as desigualdades que permeavam a comunidade.

Segundo, os coletivos e organizações feministas. Natansohn (2018) lista uma série de coletivos, sites e ferramentas de cuidado e segurança digital, conectando-os ao contexto de violência digital e coleta e mercantilização de dados pessoais como tática de rastreamento e vigilância que colocam em risco a privacidade e a intimidade.

> "Uma das práticas mais difundidas por esses grupos é o trabalho sobre os cuidados de si e das outras para prevenir e agir ante ataques misóginos, mas também para enfrentar o direcionamento que tem tomado a tecnologia digital no que se refere a seus protocolos de funcionamento, que permitem o rastreamento e a vigilância em escala nunca vista. Avaliando estas práticas e a violência que estas implicam para a segurança, a privacidade e a intimidade das mulheres, grupos feministas desenvolvem diferentes estratégias, como a produção de ferramentas para a segurança digital e a prevenção de ataques virtuais. Essas adquirem formatos diferentes quando disponibilizadas online: manuais (em formatos para fazer *download*), aplicativos ou textos online com recomendações. Como parte do ativismo feminista digital essas ações não se limitam a serem publicadas e divulgadas em ambientes virtuais. Oficinas e cursos presenciais são promovidos e realizados por muitas organizações com apoio de ONGs, em diferentes locais, sob cuidados extremos para manter o sigilo das participantes e do local, pois muitas delas são militantes dos direitos humanos em países que penalizam qualquer dissidência política." (NATANSOHN, 2018, pp. 3-4).

Dois coletivos chamados Ciberseguras e Coding Rights apresentaram suas atividades na edição de 2018 da CryptoRave e trataram de violência de gênero na Internet. Enquanto o primeiro grupo compartilhou o processo de criação do seu site, que envolveu trocas com hacker feministas de toda América Latina, e pediu para que não fossem tiradas fotos ou gravados vídeos da apresentação para a segurança das palestrantes, o segundo lançou a iniciativa SaferManas, uma série de *gifs* com dicas de segurança sobre as ameaças que mulheres e pessoas de gênero não-binário sofrem nas redes (como manter senhas seguras, cuidar das fotos íntimas, dados de localização e outros que podem ser utilizados para perseguição). Também foram distribuídos adesivos de ilustrações presentes nos *gifs*. O mais popular foi "#SAFERMANAS AMAM SAFERNUDES <3" com a ilustração de uma mulher idosa. Relacionando as colocações de Natansohn (2018) com as apresentações dos dois coletivos, fica evidente que o objetivo não é controlar ou reprimir atividades, expressões, sexualidade e outras experiências femininas na Internet, mas garanti-las através da segurança digital. Como colocam Araujo & Gitahy (2017, p. 7), "as oficinas e rodas de conversa sobre segurança no compartilhamento de imagens íntimas colaboram para um tema mais amplo a respeito da decisão sobre o próprio corpo e a liberdade sexual das mulheres".

Outro exemplo é a MariaLab, *hackerspace* feminista no Brasil abordado por Araujo & Gitahy (2017). Levando em consideração os dois tipos de organizações não governamentais discutidos por Ronfeldt & Martínez (1997) e Pitman (2007) – as orientadas para problemas específicos (direitos humanos e indígenas, ambiente, gênero, entre outros) e as orientadas à construção de infraestruturas para outras organizações e ativistas e que se mostram preocupadas com a natureza e governança da Internet – as atividades da MariaLab permitiriam identificá-la com ambos.

> "Algumas oficinas foram criadas pela MariaLab com o intuito de disseminar criptografia e ferramentas de segurança na rede, ensinando às mulheres como podem manter seus dados sigilosos e permanecer anônimas. As oficinas são direcionadas tanto para coletivos feministas como para a segurança individual. Conhecer melhor como funciona a comunicação em rede e os riscos aos quais estão expostas, faz com que as mulheres tenham mais consciência e controle sobre suas ações na rede." (ARAUJO & GITAHY, 2017, p. 7)

Junto do projeto de um servidor para hospedagem de sites de coletivos feministas e outras ferramentas para sua organização e comunicação, desenvolvido em colaboração com outros coletivos, as atividades da MariaLab estão voltadas para questões de gênero ao mesmo tempo em que oferecem infraestrutura e suporte para a atividade de outras ativistas. Para Natansohn, (2018), o cuidado entre ativistas é uma forma de intervenção política em si.

A apresentação do projeto de servidor, em particular, foi uma das mesas mais interessantes que participei da CryptoRave. Com o título "(Ciber)espaços seguros: redes autônomas feministas" (trilha gênero, 2017) e com mulheres integrantes da MariaLab e especialmente do projeto Vedetas, o tema foi a construção e manutenção de uma servidora feminista que oferece espaço seguro e autônomo para grupos feministas e suas atividades na Internet. Sobre a questão de linguagens e tecnologias feministas, foi escolha das integrantes do projeto utilizar apenas artigos, pronomes e substantivos no feminino. De acordo com uma delas, brincar com os nomes das coisas é muito comum na cultura hacker – o que é corroborado por Coleman (2013; 2017) – e, no caso do projeto Vedetas, é uma forma de posicionamento e resistência, uma vez que a maioria dos técnicos de infraestrutura e administração de redes são do sexo masculino, a ponto da parte técnica ser comumente atribuída aos homens tanto em terminologia quanto em imaginário ("o técnico", "o cara da manutenção"), trazendo à discussão, mais uma vez, a questão da invisibilidade do trabalho feminino em tecnologias da informação e comunicação. De acordo com as integrantes, um dos objetivos foi provocar reflexão sobre o que são tecnologias feministas de infraestrutura e como criar espaços digitais seguros para mulheres e pessoas transgênero. As redes autônomas descentralizadas estariam atraindo bastante interesse de ativistas, movimentos sociais e comunidades periféricas porque garantiriam autonomia e espaço seguro da vigilância em massa e mercantilização dos dados e da conectividade pelas grandes corporações e pelo Estado.

A importância de criar uma rede autônoma comunitária feminista estaria relacionada com os significados desses termos. Uma rede autônoma é uma forma de conectar mulheres, criar relações, solidariedade e cuidado através de uma infraestrutura de redes – não necessariamente a Internet – que sob controle de profissionais do sexo masculino e

propriedade de grandes corporações é dominada por uma lógica machista e capitalista. Segundo as integrantes, uma vez que mulheres sofrem grande parte dos ataques de assédio e violência na Internet, através de ameaças ou exposição de informações pessoais, é essencial que tenham conhecimento sobre segurança da informação e autonomia em relação à infraestrutura de redes para se protegerem e, se necessário, contra-atacarem. Sendo autônoma e comunitária, são as próprias mulheres que dominam o técnico, controlam o funcionamento da rede e gerem seu conteúdo, diminuindo sua vulnerabilidade em relação à dependência de aliados masculinos, à dominação das corporações capitalistas e ao controle do Estado. As redes autônomas comunitárias feministas se configuram como espaço seguro e o projeto Vedetas surge e se torna parte de uma racionalidade comum de outros espaços feministas.

Neste caso, de posicionamentos e engajamentos esclarecidos, o disputar o ordenamento do mundo a partir do reordenamento das tecnologias da informação é mais evidente em relação a outros – como as políticas que emergem do dia-a-dia do trabalho feminino nas áreas de tecnologia da informação ou na organização de comunidades de desenvolvedores de *software* livre. Considerando as descrições das integrantes do projeto Vedetas, para as redes autônomas feministas as escolhas de adoção ou não-adoção de tecnologias se configuram como alternativas tecnopolíticas porque propõem outras formas de desenhar, desenvolver e gerir tecnologias da informação a partir de outras visões de mundo.

A importância atribuída por Maxigas (2017) aos usuários especializados deriva, principalmente, do fato de que ocupam lugar privilegiado nas decisões sobre desenho, desenvolvimento e gestão das tecnologias, de forma que suas preferências teriam impacto no direcionamento do desenvolvimento tecnológico. Esses usuários sofisticados são homens brancos de meia idade, extremamente qualificados, profissionais de tecnologia e moradores de centros urbanos. As integrantes do projeto Vedetas, assim como os coletivos aos quais os serviços prestados se dirigem, não ocupam um lugar de privilégio: há um questionamento constante, como evidenciado tanto pelas publicações enquadradas nesta subcategoria quanto pelos relatos nas mesas da CryptoRave, da sua legitimidade em fazer parte do grupo de atores que podem disputar a construção de futuros. Isso torna a permanência das mulheres em empregos na área de tecnologias da informação, a ocupação de eventos como a CryptoRave e a construção de tecnologias feministas formas de resistência e subversão, assim como faz com que todas as escolhas tecnológicas sejam políticas e apontem para a possibilidade de outros futuros.

4.3 Transposição do ser hacker para outros meios

Nesta categoria, as análises apontam para elementos do ser e fazer hacker que são transpostos por outros meios inicialmente não vinculados ao hackerismo – como arte, literatura, educação, saúde, meios urbanos. A transposição do ser e fazer hacker, no caso desse conjunto de publicações, nunca é completa, mas são escolhidas algumas características específicas que, para os autores, dão outros sentidos para esses meios. Dessa forma, a transposição funciona como um processo de apropriação, adaptação e aprendizado e engendra novas políticas. Novamente, um dos elementos em comum das análises realizadas foi a centralidade das tecnologias livres (*softwares* e *hardwares*).

De forma geral, foi possível distribuir as publicações em duas subcategorias utilizando os termos mencionados nas análises realizadas: comportamentos hackers e metodologias hackers.

Comportamentos hackers

Em comportamentos hackers estão contidos elementos como apropriação, experimentação e subversão e foram identificados principalmente em relação à música, arte e literatura. Esses elementos conversam diretamente com o preceito "*you can create art and beauty on a computer*" da ética hacker observada por Levy (1984, p. 31). É interessante que em todas as publicações desta subcategoria, os elementos do ser e fazer hacker são identificados como parte fundamental destas novas formas de música, arte e literatura que são politizadas. Nesse sentido, o processo criativo e os produtos se tornam formas de engajamento político. Outro elemento em comum é o contexto em resposta ao qual surgem essas novas formas de música, arte e literatura – o mesmo apontado pelas publicações em "resistência" e "gênero, desigualdade, violência e cuidado": capitalismo neoliberal, globalização, controle e vigilância massivos e memórias de ditaduras violentas.

Dentre os casos estudados estão o *chipmusic*, *netart*, *codework* e a literatura cyberpunk, que proveem exemplos interessantes de outras formas de emergência das políticas hackers.

Em relação à música, Schäfer (2015) discute as características da *chipmusic*, produzida a partir dos chips sonoros de consoles e computadores pessoais antigos, principalmente das décadas de 1980 e 1990. Nos equipamentos são instalados *trackers*, *softwares* que permitem a criação de sons digitais. Pela dificuldade em trabalhar com *hardware* antigo e criar/adaptar *softwares*, superar limitações, apropriar os circuitos e

experimentar com os equipamentos para encontrar funções não previstas em manuais são partes essenciais da *chipmusic*, que trabalha com proximidade da ideia subversão da obsolescência. Como coloca Schäfer (2015, p. 93), "da mesma forma, os hackers e os músicos da *chipmusic*, quando modificam os equipamentos ou *softwares* para que executem funções que não foram predeterminadas em sua concepção, estão tentando adentrar a caixa-preta, jogar contra o aparelho". Esses *softwares*, assim como as músicas criadas por meio da *chipmusic* são compartilhados livremente na Internet pelos programadores e artistas, como parte de seu ativismo contra a apropriação privada e comercial dos elementos culturais e técnicos relacionados a essa forma de arte.

Um dos primeiros exemplos do livro de Levy (1984) sobre hackers e sua capacidade de experimentar, aprender e transformar tecnologia envolve música. Um dos fundadores do *Tech Model Railroad Club,* Peter Samson, teria sido o primeiro a criar música a partir do TX-0 quando percebeu que o computador emitia uma série de sons de acordo com o posicionamento de caracteres binários no código escrito. Interessado em música, Samson começou a programar, variando os binários em posições específicas, conseguindo assim diferentes sons.

> *"So it was that a computer program was not only metaphorically a musical composition - it was literally a musical composition! It looked like - and was - the same kind of program which yielded complex arithmetical computations and statistical analyses. These digits that Samson had jammed into the computer were a universal language which could produce anything - a Bach fugue or an antiaircraft system."* (LEVY, 1984, p. 22)

Fernández (2011) e Ledesma (2015) fazem suas análises em relação a duas formas específicas de *netart*: arte hacker e poesia em código, respectivamente. Ambos os autores partem da perspectiva que os artistas latino-americanos usam código e programação como forma de posicionarem-se criticamente contra o capitalismo pós-industrial, o poder das grandes corporações e as formas de controle que vêm junto da intensificação da adoção das tecnologias da informação. Particularmente, ao trazer essas formas de arte para o contexto latino-americano, os artistas buscam reconfigurar a cartografia do ciberespaço, infectando o idioma oficial da Internet (FERNÁNDEZ, 2011), e democratizar a programação, encorajando usuários a se transformarem em artistas-programadores (LEDESMA, 2015).

Portanto, assim como em "resistências", as tecnologias da informação que criam formas de opressão também abrem espaços para novas formas de subversão e, neste caso, os artistas se tornam hacktivistas.

> *"Si el artista muestra una cierta visión de la vida y la sociedad, el activista de arte hacker muestra las quiebras del sistema y demuestra como la dictadura de la máquina puede subvertirse o lo que es lo mismo, que la sociedad capitalista puede descontrolarse utilizando en beneficio próprio sus mismas herramientas de control. La pregunta que nos surge ahora es donde acaba el activismo y comienza el arte y vice-versa."* (FERNÁNDEZ, 2011, p. 91)

Para os artistas estudados por Fernández (2011) e Ledesma (2015), parte da experimentação e subversão vêm da criação coletiva da arte, de forma que a relação entre arte e espectador se transforma em uma relação entre desenvolvedor e usuário, que também se torna desenvolvedor no contexto das tecnologias livres, como no caso da arte hacker e da poesia em código.

As táticas e ferramentas utilizadas, porém, são diferentes. A arte hacker apresentada por Fernández (2011) utiliza de desfiguração e clonagem de sites em outras línguas, propagação de vírus, lentidão no acesso e programação de *bugs* no processo de criação e divulgação das artes. Já a poesia em código se configura como escrita experimental que combina linguagens computacionais e humanas para criar poesias que, muitas vezes, precisam ser rodadas como programas, causando desfigurações na interface do usuário, em navegadores e sites ou evidenciando os aspectos humanos dos códigos.

Por fim, quanto à literatura, foram identificados dois movimentos: o primeiro sobre a inter-relação entre forma e conteúdo da obra de Nalo Hopkinson, autora do cyberpunk cubano e o segundo sobre as influências das experiências hacktivistas zapatistas e seus desdobramentos no cyberpunk mexicano.

Quanto ao primeiro, Enteen (2007) demonstra que Hopkinson escreve sobre hackers e, ao mesmo tempo, hackea uma série de tradições linguísticas, estilos e gêneros literários – hacking, aqui, significando subversão:

> *"To create such a text, Hopkinson combines English with Trinidadian and Jamaican creole, 'hacking' a language that recalls the histories of the middle passage, slavery, and imperialism. Furthermore, her characters break and create code, 'hacking' in speech as well as through their conceptions of community, 'hacking' the genre of science fiction through the blending of cyberpunk and planetary romance, creating fiction reminiscent of the corpus of Bruce Sterling's 'global tourism' sf [science fiction] (Jameson, Archaeologies 384-85), but seen from the other side. Centered on a feminine Artificial Intelligence commanding the planet and its inhabitants, Midnight Robber challenges the conventions of cyberpunk, revealing its ideological underpinnings, and com accounts of the intersections of gender, technology, and corporate presence"* (ENTEEN, 2007, pp. 263-264)

Quanto ao segundo, García (2012) analisa um tema comum das obras do cyberpunk mexicano: os paradigmas nacionais que colocaram o México como uma nação

moderna e o fato dos hackers aparecerem não como fonte cultural de inovação, mas como trabalhadores forçados a escolher entre a economia da informação ou crime organizado. García (2012) discute que os anos seguintes ao levante zapatista foram marcados pelas tentativas de grupos políticos mexicanos em corromper o espírito hacker das comunidades interessadas em desenvolvimento técnicos e políticos como forma de exercer cidadania através da privatização do conhecimento hacker e de sua absorção pelo sistema corporativo e político. A incorporação dos efeitos da absorção dos hackers pelo sistema corrupto mexicano, das reformas neoliberais e da globalização teriam dado o tom dos cenários do cyberpunk mexicano, cercados de crise econômica, desemprego, pobreza extrema e desesperança.

Metodologias hackers

Nesta subcategoria, os estudos analisam a implementação de formas de organização e trabalho hackers em outras áreas. Ainda que os autores tratem de aplicações e resultados diferentes, o elemento em comum são as redes de comunicação e colaboração pela Internet, entendidas como características dos hackers, como solução para problemas específicos dos seus objetos de estudo. Especificamente, Pretto (2010) encontra nas tecnologias digitais de informação e comunicação uma solução para a falta de oferta de professores através do uso de ferramentas de compartilhamento de arquivos em rede, que seriam um caminho para a democratização e socialização da produção acadêmica e dos processos formativos. As redes, de acordo com Pretto (2010), não serviriam apenas para compartilhamento de conteúdo, mas para a formação contínua dos professores através da ampliação da rede colaborativa entre diferentes níveis de ensino e instituições. Já para Guizardi et al. (2018) as redes de colaboração dos hackers tomam forma de hackatons. Nesse sentido, “a reunião de pessoas engajadas pelo desenvolvimento tecnológico, a duração limitada das atividades e o compartilhamento de objetivos em atividades intensivas” junto do caráter lúdico, criativo e colaborativo do trabalho hacker (GUIZARDI et al., 2018, p. 449) fariam dos hackatons uma forma eficiente de direcionar a inovação e melhoria de respostas a questões sociais, governamentais e corporativas. Sendo um fenômeno relativamente novo, Guizardi et al. (2018) advogam pela utilização dos hackatons por governos e corporações para a solução de problemas da área da saúde, identificando algumas das iniciativas já realizadas. Por fim, Chiesa & Cavedon (2015) discutem as redes de colaboração hackers a partir de uma característica específica: a descentralização ou, como colocam, a organização não-hierárquica. Para os autores, formas não hierárquicas de organização através do digital não só permitem

um processo de decisão com base no consenso, mas sua filosofia – a de defesa da Internet livre, aberta e fora do controle das grandes corporações – seria absorvida pelos grupos que as implementam.

4.4 Outras formas de fazer política pública, influenciar tomada de decisões ou se expressar politicamente: democracia e tecnologia

Nesta categoria, os estudos apontam para a discussão entre hackers e hackerismos em relação ao Estado e às formas de interação com instâncias tradicionais de política para exercício de direitos civis e da cidadania. Ainda que as análises difiram em relação ao seu significado, o ponto de partida comum foram as consequências e impactos da introdução e expansão das novas tecnologias da informação. De modo geral, nos casos estudados, entende-se que as novas tecnologias da informação transformam as relações entre indivíduos-Estado, de onde emergem as políticas hackers.

Algumas das análises apresentadas em "resistências" e "transposição do ser hacker para outros meios", particularmente a arte hacker, também poderiam ser consideradas nesta categoria. Isso porque as resistências e os hackerismos em outros meios implicam na utilização de táticas de hacktivismo e estratégias legais de manifestação como forma de expressão política, em alguns casos, buscando reações (Anonymous) ou negociações com as instituições de poder (maias hackers e zapatistas). Nas publicações em que esta foi a forma primária de emergência das políticas hackers, as discussões realizadas giraram em torno dos usos de ferramentas de tecnologia da informação para fomentar governo aberto e como forma de participação cidadã; as políticas que emergem de novas formas de relação entre indivíduos-Estado e Estado-hackers, e; a utilização de características hackers como racionalidade de políticas públicas de inclusão digital.

Considerando essas diferentes formas de emergência das políticas hackers e as considerações de Coleman (2017), é possível afirmar que, enquanto aquelas em "resistências" e "transposição do ser hacker para outros meios" se configuram como políticas radicais, as relacionadas ao governo aberto e hacking cívico seriam políticas liberais. Essa distinção se faz possível tanto pelos casos estudados em cada publicação quanto por sua análise. Dessa forma, foi possível identificar em parte das publicações desta categoria um entusiasmo acrítico em relação às tecnologias da informação como meio de transformação da relação cidadão–Estado e o foco das análises foram as formas de exercer liberdade de expressão e a participação política dentro das vias tradicionais da política.

Parra (2012), por outro lado, desenvolve uma discussão mais ampla sobre as formas contemporâneas do exercício do poder e da prática política mediados pelas novas tecnologias da informação, especificamente em relação à produção e ao controle de informações nas redes digitais. As configurações das redes digitais que interessam à análise de Parra (2012) são aquelas responsáveis pela desterritorialização e reterritorialização simultâneas – como os protocolos. Isso porque ao mesmo tempo em que a Internet dá a possibilidade de interação simultânea entre pessoas e objetos fisicamente distantes, ferramentas de localização e rastreamento permitem a identificação de várias informações sobre as interações.

> "Quando essas duas dinâmicas se articulam, confrontamo-nos com novas possibilidades de coleta de dados informáticos transacionados nas redes digitais pelos sujeitos conectados, criando tanto possibilidades de interação e colaboração social como condições ampliadas de identificação e vigilância." (PARRA, 2012, p. 112)

> "Na medida em que a comunicação em redes digitais funciona segundo determinadas configurações, resultantes de dinâmicas simultaneamente sociopolíticas e técnicas, a disputa sobre a regulação jurídica das atividades ciberneticamente mediadas torna-se fundamental para evitar a emergência de um controle social tirânico, seja ele corporativo ou estatal." (PARRA, 2012, p. 112)

Os mecanismos de controle e vigilância seriam apenas o outro lado – inicialmente não previsto pela sociedade civil – da utilização livre das redes digitais. Dessa forma, ao refletir sobre a política na cibercultura por duas direções, a política das tecnologias digitais (tecnopolítica) e a política ciberneticamente mediada (ciberpolítica), Parra (2012) argumenta que as disputas sobre as configurações das tecnologias também são disputas sobre a esfera política. Um dos exemplos está relacionado à escolha do Ministério da Cultura (MinC) em utilizar de tecnologias livres e identificação voluntária para realização da consulta pública sobre as reformas da Lei dos Direitos Autorais em 2010. Ciberativistas que analisaram os dados da consulta pública notaram que o grande volume de respostas contrárias às mudanças tinham origem nas mesmas duas instituições, que mobilizaram seus funcionários para a votação. Outro exemplo interessante seria a expansão da comercialização de dados pessoais coletados através de rastreamento digital por empresas privadas para instituições governamentais. A obtenção de dados pessoais por instituições governamentais é facilitada pela mediação das empresas privadas, que estão presentes em diferentes espaços na Internet e encontram uma regulação mais flexível sobre coleta e comercialização de dados. Mas há um desnível em relação aos atores que podem ou não coletar e utilizar dados e informações.

Mota, Hayashi & Fernandes (2016) discutem o outro lado da jurisdição: quando os dados coletados e distribuídos são do governo. Os autores expõem os esforços dos legisladores em garantir que as táticas de desobediência civil eletrônica sejam enquadradas como crime. Particularmente tratando das ações políticas dos Anonymous, Mota, Hayashi & Fernandes (2016) apontam que a legislação brasileira não prevê desfiguração de sites, ataques de DDoS, manifestações e sabotagens virtuais como crime porque essas táticas não se configuram como invasão de dispositivo, considerada crime pela lei. Porém, o Código Penal Brasileiro pune interrupções, perturbações e atos que prejudiquem serviços de informação. Além disso, o anonimato e o acesso a informações privadas institucionais, segredos empresariais e outras informações sigilosas – táticas características dos Anonymous – são legalmente proibidos e podem agravar as punições.

Duas das publicações dessa categorias analisaram uma forma específica e legal de obtenção de dados governamentais, o governo aberto. Essa forma de relação entre indivíduos e governo pressupõe certo entusiasmo em relação aos aspectos interativos, colaborativos e organizacionais das redes digitais, que trariam novas possibilidades para participação cidadã nos sistemas democráticos. Segundo Jolías & Prince (2013), o paradigma do governo aberto se sustentaria em três pilares – transparência, colaboração e participação. Nele, os dados criados pela administração pública são considerados pertencentes à sociedade.

> "Trata-se de uma filosofia e de uma prática que consiste na abertura dos dados produzidos pelos governos de forma que os cidadãos possam não apenas acessá-los, mas manipulá-los a fim de produzir novas informações e conhecimentos capazes de gerar serviços mais eficientes. Nasce no contexto digital como replicação de modelos representados pelo *software* livre (*open source*), da World Wide Web e todo o desenvolvimento da tecnologia de compartilhamento de arquivos e produção colaborativa aplicado a gestão pública governamental. Implica numa nova técnica de governo, também chamada de Governo 2.0, que o entende como uma plataforma aberta a inteligência distribuída em rede para o trabalho colaborativo como um novo sentido da participação cidadã." (TAVARES, 2011, p. 22).

Pela análise dos autores, a ideia por trás do governo aberto seria aproveitar a criatividade de outros atores interessados – empresas privadas, organizações da sociedade civil, ativistas – disponíveis nas redes para gerar soluções para gerar informações, conhecimentos e serviços. Essa racionalidade se assemelha ao modelo bazar discutido por Eric Raymond (1999) em que a ideia em compartilhar o código é garantir que mais pessoas despendam tempo no desenvolvimento de *software* e resolução de problemas de forma colaborativa, utilizando a inteligência coletiva espalhada pela Internet. O mesmo aconteceria

para os dados públicos, o desenvolvimento de aplicativos de valor cívico e a resolução de problemas sociais.

Uma das questões importantes levantadas por Tavares (2011) e Jolías & Prince (2013) é a utilização de tecnologias livres e formatos abertos. Abertura dos dados significa, nesse contexto, não existir barreiras de propriedade para acesso e compartilhamento dos dados públicos por qualquer um que esteja interessado em tratá-los e utilizá-los.

Os hackers fariam parte do ecossistema de governo aberto como intermediários entre os dados públicos e os cidadãos. Seu papel seria garantir não só a abertura e disponibilização dos dados, mas também os *softwares* livres para seu tratamento, além de advogar pela importância da transparência da administração pública e pressionar os órgãos governamentais a adotarem formatos abertos para os dados (TAVARES, 2011).

Ainda que ambos apresentem uma visão otimista sobre as possibilidades de participação cidadã propiciadas pelas dinâmicas do governo aberto, Jolías & Prince (2013) apresentam críticas em relação ao alcance das políticas de governo aberto: em alguns casos, os hackers tomam para si a responsabilidade em produzir informação acessível e compreensível, função que deveria ser assumida pela administração pública, que acaba terceirizando os custos de adotar dados em formato aberto. Além disso, os autores contestam a quantidade de dados que são disponibilizados pelos governos, que seriam irrelevantes para fins de transparência e participação e suficientes apenas para criar aplicativos de prestação de serviços do setor público ao cidadão, que também deveriam ser de responsabilidade da administração pública.

O último conjunto de publicações pertencentes a esta categoria analisa as relações entre hackers, tecnologias da informação e administração pública por meio da formulação e implementação de políticas públicas. De um modo geral, as publicações exploram como preceitos hackers são inseridos nas políticas públicas, discutindo as possibilidades (MENDOZA, 2002; DONAS, 2007) e desdobramentos (VILLANUEVA & OLIVERA, 2012; CHAN, 2014) de sua incorporação.

Duas políticas diferentes são discutidas por esses autores. A primeira é o governo eletrônico, que Donas (2007) descreve como uma forma de aproximar o Estado do cidadão através do acesso a serviços públicos pela Internet e Mendoza (2002) como a modernização do Estado nos âmbitos da participação, conteúdos e compromisso cultural pelo uso da Internet. A segunda é o programa *One Laptop Per Child* (OLPC) no Peru, que previa a entrega de um computador portátil (modelo XO) por criança para ser utilizado dentro e fora

do ambiente escolar, com o objetivo de melhorar a qualidade da educação pública primária de crianças da zona rural do Peru e em situação de extrema pobreza.

Tanto no caso do governo eletrônico quanto do OLPC, a racionalidade por trás da formulação da política seria a mesma: forte determinismo tecnológico na forma de entusiasmo acrítico em relação às tecnologias da informação como caminho para emancipação do indivíduo e da ideia de que a falta de acesso às tecnologias da informação são principal impedimento à transformação social na sociedade da informação.

> *"Junto con estas nuevas formas de apropiación social de la tecnología, las medidas de universalización de acceso a la información, la inclusión digital y el uso intensivo de las TIC contra las desigualdades, forman parte de una malla de iniciativas institucionales estratégicas para un desarrollo sostenible, el combate contra la pobreza, la democratización y la inserción de países semiperiféricos del área latinoamericana en un contexto de globalización. Salvar la brecha entre info-ricos e infopobres es uno de los elementos de cohesión social y estabilidad democrática, y por tanto debe ser un objetivo clave para las administraciones públicas."* (DONAS, 2007, p. 25)

> *"El progresivo desarrollo y abaratamiento de las tecnologías de la información y la comunicación, hacen que su uso se extienda cada vez más y sea más difícil restringir su disfrute a sectores habitualmente desfavorecidos de la sociedad. Quizá la propia esencia del SL no sea por sí sola un elemento de transformación de la sociedad. Sin embargo, la intersección de pericia técnica con una voluntad solidaria de desarrollo y profundización de la democracia, puede convertirse en uno de los elementos defnidores de los nuevos patrones liberación de los pueblos en la sociedad futura."* (DONAS, 2007, p. 18)

Nesse sentido, a solução para os problemas dos países de terceiro mundo seria a inclusão digital, parte esforço da administração pública, parte resultado esperado da perspectiva de barateamento das tecnologias da informação. Inclusão digital por meio da Internet, como entendida por Donas (2007), diz respeito à interação com as administrações públicas, à inserção de coletivos marginais no mercado de trabalho e ao acesso às políticas de educação para formação de uma inteligência coletiva.

A racionalidade por trás do programa OLPC é semelhante. Tendo como porta-voz Nicholas Negroponte – fundador do MIT MediaLab – durante o Fórum Econômico Mundial, o programa foi apresentado como algo imprescindível para o futuro de crianças. A base para o programa, segundo Negroponte, estaria na premissa de que crianças são individualistas e autodidatas e que a existência de fatores externos, como escolas e professores, são prejudiciais ao aprendizado infantil, de forma que garantir o acesso aos computadores portáteis seria a única e certeira solução para a emancipação de crianças em países e regiões mais pobres (CHAN, 2014).

Os preceitos hackers são incorporados na política em relação às formas de criação de conhecimento e aprendizagem. Como aponta Villanueva & Olivera (2012), esperava-se que as crianças, ao utilizar os XO, criassem formas próprias de aprendizado, explorando o equipamento e modificando seus conteúdos fora do ambiente escolar. De acordo com Chan (2014), ao entrevistar um dos engenheiros responsáveis pela implementação do OLPC no Peru:

> "*He recalled how the prospect of globally extending hacker ethics and its values of self-driven learning and problem solving through tinkering especially motivated his dedication to OLPC. Speaking abstractly for hacker collectives, he explained: 'The project gave a lot of visibility to hacker culture, and what we believe is real learning versus what a traditional school defines as learning. We completely reject the notion of memorized knowledge; we completely reject the notion that you go to a school to get filled with knowledge. We do subscribe to the fact that everyone is a learner, and that everyone learns from each other, peer to peer.' Pausing, he specified how OLPC allowed him to identify a language to describe the education-centered philosophy of hackers, adding simply: 'This project embodied all our beliefs. Including beliefs like constructionism [on self-directed learning] that I didn't even know there were words for'.*" (CHAN, 2014, p. 191)

Dessa forma, não só os preceitos hackers da curiosidade e aprendizado pela experimentação foram incorporados pelo OLPC, mas também um certo antiautoritarismo nas salas de aula, ainda que a participação dos professores fosse prevista pelo programa.

Quando os primeiros relatórios de avaliação do programa começaram a surgir com resultados aquém aos esperados tanto em número de computadores portáteis distribuídos quanto em impacto no aprendizado, Negroponte e o ministro da educação peruano culparam questões externas ao programa, como a falta de qualificação e resistência ao uso dos professores e otimismo das crianças em situação de pobreza. Negroponte, em um primeiro momento, teria se recusado a realizar avaliações porque as vantagens da implementação dos programas seriam óbvias.

Chan (2014) conecta esse posicionamento com a pervasividade da ideia de que ciência e tecnologia são efetivas, universais, misteriosas e vêm de fora nas políticas regionais. A denominada "mágica importada" reforçaria as relações de dependência tecnológica entre centro-periferia. O discurso de empoderamento de Negroponte foi facilmente aceito por governos e sociedade civil (VILLANUEVA & OLIVERA, 2012). Ainda que proponham adaptações e apropriações no contexto de países latino-americanos, os posicionamentos de Mendoza (2002) e Donas (2007) também ressoam a ideia de "mágica importada" como forma de organização e trabalho dentro dos projetos de governo aberto ou na expectativa dos resultados da inevitável inclusão digital.

Ainda que ignorados pelos idealizadores e governos implementadores, os relatórios de avaliação do programa OLPC apontaram diversos problemas em todas as fases da política pública. Villanueva & Olivera (2012) e Chan (2014) entrevistaram crianças/professores e engenheiros implementadores, respectivamente. Quanto à formulação do programa, os autores apontaram que um dos principais problemas foi que tanto as premissas quanto os computadores foram desenhados por visionários, sem incorporação de dados ou testes com os usuários (crianças ou professores), de forma que tanto o desenho quanto os programas instalados no computadores, que eram universais e foram utilizados em todos os países que adotaram a política, foram mal recebidos pelos usuários. Quanto à implementação, os problemas foram os mais variados. Além do preço final muito além do anunciado, os recursos e configurações do XO não atenderam ao esperado. Villanueva & Oliveira (2012) apontam que as crianças peruanas já estavam familiarizadas com computadores que utilizavam nos pontos de acesso à Internet nas comunidades e acharam a tecnologia dos computadores do OLPC lenta e inferior aos comunitários. Do lado dos professores as reclamações foram em relação à capacitação, que se focou nos aspectos técnicos do computador e não em formas de integrá-lo nas práticas pedagógicas e no conteúdo programático do sistema educacional.

Chan (2014) aponta que não houve esforço da fundação responsável pelo programa em garantir a colaboração entre os engenheiros e os professores, responsáveis pelas questões técnicas e pedagógicas da implementação, respectivamente. Os problemas de comunicação entre engenheiros e professores giravam em torno dos diferentes interesses e perspectivas de uso do XO no sistema educacional, ou como coloca Chan (2012), da implementação de uma política multidisciplinar em que os formuladores e fiscalizadores não interagiam com os implementadores.

Os lugares em que o programa OLPC obteve os melhores resultados foram aqueles em que houve tradução e localização das tecnologias através das interações entre engenheiros, professores e comunidade, que realizaram conferências para professores rurais e oficinas para tradução dos *softwares* do XO para as línguas indígenas locais, portanto, através da abertura da caixa-preta e do hackeamento do computador portátil.

> "'*Our goal, we realized, was to improve a social problem [rather than a technological one]. Under the direction of just engineers, [we would never] have seen that the problem could be engineers. [Since] engineers always think of themselves as bringing solutions. ... [But] through having multidisciplinary input ... we realized that the problem was with us, in how we thought, and in what we said was the miracle solution and magic wand that would resolve everything. We*

> *realized we were creating more problems than solutions for teachers.' Pausing for a moment, he underscored then how the process of technological translation might in fact operate as much to decenter and reform the technologist' consciousness as to localize technological artifacts, adding: 'But we only achieved this after we sat around the table with everyone together. Only then could we really see what we were all doing ... as engineers, teachers, sociologists, linguists, or ordinary people'*." (CHAN, 2014, p. 195).

4.5 Violência e ilegalidade: hackers, delitos e controvérsias

As publicações desta categoria, de modo geral, restringiram a emergência das políticas hackers a cibercrimes e violência online e os hackers foram tratados como um grupo homogêneo de indivíduos cujo objetivo é cometer delitos informáticos. Dentre todas as categorias, esta foi aquela que apresentou maior homogeneidade entre os objetos, as definições de hacker e as análises.

É interessante que todas as publicações contextualizaram seu objeto de estudo da mesma maneira, partindo da ideia de que a introdução das tecnologias da informação trouxe importantes inovações para o mundo, mas também abriu caminho para novas ameaças.

> *"La variedad, amplitud y complejidad de los sistemas de información que adquieren, requieren o encuentran disponibles las organizaciones actuales, junto a la dinámica del permanente cambio observado en las tecnologías de la información y las comunicaciones, han impulsado de múltiples formas y, al mismo tiempo, condicionado las grandes transformaciones de las organizaciones, los mercados y el mundo de la modernidad y de la posmodernidad. Son cambios que, además de sus innegables ventajas, han traído simultáneamente para las personas y las organizaciones, amenazas, riesgos y espectros de incertidumbre en los escenarios de internet, intranet, desarrollo tecnológico, gestión de la información, la comunicación y los sistemas."* (OJEDA-PÉREZ et al., 2010, pp. 42-43)

> *"En los tiempos que corren, las nuevas tecnologías, en general, y la informática, en particular, introducen incansablemente no sólo nuevas formas de realizar tareas conocidas, sino también nuevas actividades, muchas de las cuales se manifiestan como antisociales y reprobables, en razón de interferir en la pacífica convivencia de los ciudadanos."* (AROCENA, 2012, p. 946)

Como hacking é entendido como crime informático, o comportamento malicioso dos hackers seria consequência, ao mesmo tempo que ampliado, pela mediação das tecnologias da informação. Os autores, porém, apresentam uma visão bastante neutra em relação às tecnologias da informação, fazendo transparecer que são inerentemente benéficas, exceto quando atores mal-intencionados as utilizam para fins não previstos. O hackerismo seria, nesse sentido, um desvio.

Algumas outras questões são interessantes. Em nenhuma das publicações houve qualquer discussão sobre tecnologias proprietárias e livres. As tecnologias livres normalmente

são vinculadas com formas de proteção contra o rastreamento e coleta, obtenção e comercialização de dados pessoais porque garantem maior controle ao usuário, mas normalmente a partir da perspectiva de que a privacidade é uma forma de defesa contra formas de violência, controle e vigilância do Estado e grandes corporações. No caso das publicações desta categoria, ficou evidente que a violência e as ações maliciosas têm um sentido único – dos hackers e criminosos para o Estado, corporações, instituições e indivíduos. Portanto, a coleta, comercialização e uso de dados não é vista como problemática e o uso de tecnologias proprietárias não é questionado. Ao contrário, devido às dificuldades na apuração e responsabilização dos delitos informáticos, alguns autores entendem a coleta e armazenamento de dados como uma questão de segurança, mesmo que coloque em risco as liberdades individuais.

> "Essa disposição de não permitir que uma única entidade guarde todo o registro de navegação do usuário, na verdade, dificulta a investigação criminal, pois, ao mesmo tempo que representa um avanço na proteção das garantias individuais, representa também uma dificuldade adicional para o processo investigativo." (CERQUEIRA & ROCHA, 2013, p. 136)

Outro elemento em comum nas publicações foi a perspectiva de que o aparecimento de inovações em crimes cibernéticos é mais rápido que a capacidade da legislação de se adequar a eles. Nesse sentido, emergem uma série de desafios, políticas e conflitos do fato de que as mudanças nas leis sobre Internet e direito autoral, assim como no código penal, vêm a posteriori dos delitos informáticos, o que causaria a sensação de impotência às forças policiais e de impunidade aos hackers. Alguns outros elementos que dificultariam a apuração e penalização por crimes informáticos seriam seu caráter transnacional, a dificuldade na obtenção de dados por agências e organizações internacionais e os marcos de proteção à liberdade na Internet e privacidade.

O caráter transnacional dos delitos informáticos também exigiria que os países adequassem suas legislações e absorvessem medidas propostas por acordos internacionais, como a Convenção de Budapeste, legislação europeia criada em 2001 em resposta aos ataques do onze de setembro (AROCENA, 2012; CERQUEIRA & ROCHA, 2013; HERNÁNDEZ, BAQUERO & GIL, 2018). Porém, apesar do esforço, os países ainda teriam muita dificuldade em tipificar o crime cibernético. Um dos únicos consensos entre diferentes legislações seria a relação entre os delitos e os sistemas informáticos.

> *"el concepto de ciberdelito se construye en derredor de la noción de 'sistema informático', pues, como se acaba de ver, es éste el que, en la clase de infracciones que analizamos, se constituye en el instrumento del delito o su objeto de ataque, o sea, el medio a través del cual el ilícito se comete, o en el objeto material sobre el cual recae la conducta típica."* (AROCENA, 2012, p. 950)

Ainda assim, o que é considerado delito informático aparenta variar em cada país em termos de ação. Entrariam aqui invasão, roubo, vazamento (OJEDA-PÉREZ et al., 2010; AROCENA, 2012; CERQUEIRA & ROCHA, 2013; RODRÍGUEZ, ODUBER & MORA, 2017; HERNÁNDEZ, BAQUERO & GIL, 2018) e calúnia, difamação e manifestações hacktivistas (RUIZ, SEGURA & QUESADA, 2009).

Nessa direção, Gacharná G. (2009), Ojeda-Pérez et al. (2010), Arocena (2012) e Cerqueira & Rocha (2013) levantam a questão que a dificuldade em tipificar os delitos informáticos e, muitas vezes, as formas com que as legislações os absorvem transformam em crime o hacking ético. De acordo com Gacharná G. (2009):

> *"Hacking ético, es una actividad que incluye diversos ataques a redes de computadores en ambientes controlados donde los responsables de los sistemas a atacar han sido previamente informados y han autorizado los mismos con el fin de establecer el estado de inseguridad de su sistema y conocer detalladamente sus vulnerabilidades y que son practicados por profesionales en Seguridad Informática."* (GACHARNÁ G., 2009, p. 47)

O hacking ético, na percepção de Gacharná G. (2009) e dos outros autores, seria uma função dentro das empresas de segurança da informação necessária para a evolução dos sistemas de segurança. Porém, as atividades desenvolvidas por hackers éticos se enquadrariam em delitos informáticos. Surgem, então, questões sobre consentimento ou não do sistema, corporação ou instituição invadidos.

4.6 Considerações sobre as políticas hackers e as disputas pelo ordenamento do mundo

No início da trajetória de pesquisa, como mencionado na introdução, a percepção prevalecente era a dos hackers como representantes de um movimento de não-aceitação da condição de caixa-preta das tecnologias da informação, envolto em subversão, liberdade, autonomia e circunvenção das imposições do Estado e das grandes corporações sobre como as tecnologias deveriam funcionar e o que deveria ser feito com seus dados. Essa percepção foi construída, principalmente, a partir de leituras sobre *hacklabs* e *hackerspaces*, espaços de socialização hacker em que indivíduos de diferentes interesses e motivações se encontram para compartilhar conhecimentos, ferramentas e recursos e onde as tecnologias são

apropriadas e transformadas. Essa percepção carrega consigo uma definição de hackerismo como algo inerentemente politizado.

O contato com a literatura do primeiro e segundo momento dos estudos hackers colocou essa percepção em perspectiva, uma vez que tanto os autores quando os indivíduos, grupos e comunidades hackers entrevistados e analisados pelos autores buscaram afirmar a não-politização como característica ou a politização como algo secundário à busca por melhores soluções técnicas, caracterizando, assim, o *ethos* tecnomeritocrático dos hackers. Nessa lógica, o engajamento político aconteceria apenas sob circunstâncias relacionadas à percepção dos hackers de que suas liberdades em criar, distribuir e transformar tecnologias – portanto sua existência como público – estivessem em risco.

Considerando as políticas hackers identificadas no conjunto de publicações selecionadas, a primeira percepção desta pesquisa sobre os hackers não pareceu tão distante da realidade latino-americana. O foco desta definição, porém, estava nos artefatos: as resistências e subversões estavam relacionadas aos novos usos e funções dados às tecnologias já existentes, possibilitados pela liberdade individual em criar, distribuir e transformar tecnologias. Isso fez com que esta percepção se assemelhasse às formas mais liberais e libertárias das políticas hackers, como as de Levy (1984), Raymond (1996 revisão 1.51 out. 2017) e dos gêneros hackers apresentados por Coleman & Golub (2008). Nesse sentido, o "que" era mais importante que o "quem", que se conformava quase como algo exógeno às tecnologias em questão. Essa percepção pode parecer contraditória ao pressuposto da não-neutralidade das tecnologias, mas em realidade depositava os elementos políticos completamente nos artefatos ao deixar sua rede sociotécnica em segundo plano na análise. O problema, portanto, estava em não situar as manifestações hackers geográfica e historicamente.

A importância do "quem" surgiu ao explorar o conhecimento gerado sobre hackers na América Latina e entrar em contato com manifestações hackers na CryptoRave. De forma geral, as tecnologias criadas, distribuídas e transformadas por hackers estadunidenses, europeus e latino-americanos parecem semelhantes – tecnologias livres em forma de sistemas operacionais, infraestruturas de rede, ferramentas de comunicação, criptografia e segurança da informação, navegadores, *software* de processamento de textos e imagens, entre outros. Mesmo assim, as políticas identificadas entre diferentes manifestações (mesmo dentro da CryptoRave) eram múltiplas, o que colocou em perspectiva, novamente, a percepção sobre hackers.

Por esse motivo, um dos primeiros questionamentos foi a força do estereótipo do hacker – homem jovem, branco, apolítico e libertário, com ensino superior em áreas tecnológicas e de classe média que utiliza o hackerismo como forma de diversão e satisfação pessoal – na literatura sobre hackers e na definição do que são e de onde emergem as políticas hackers. As diferenças notadas entre indivíduos, grupos e comunidades abordados pela literatura que trata de resistências e subversões – como Coleman (2017), Maxigas (2012; 2017) e Söderberg (2013) – repousavam no posicionamento político identificado (liberais ou radicais) e não nas características da populações. As manifestações hackers na América Latina confrontam justamente esse estereótipo e identificar "quem" se torna essencial para entender quais são suas características, como emergem e por que são diferentes daquelas estadunidenses e europeias.

A questão do "quem" perpassa o fato de que tecnologias são mais do que as funções para as quais foram designadas e seus significados dependem dos interesses e visões de mundo daqueles que as criam, distribuem e transformam (FEENBERG, 2016). Quando quem reordena as tecnologias da informação são povos tradicionais, mulheres, pessoas transgênero e outras populações normalmente excluídas dos processos decisórios e do desenvolvimento das tecnologias – ao contrário da população que conforma o estereótipo hacker – resistência e subversão não emergem apenas em relação aos usos e funções das tecnologias, mas em resposta ao lugar que essas populações ocupam.

O passado colonial, as ditaduras violentas, as reformas neoliberais, a modernização excludente, a situação periférica, a ausência de políticas afirmativas, as ameaças à autonomia e à integridade física e moral são constantemente trazidos como motivos para indivíduos, grupos e comunidades na América Latina se engajarem em hackerismos. Ativismo e militância dos hackers e por tecnologias livres não buscam apenas garantir o direito e a liberdade em criar, distribuir, transformar e acessar tecnologias do ponto de vista do indivíduo e lutar contra o enrijecimento das leis de propriedade intelectual que se tornam barreiras a essas liberdades. Isso porque os hackerismos na América Latina já nascem politizados e atrelados aos interesses e visões de mundo de populações que conformam minorias políticas que são exploradas e violadas em seus direitos de existir. Mesmos nos casos em que o foco são comunidades de desenvolvedores, as tecnologias livres e o engajamento em hackerismos são identificados como forma de alcançar autonomia e reduzir a dependência tecnológica de grandes corporações.

Essa característica dos hackerismos na América Latina foi um dos principais achados de pesquisa e está relacionado ao fato de que o público recursivo desses hackers

também foi construído em torno de outros fatores, como pertencimento a povos tradicionais, ser mulher, ser latino-americano ou viver em um país em desenvolvimento. Ser e fazer hacker incluem outras questões do estar, agir e ser no mundo próprias desses atores.

Considerando as políticas hackers como formas de disputar o ordenamento do mundo através do reordenamento das tecnologias da informação, é possível afirmar que o elemento comum que perpassa todas as diferentes políticas hackers na América Latina é a ***construção de alternativas*** tecnopolíticas – relacionadas à governança das tecnologias da informação – e sociotécnicas – porque são formas de disputar a construção de futuros.

Ativismo, militância, forma de organização, trabalho e ética hackers, para o conjunto de publicações selecionadas, foram identificados como alternativas à exclusão (do mercado de trabalho, do sistema educacional, dos benefícios da utilização de tecnologias da informação), à dependência tecnologia (dos indivíduos e nações frente às grandes corporações), ao subdesenvolvimento (organização do trabalho em outra lógica que não a capitalista, como forma de racionalidade de política pública), à vigilância estatal e à violência (por parte do Estado, colegas, companheiros, empregadores etc.). Essas manifestações hackers parecem não buscar tomar o poder do Estado, mas transformar e balancear os arranjos de poder e autoridade nas relações entre Estado-grandes corporações-indivíduos.

Dentre a amostra de manifestações hackers, foi possível identificar a prevalência de três caminhos de construção de alternativas, em outras palavras, de formas com que os hackers de computador na América Latina reordenam tecnologias da informação e disputam a construção de futuros.

O primeiro deles são a organização e a articulação de movimentos em rede, com o objetivo de agregar aqueles que compartilham de uma mesma visão de mundo. As redes são utilizadas tanto para coordenação de atividades quanto para colaboração e compartilhamento de tecnologias e conhecimentos seja fora da lógica capitalista, seja com o objetivo de exercer a liberdade de expressão e ação, seja longe da vigilância estatal. Esse caminho, em particular, foi apontado como a contribuição da América Latina para a cibercultura: a utilização das tecnologias da informação para formação de redes de solidariedade e organização do ativismo na Internet (PITMAN, 2007).

O segundo é a ocupação de espaços existentes ou criação de outros exclusivos. Aqui estão incluídos não só os espaços virtuais e físicos de socialização hacker, mas também o lugar que esses hackers lutam para ocupar na sociedade e na construção de futuros: i) comunidades de desenvolvedores, fóruns e eventos de *software* livre, assim como *hackerspaces* e comunidades de *software* livre feministas que surgem em resposta aos

conflitos internos nos primeiros; ii) intersecções com instâncias de governo com o objetivo de influir na formulação de políticas públicas e trazer os preceitos das tecnologias livres como caminho para inclusão e autonomia (dos indivíduos ou nações) e; iii) infraestruturas de rede alternativas – fora do alcance do Estado e grandes corporações – que se conformam como espaços seguros para a organização e articulação de dissidências e resistências.

O terceiro caminho é tomar para si a construção, organização e gestão das tecnologias que garantem sua associação e existência como movimentos de resistência e subversão. Não só em relação às ferramentas de privacidade e segurança na Internet, há também uma crescente preocupação em criar redes autônomas alternativas organizadas e geridas coletivamente por cooperativas, coletivos e organizações não governamentais de defesa às tecnologias livres para garantir infraestrutura para movimentos sociais e coletivos de feministas, jornalistas, artistas e outras organizações sociais. Essas infraestruturas de rede alternativas e tecnologias livres são vistas como espaços seguros e democráticos onde movimentos poder ser articulados livremente, sem o risco de serem reprimidos antes mesmo de organizados (em contraponto às infraestruturas privatizadas e tecnologias proprietárias, que permitem diversas formas de cibervigilância). A governança das tecnologias da informação se configurou como tema central tanto nos estudos de caso sobre hacker de computador na América Latina tanto nas discussões da CryptoRave.

Como o público recursivo dos hackers da América Latina também é construído em torno de fatores relacionados às especificidades das populações que se engajam em hackerismos, as limitações de suas políticas hackers atravessam os perigos aos quais essas populações estão expostos e que colocam em risco sua existência não só como hackers, mas como grupos, comunidades, movimentos e indivíduos – recuperando aqui a ideia de matriz de dominação discutida por Sasha Costanza-Chock na edição de 2017 da CryptoRave. O recrudescimento da violência física, repressão por força policial, censura, deslegitimação, invisibilização e silenciamento são alguns exemplos de potenciais barreiras aos discursos e práticas desses hackers. O fortalecimento das leis de proteção intelectual, a tomada de controle e comercialização de todos os aspectos da gestão e manutenção das tecnologias da informação e estruturas de redes também se configuram como possíveis limitantes às políticas hackers porque criam barreiras à autonomia e à liberdade de associação e podem se configurar como censura e repressão.

A cooptação pelas forças do capitalismo – considerada a principal fonte de limitações às políticas hackers pelos autores consultados dos estudos hackers (COLEMAN, 2017; DELFANTI & SÖDERBERG, 2018; GRENZFURTHNER & SCHNEIDER, 2009;

MAXIGAS, 2012; 2017) também foi notada em manifestações hackers na América Latina, mas principalmente naquelas em que prevalecem homens brancos, jovens e com formação em áreas de tecnologia da informação, que junto das empresas capitalistas que buscam recrutá-los, começaram a ganhar mais espaço em eventos de *software* livre como o FISL. Se Delfanti & Söderberg (2018) reconhecem a existência de ciclos de politização e despolitização dos hackers, no caso do movimento percebido por Evangelista (2014) no FISL o que também está em jogo são as percepções sobre dependência tecnológica, condição subalterna e soberania nacional frente às grandes corporações e nações desenvolvidas. *Software* livre na América Latina, como aponta Zanotti (2014), sempre foi objeto político, de modo que o movimento político sempre maior que o técnico – percepção que faz oposição direta à ideia de agnosticismo político de Coleman (2004). Sob o capitalismo de vigilância, em que a lógica de acumulação das grandes corporações passa pela coleta e comercialização de dados dos usuários, as relações entre tecnologias livres, autonomia e soberania nacional ficam mais evidentes. A escolha em utilizar tecnologias livres traz à tona a relação entre Estado-grandes corporações-indivíduos porque coloca em disputa o poder e controle das informações.

Por fim, as políticas hackers também se manifestaram na relevância dos zapatistas para o imaginário do que é ser hacker na América Latina e do ser e fazer hacker para o imaginário do que é engajamento político na América Latina no contexto do capitalismo informacional/de vigilância. O levante zapatista – a construção e organização, o caráter de resistência e de movimento antiglobalização, as demandas e os desdobramentos – impactaram em como hackers são retratados na literatura *cyberpunk* latino-americana e em como táticas e elementos hackers são apropriados e utilizados nas artes visuais, poesia e música para subverter gêneros e mostrar dissidência em relação ao mesmo contexto contra o qual os hackers de computador na América Latina construíram e constroem suas resistências.

CONCLUSÃO – Hackers, políticas, América Latina e a literatura dos estudos hackers

O objetivo geral desta pesquisa foi identificar como os estudos de caso sobre hackers de computador na América Latina contribuem com o conhecimento sobre políticas hackers e, desta forma, com o campo dos estudos hackers como um todo. Para cumprir esse objetivo, a escolha metodológica foi pela Revisão Sistemática de Bibliografia (RSB), que propõem passos para mapear, sistematizar e discutir o corpo de conhecimento existente sobre um objeto ou tema específico.

A partir da definição de palavras-chaves e critérios de inclusão, foram selecionadas setenta publicações para sistematização e análise. Este estudo exploratório sobre as políticas hackers foi construído a partir desse conjunto específico de publicações, que se configura como uma amostra do total de publicações sobre hackers e temáticas semelhantes. Portanto, esta pesquisa não se propôs a exaurir o tema – ou considerar que as conclusões extraída deste conjunto representam a totalidade das análises –, mas sim identificar algumas questões-chave das políticas hackers na América Latina.

A sistematização proposta pela RSB também dá recursos para identificar como os autores que pesquisam e escrevem sobre hackers da América Latina estão olhando para essa temática. Nesse sentido, a maior parte das publicações têm caráter exploratório e utilizou de dados obtidos de notícias, relatórios, wikis, manifestos, artes e outros materiais disponíveis na Internet na construção dos estudos de caso, uma vez que, sendo um dos espaços de socialização hacker e parte essencial do seu público recursivo, a Internet torna-se um lócus de informação. Ademais, foi possível identificar que muitos autores utilizaram também literatura existente sobre hacker ou sobre outros objetos, mas com nova compreensão a partir da perspectiva de grupos, espaços, atividades, práticas ou eventos ligados aos hackers.

O caráter exploratório teve um impacto importante nas publicações: os casos apresentados e as análises voltaram-se mais para identificação de dinâmicas, descrição de atividades, apontamento de tendências e possíveis direcionamentos e menos para a construção de teorias mais gerais sobre hackers e hackerismos a partir dos casos. A percepção é, portanto, que hackers, hackerismos e aspectos relacionados ainda estão em fase de descobrimento, exploração e desenvolvimento no âmbito da pesquisa acadêmica. Essa parece ser uma primeira divergência em relação à literatura dos estudos hackers consultada para o estudo de escopo, que também parte de casos, mas como forma de se direcionar para teoria. Porém, dois comentários são necessários nesse sentido. Primeiro, o conjunto de publicações obre a América Latina é maior do que o consultado para o estudo de escopo. Segundo, exceto por

alguns casos, não foi possível verificar se os estudos de caso são pontuais ou parte de uma trajetória de pesquisa, de modo que as análises tenham sido continuadas e aprofundadas.

A identificação do que os autores entendem por hacker e hackear foi um dos primeiros passos tomados para analisar o conhecimento criado sobre os hackers de computador na América Latina. Assim como na literatura dos estudos hackers consultada, as definições foram múltiplas e variadas. A maior parte dos autores definiram hackers a partir de sua relação com ferramentas e tecnologias da informação e em relação às práticas que são características do trabalho hacker. Considerando o conjunto de publicações, foi notado um equilíbrio entre a utilização de definições já existentes na literatura e definições propostas a partir dos casos estudados.

Mais interessante, foi possível observar que mesmo definições construídas a partir dos casos, muitas vezes, continham elementos daquelas desenvolvidas por autores dos estudos hackers. Foi possível identificar dois padrões nesse sentido. Primeiro, os autores que definiram hackers e hackerismos a partir das características do trabalho hacker e do entusiasmo com tecnologias da informação apresentaram conceitos semelhantes àqueles de Eric Raymond, Pekka Himanen e Manuel Castells. Segundo, os autores que definiram hackers a partir da relação com ferramentas e tecnologias da informação e das características atribuídas ao ser hacker apresentaram conceitos semelhantes aos preceitos da ética hacker observada por Steven Levy. Enquanto as definições de Raymond, Himanen e Castells englobam questões mais específicas do trabalho dos hackers de *software* dos anos 1980 e 1990 envolvidos com as comunidades de *software* livre e código-aberto, os preceitos descritos por Levy são mais abrangentes e possibilitam pensar em diferentes hackerismos como formas de ser e existir no mundo.

Adentrando propriamente nas políticas hackers, foi possível verificar nos estudos sobre a América Latina a presença das três subjetividades políticas propostas por Coleman (2017), a saber, valorização do artifício, coletivismo e comportamento extremamente social e tendência ao antiautoritarismo. Em algumas categorias de análise criadas para as políticas hackers, as formas tomadas por cada uma destas sensibilidades apresentou diferenças e, em muitos casos, suas especificidades foram utilizadas para definir hackers e descrever suas práticas. O quarto capítulo provou-se repleto de exemplos. A valorização do artifício pôde ser encontrada entre as práticas internas das comunidades de *software* livre em busca de soluções astutas para problemas técnicos, nas táticas de hacktivismo apropriadas por movimentos sociais, nas estéticas da *netart* e poesia em código e nos hackatons como formas de encontrar soluções para problemas sociais. O coletivismo e comportamento extremamente social foi

entendido como algo inerente a todas experiências hackers e, muitas vezes, foram apontados como um dos principais elementos característicos dos hackers que deveriam ser apropriados para outras situações através da ideia de formação de redes de colaboração. O cultivo histórico ao antiautoritarismo foi a sensibilidade que apresentou mais variações em decorrência das diferentes formas em que grupos, comunidades, eventos e fenômenos hackers pelos autores interagem com seus contextos.

Os exemplos e descrições de Coleman (2017) em seu argumento sobre o antiautoritarismo como parte da subjetividade hacker trazem consigo a importância do contexto como motivação para o engajamento político. Nesse sentido, quando Coleman (2017) trata dos hackers norte-americanos e Maxigas (2012) dos espaços hackers europeus, há um consenso de que as sensibilidades políticas, entre os hackers, costumam espelhar padrões políticos regionais ou dominantes, ainda que as estratégias e táticas hackers possam ser comuns. Coleman (2017) reafirma este argumento ao ressaltar que a passagem massiva dos hackers para a arena política nos últimos anos foi consequência dos atos de denúncia de Snowden, que se tornaram um chamado para hackers e outros entusiastas da tecnologia se engajarem na agenda política da privacidade através do esforço conjunto em desenvolver ferramentas de criptografia. Portanto, é coerente analisar o antiautoritarismo em relação às políticas liberais e radicais.

Em termos de políticas liberais, descritas por Coleman (2017) como aquelas em que as liberdades civis são vistas como condição essencial dos direitos individuais – de expressão, autonomia, acesso e participação política –, foram encontradas semelhanças entre os estudos de caso sobre a América Latina e os exemplos apresentados pelos autores consultados para o estudo de escopo. As políticas hackers em questão foram aquelas que emergem das práticas, atividades cotidianas, regras internas e relações dentro das comunidades de *software* livre e código aberto (políticas do dia-a-dia), do trabalho hacker como característica da sociedade em rede (políticas do dia-a-dia), da absorção de metodologias hackers para outros meios (transposição do ser hacker para outros meios) e das interações entre hackers e outras organizações e instituições por meio das propostas de governo aberto e hacking cívico (outras formas de fazer política pública, influenciar tomada de decisões ou se expressar politicamente).

Para esses casos, as racionalidades evidenciadas pelos autores foram semelhantes àquelas das políticas liberais apontadas por Coleman & Golub (2008) e Coleman (2017), principalmente quanto às relações entre indivíduos, comunidades e tecnologias livres. Como exemplo, Evangelista (2014) evidenciou que a mesma disputa entre os grupos de *software*

livre e código aberto descrita por Raymond (1996, revisão 1.51 out. 2017), Coleman & Golub (2008) e Söderberg (2013) pôde ser verificada, ao longo dos anos, no movimento de *software* livre no Brasil, utilizando como exemplo as dinâmicas observadas do FISL. A existência dessas disputas também foram observadas em outros casos, como o argentino (ZANOTTI, 2011; 2014) e o costarriquenho (SOLÓRZANO, 2009).

As políticas liberais estão conectadas com uma série de manifestações hackers entorno da liberdade individual de criar, usar e distribuir *software* e outras tecnologias livres, com intersecções com liberdade de expressão, meritocracia e autonomia. Tanto na literatura dos estudos hackers quanto nos estudos sobre a América Latina, o antiautoritarismo pareceu se manifestar contra tudo aquilo – regras tácitas, lógicas de trabalho, imposições, leis de direitos autorais – que coloca em risco essas liberdades individuais.

São nas políticas radicais, que para Coleman (2017) emergem quando a defesa das liberdades civis se torna porta de entrada para projetos mais robustos voltados à luta por igualdade e justiça, que começam a despontar as especificidades das políticas hackers na América Latina[56]. Uma primeira evidência é a proporção de publicações que trataram de intersecções entre hackers/movimentos sociais e hackers/gênero, refletida nas discussões assistidas na CryptoRave, para a qual não foi encontrada correspondência na literatura consultada para o estudo de escopo ou na Escola Doutoral de Estudos Digitais.

Em relação às intersecções entre hackers e movimentos sociais, os estudos de caso sobre a América Latina ajudaram a firmar uma genealogia hacker latino-americana e estabelecer sua importância em relação à cibercultura e aos movimentos hacktivistas como um todo. Ainda que haja controvérsias sobre a denominação dos zapatistas como o primeiro movimento de guerrilha informacional, apresentadas por Pitman (2007) em resposta a Cleaver (1998), o impacto do movimento zapatista no imaginário sobre hackerismo na América Latina, assim como nas lutas por direitos dos povos tradicionais e indígenas, é inegável. A maioria das publicações que trataram de hacktivismo mencionaram o movimento zapatista como originário e muitos citaram Cleaver (1998) e seu conceito de *electronic fabric of struggle*. Como consequência, a ideia de que o hackerismo nasce na América Latina já politizado e conectado com as demandas e necessidades de movimentos sociais de defesa de direitos de povos tradicionais e indígenas é bastante forte entre as publicações do conjunto selecionado. Além disso, as táticas utilizadas durante o levante zapatista – aquelas de

[56] De acordo com Coleman (2017), os Anonymous se conformam como parte das políticas radicais pela proximidade de suas táticas às de desobediência civil eletrônica. No caso da América Latina, as políticas dos Anonymous descritas por Machado (2015) são semelhantes àquelas do movimento internacional, então não foram consideradas como especificidades latino-americanas.

desobediência civil eletrônica, contrainformação, organização em redes de colaboração e solidariedade etc. – passam a ser sinônimos de práticas hackers na América Latina.

Em contrapartida, a afirmação de Pitman (2007) de que a força do movimento zapatista parece ter eclipsado exemplos anteriores de redes ativistas que utilizaram de táticas semelhantes na América Latina, como os maias hackers, foi verificada para o conjunto de publicações analisadas. Exceto pelo artigo original de Nelson (1996) e algumas citações nos textos sobre transposição do ser hacker para a literatura, nenhum outro exemplo foi citado.

As intersecções entre hackers e gênero, em particular, foram a primeira especificidade dos estudos sobre hackers na América Latina encontrada logo no início da trajetória de pesquisa. Um dos meus primeiros contatos com hackers e hackerismos foi a partir das discussões sobre gênero e tecnologia através de uma colega de pós-graduação e logo na Escola Doutoral pude perceber que existiam poucas discussões a respeito.

As publicações do conjunto analisado que trataram sobre gênero e hackerismos foram todas escritas por mulheres, sendo que algumas delas escreveram mais de uma publicação no conjunto, o que poderia indicar que a exploração dessa temática por essas autoras não é pontual, mas contínua. Mais interessante, as intersecções entre hackers e gênero foram exploradas de diferentes perspectivas: desigualdades de gênero no ambiente de trabalho, invisibilização do trabalho feminino em áreas de tecnologia da informação e comunicação, violência de gênero, iniciativas de coletivos feministas, entre outros. Também é bastante interessante que a ocupação e apropriação de espaços tipicamente masculinos e a criação de outros exclusivos para mulheres – assim como a criação de suas próprias tecnologias e infraestruturas – foram as estratégias comuns apontadas pelas autoras, identificadas nos diferentes casos estudados e consideradas táticas de políticas hackers.

O antiautoritarismo, nestes casos, vem em resposta a um contexto específico e parece ser reflexo da violência física e moral, da negação dos direitos humanos e de subordinações e desigualdades perpetradas ou permitidas pelo Estado e pelas grandes corporações. Entre esses estudos e a CryptoRave, ficou evidente a percepção de uma disparidade de poder entre indivíduos/movimentos sociais e Estado/grandes corporações. A livre expressão, livre circulação de informação e a organização política poderiam ser facilmente bloqueadas no contexto do capitalismo informacional/de vigilância em que a conectividade é controlada por grandes corporações e as informações são centralizadas pelo Estado. Nesse sentido, foi bastante comum nos estudos sobre a América Latina encontrar a reflexão de que as tecnologias da informação utilizadas como ferramenta de controle, vigilância, repressão são as mesmas utilizadas para resistência e subversão e, por isso, hackers

se tornaram importantes atores políticos, uma vez que reordenam as tecnologias da informação, muitas vezes sem consentimento dos grandes poderes. Essas reflexões teriam implicações para o conceito de liberdade na América Latina, que parece assumir outros significados para esses autores: os de proteção, cuidado, inclusão e direito de existir.

As análises realizadas sobre o contexto latino-americano apontaram outra especificidade: a ideia de sociedade de controle, no caso latino-americano, remete a memórias de contextos específicos: o passado colonial, os regimes ditatoriais violentos, as reformas neoliberais de privatização, desregulação e abertura e a modernização excludente.

Neste ponto, é possível retomar o conceito de agnosticismo político de Coleman (2004), que contempla a indiferença dos hackers em relação às diferenças ideológicas quando estas podem se tornar um obstáculo ao processo de encontrar a melhor solução para um problema. Na maioria dos casos estudados o agnosticismo político não foi verificado, uma vez que os posicionamentos políticos foram ressaltados como parte essencial das motivações para organização de comunidades e engajamento em hackerismos. Essa especificidade foi encontrada quando o público recursivo foi construído também em torno de outros fatores, como pertencimento a povos tradicionais e indígenas, ser mulher, ser latino-americano ou viver em um país em desenvolvimento. Ser e fazer hacker, então, acabam incluindo outras questões do estar, agir e ser no mundo próprio desses atores e as políticas hackers, nesses casos, tomam forma de resistência contra apropriação por culturas dominantes e invisibilização, cuidados digitais e proteção contra violências no contexto do capitalismo informacional/de vigilância e luta por autonomia e pela possibilidade de construir tecnologias próprias.

Coleman (2004) parte seu conceito de agnosticismo político de observações nas comunidades estadunidenses de *software* livre e código aberto. No caso dos estudos latino-americanos, não foi possível observá-lo nem mesmo dentro dessas comunidades (EVANGELISTA, 2014; ZANOTTI, 2014). Questões como apropriação e desenvolvimento de *softwares* livres surgem como estratégias para lutas sociais, subdesenvolvimento, industrialização parcial, domínio econômico de grandes empresas de informática e independência tecnológica nacional. Mesmo nos meios não tipicamente vinculados aos hackers – especificamente arte, música e literatura – a apropriação e absorção de elementos característicos do ser e fazer hacker não foram acidentais, mas com o objetivo manifestar-se politicamente.

Outra questão foi o determinismo tecnológico, ou seja, a lógica de que tecnologias se desenvolvem a partir de lógicas próprias exógenas à sociedade e a moldam em seus

padrões quando introduzidas – de forma que, para hackers, mudanças sociais dependeriam do desenvolvimento tecnológico. A literatura consultada para o estudo de escopo faz duas críticas aos acadêmicos dos estudos hackers relacionadas ao determinismo tecnológico. Primeiro, àqueles que entendem que a tecnofilia minaria o potencial emancipatório e o engajamento político dos hackers (SÖDERBERG, 2013). Segundo, àqueles que não exploram hackerismos além do potencial emancipatório (DELFANTI & SÖDERBERG, 2018).

No caso das publicações selecionadas, lógicas tecnologicamente deterministas foram identificadas pelos autores dos estudos, mas não como obstáculo ao engajamento político. Pelo contrário, o potencial emancipatório das práticas e ética hackers – por sua relação com tecnologias da informação – foi muitas vezes utilizado como justificativa para a realização da pesquisa. A prevalência desta perspectiva nas publicações parece estar conectada com a percepção dos autores sobre tecnologias da informação – hackers são vistos como expressão recente e bem-sucedida das possibilidades de transformação que a introdução e expansão das tecnologias da informação trariam nas sociedades contemporâneas.

A percepção dos autores não parece ser a de "mágica importada", como analisa Chan (2014) sobre a perspectiva dos governos nacionais sobre o programa OLPC, em que tecnologias são efetivas, universais e sempre vêm de fora. Isso porque foi bastante comum encontrar nas publicações a percepção de que as tecnologias não são neutras e precisam ser apropriadas, adaptadas ou recriadas para os contextos de interesse, ações essas características das práticas hackers[57]. O reforço da promessa emancipatória, portanto, parece ter origem na percepção de que as tecnologias da informação ainda não foram completamente exploradas na América Latina em comparação com outros países desenvolvidos. A questão da falta de acesso ou falta de conhecimento apareceu inúmeras vezes como barreira ao potencial dos hackers e hackerismos, principalmente nas publicações mais acríticas em relação aos desdobramentos dos usos dessas tecnologias. Ao mesmo tempo, pairou sobre essas publicações a ideia da inclusão digital como solução para os problemas de países em desenvolvimento. Nesse sentido, o autodidatismo, aprendizado por experimentação e exploração das tecnologias e formação de redes de colaboração associados aos hackers foram vistos como racionalidades a ser incorporadas para esse fim, seja pela administração pública por meio de políticas públicas de inclusão, seja pelos grupos e comunidades buscando transpor essa barreira.

[57] Particularmente, a questão da apropriação e adaptação de tecnologias faz parte de uma tradição do pensar ciência e tecnologia na América Latina que vem desde as análises sobre industrialização tardia e relações centro-periferia, até uma série de autores que tratam especificamente de políticas científicas e tecnológicas desde os anos 1960, como Amílcar Herrera e Oscar Varsavsky.

As exceções às análises tecnologicamente deterministas e com foco no potencial emancipatório do hackerismo foram os estudos realizados a partir das perspectivas de Estudos Sociais da Ciência e da Tecnologia, das Teorias Feministas e das Teorias dos Movimentos Sociais, cujo corpo de conhecimento compreende uma série de reflexões – e aparatos teórico-analíticos – sobre as mais diferentes relações entre tecnologias e sociedade. É particularmente interessante que essas publicações também foram aquelas que construíram a análise de forma interdisciplinar em torno de diferentes aspectos de seus objetos de estudo, inclusive em relação às políticas que emergiam dos casos estudados.

Não foi possível identificar para o conjunto de publicações discussões sobre os aspectos luditas do hackerismo, que segundo Maxigas (2017) se configura como práticas de resistência tecnológica dos hackers que emergem de escolhas de adoção ou não-adoção de acordo com as preferências tecnológicas de usuários sofisticados. As discussões de adoção e não-adoção foram manifestas na maioria das publicações, mas implícitas nas menções constantes sobre a importância das tecnologias livres, normalmente vinculadas com formas de proteção contra o rastreamento e coleta, obtenção e comercialização de dados pessoais, uma vez que garantiriam maior controle ao usuário e, também, porque permitiriam que outros as copiassem, redistribuíssem, utilizassem e modificassem livremente.

Uma ampliação da perspectiva dos aspectos luditas do hackerismo para além do recorte populacional que Maxigas (2017) considera "usuários sofisticados" e do conceito de resistência tecnológica para incluir outras formas de agência em relação às tecnologias que não apenas a adoção ou não-adoção permitiria incluir aqueles grupos que criam tecnologias da informação e infraestruturas alternativas, como os movimentos sociais e os coletivos feministas. Nestes casos, a escolha por tecnologias livres e/ou seguras são resultado de decisões e disputas políticas dentro dos grupos e acontecem em relação ao contexto de controle e vigilância. Esses grupos compartilham valores, possuem expertise técnica e consciência coletiva em relação a sua história, quando não também em relação à cultura hacker. Ainda que suas resistências não sejam especificamente contra a cooptação da Internet, como sugere Maxigas (2017), ainda assim fazem parte do contexto em resposta ao qual as constroem. Nesses casos, as resistências tecnológicas se assemelham àquelas discutidas por Pfaffenberg (1992), pois se configuram como enfrentamento às formas de controle, ordenamento e exclusão relacionado ao processo de desenho e desenvolvimento das tecnologias.

Como apontado no quarto capítulo, a construção do público recursivo dos hackers inclui fatores próprios do pertencimento a povos tradicionais, ser mulher, ser latino-americano

e viver em um país em desenvolvimento, de forma que barreiras ou limitações às políticas hackers decorreriam dos riscos aos quais essas populações já são vulneráveis, como violência, repressão, deslegitimação e silenciamento. Porém, considerando a discussão de limites das políticas hackers propostos por Delfanti & Söderberg (2018), são necessários comentários em relação aos processos de adoção, adaptação e reaproveitamento de discursos, práticas e inovações hackers por corporações e instituições analisados a partir dos ciclos de recuperação.

Como foi apontado no terceiro capítulo, a maioria das análises tratou dos seus objetos de estudo a partir de duas perspectivas temporais: da incorporação de uma única tecnologia ou comunidade e da evolução dos hackers como movimento ou em relação ao contexto ou outros atores. A preocupação expressa nas análises em identificar dinâmicas, descrever atividades, apontar tendências e direcionamentos dos grupos, comunidades e movimentos, somada às percepções de que hackers, hackerismos e aspectos relacionados ainda estão em fase de exploração e possuem potencial emancipatório, tiveram implicações. Mesmo quando as discussões foram mais críticas em relação aos desdobramentos dos casos e às tecnologias da informação, as análises não se focaram no processo de recuperação. A exceção seria o artigo de Evangelista (2014) sobre o movimento do *software* livre no Brasil, em que a transformação ao longo dos anos do FISL como resultado do processo de cooptação do movimento pelo grupo do código aberto – mais inclinado à lógica capitalista – é parte central da análise. Em outras publicações, aspectos que seriam considerados como evidências de processos de recuperação são mencionados, mas não fazem parte da análise, como no caso dos hackatons liderados pelo Estado e grandes corporações e a absorção de elementos hackers como racionalidade na formulação e implementação de políticas públicas de inclusão digital, como no OLPC (VILLANUEVA & OLIVERA, 2012; CHAN, 2014).

A literatura dos estudos hackers consultada para realização do estudo de escopo – principalmente aquelas do segundo momento[58] – não foi suficiente para abranger a totalidade das políticas hackers que emergem na América Latina, o que está relacionado tanto à forma com que criam conhecimento – propondo teorias mais gerais sobre engajamento político dos hackers a partir dos estudos de caso – quanto pelo fato de que trabalham com outras realidades sociotécnicas. Explorar quem são os hackers de computador na América Latina abre caminho para identificar uma série de manifestações e políticas que não são abordadas por esses autores, diversifica quem são os hackers e os motivos de engajamento em

[58] É importante reiterar que as comparações foram realizadas em relação ao grupo de autores consultados para o estudo de escopo, autores estes cujo foco é produzir conhecimento sobre políticas hackers, estavam presentes na Escola Doutoral de Estudos Digitais e trouxeram questionamentos que levaram à proposição da pesquisa realizada durante o doutoramento.

hackerismos, questiona conceitos utilizados amplamente (como o agnosticismo político) e amplia outros (como os aspectos luditas do hackerismo como resistência tecnológica ou as fontes de limitação às políticas hackers). Além disso, a produção acadêmica sobre hackers de computador na América Latina apresenta uma série de perspectivas diferentes a partir das quais as manifestações e políticas hackers podem ser abordadas. Nesse sentido, foi possível identificar o desenvolvimento de agendas de pesquisa que se mostraram características à América Latina:

1. Hackers e intersecções com movimentos de povos tradicionais e indígenas;
2. Hackers e intersecções com gênero;
3. Arte e literatura como hackerismos;
4. Racionalidades hackers na formulação e implementação de políticas públicas, e;
5. *Software* livre e políticas nacionais de desenvolvimento.

Considerando o conjunto de publicações selecionadas, alguns comentários podem ser tecidos sobre a criação das categorias de análise para políticas hackers e o trabalho realizado a partir delas. Como apontado no terceiro capítulo, as categorias foram criadas com base nas análises realizadas pelos autores, principalmente em relação às relações, conflitos e disputas identificadas. Tendo isso em consideração, é importante mencionar que algumas das análises identificadas na literatura consultada para a composição do estudo de escopo se enquadrariam nas categorias e subcategorias criadas – como os casos mencionados em políticas liberais e radicais. Essa percepção remeteria às observações de Maxigas (2012) e Coleman (2017) de que alguns aspectos relacionados aos hackers – como materialidades, táticas e sociabilidades – são particulares ao hackerismo como movimento, enquanto outras são próprias das intersecções entre hackers e as especificidades de seus contextos.

Ao mesmo tempo, quando analisadas em relação ao conteúdo das publicações, as categorias e subcategorias apresentam aspectos tipicamente latino-americanos. Resistência de povos tradicionais e indígenas, intersecções entre hackers e gênero, elementos hackers como racionalidade de políticas públicas são alguns exemplos que pouco apareceram – ou não apareceram em nenhum momento – nas análises da literatura consultada para o estudo de escopo, como apontado anteriormente. Esse resultado não indica que essas perspectivas das políticas hackers não sejam exploradas por outros autores, mas reflete as leituras realizadas para o desenvolvimento desta pesquisa e aponta caminhos para aprofundamento das buscas sobre grupos, comunidades, eventos e fenômenos hackers em outras localidades e contextos.

Por fim, as categorias permitiram realizar comparações e, a partir delas, identificar as especificidades das análises realizadas e casos estudados. Este exercício pareceu particularmente importante para a identificação de contribuições de um conjunto de publicações para um corpo de conhecimento, que é o objetivo desta pesquisa. Ao tornar transparente os parâmetros utilizados, espera-se ser possível criar outras categorias e subcategorias quando necessário e permitir a inclusão de novos estudos para comparação e análise futuras.

Nessa direção, alguns questionamentos surgidos ao longo deste estudo poderiam indicar possíveis desdobramentos desta pesquisa. Por construir um panorama dos estudos de caso e identificar agendas de pesquisa sobre hackers de computador características à América Latina, o estudo aqui desenvolvido acabou abrindo caminhos para aprofundamentos tanto dos principais temas identificados quanto em relação às potenciais intersecções que não foram exploradas, seja por meio da escolha de outras palavras-chave mais específicas à cada tema identificado, seja explorando por outras perspectivas as publicações selecionadas.

Uma dimensão não explorada foi o engajamento político dos autores que pesquisam sobre hackers de computador na América Latina, que muitas vezes compartilham interesses e são ativistas das mesmas causas que seus objetos de estudo. Esses acadêmicos ativistas são encontrados em eventos como a CryptoRave, em que muito deles propõem mesas de discussão sobre criptografia, privacidade e o contexto de capitalismo de vigilância, como é o caso daqueles do ICTS-Unicamp, do MediaLab-UFRJ e de Sérgio Amadeu da Silveira. Particularmente, os pesquisadores vinculados a esses dois grupos, assim como Sérgio Amadeu, são membros da Rede Latino-Americana de Estudos sobre Vigilância, Tecnologia e Sociedade (LAVITS). Apesar de ter tido contato com o trabalho dos pesquisadores dessa rede, suas publicações não foram contempladas por este estudo. Minhas hipóteses sobre essa ausência recaem sobre as escolhas dos parâmetros das buscas, mas também sobre uma possível perspectivas desses autores sobre como seus objetos se interseccionam com hackers, que podem ser entendidos como parte do espírito de época do capitalismo informacional.

Ainda assim, a LAVITS explora diversos aspectos do capitalismo de vigilância que, como foi possível constatar, é o contexto em resposta ao qual as diferentes manifestações hackers que compartilham o espaço da CryptoRave estão criando ferramentas, promovendo discussões e organizando resistências. Nesse sentido, mapear e explorar a produção de conhecimento da LAVITS seria um aprofundamento interessante para este estudo, assim como acompanhar o desenvolvimento de temas na CryptoRave e identificar as intersecções.

Este estudo buscou contribuir com os estudos hackers como um todo ao demonstrar que hackers de computador na América Latina são um objeto de estudo amplamente discutido. Especificamente sobre as políticas hackers, a realização da Revisão Sistemática de Bibliografia e a identificação de agendas de pesquisa específicas podem configurar este estudo como um dos pontos de partida para a compreensão de que as discussões sobre políticas hackers são abordadas pelos estudos sobre a América Latina desde os anos 1990 em resposta às especificidades dos grupos, comunidades, eventos e fenômenos hackers. Neste sentido, uma das principais contribuições foi evidenciar que a literatura existente sobre a América Latina identifica e explora genealogias e manifestações nossas, muitas vezes analisadas a partir de outras perspectivas, atribuindo novos significados aos hackers e hackerismos, assim como às suas políticas.

REFERÊNCIAS

AKRICH, Madeleine. The de-scription of technical objects. In: BIJKER, W. E.; LAW, J. (Eds.) **Shaping technology/Building Society**: studies in sociotechnical change. Cambridge e Londres: The MIT Press, 1992, p. 205-224.

ARAUJO, Daniela Camila. **Feminismo e cultura hacker: intersecções entre política, gênero e tecnologia**. Campinas, Unicamp, 2018. 147 p.

ARAUJO, Daniela Camila.; GITAHY, Leda Maria. Marias da tecnologia: da exclusão ao empoderamento. In: JORNADAS LATINO-AMERICANAS DE ESTUDOS SOCIAIS DA CIÊNCIA E DA TECNOLOGIA, 11., 2016, Curitiba, **Anais**... Curitiba: UTFPR, 2016. Disponível em: < http://www.esocite2016.esocite.net/resources/anais/6/1471456835_ ARQUIVO_artigo_esocite_2016_daniela_araujo.pdf >. Último acesso em 17 jul. 2017.

BARBROOK, Richard; CAMARON, Andy. The California ideology. **Science as Culture**, v. 6, n. 1, p.44-72, 1996.

BURTET, Cecilia. G. **Os saberes desenvolvidos nas práticas em um hackerspace de Porto Alegre**. Porto Alegre, UFRGS, 2014. 223 p.

CASTELLS, Manuel. O informacionalismo e a sociedade em rede (posfácio). In: HINAMEN, P. **A ética dos hackers e o espírito da era da informação**. Tradução Fernanda Wolff. Rio de Janeiro: Campus, 2001, p. 137-154.

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

CHAN, Anita Say. Beyond technological fundamentalismo: peruvian hack labs & inter-technological" education. **Journal of Peer Production**, v. 5, 2014. Disponível em: < http://peerproduction.net/editsuite/issues/issue-5-shared-machine-shops/peer-reviewed-articles/beyond-technological-fundamentalism-peruvian-hack-labs-and-inter-technological-education/ >. Acesso em: 24 fev. de 2017.

COLEMAN, Gabriella. The Political Agnosticism of Free and Open Source *Software* and the Inadvertent Politics of Contrast. **Anthropological Quarterly**, v. 77, n. 3, p. 507-519, 2004.

COLEMAN, G. Hacker politics and publics. **Public culture**, v. 23, n. 3, p. 511-516, 2011.

COLEMAN, Gabriella. **Coding Freedom**: the ethics and aesthetics of hacking. Princeton and Oxford: Princeton University Press, 2013.

COLEMAN, Gabriella. **Hacker, hoaxer, whistleblower, spy**: the many faces of Anonymous. Londres: Verso, 2014.

COLEMAN, G. Hacker. In: PETERS, B. (Ed.). **Digital Keywords**: a vocabulary of information society and culture. Princeton: Princeton University Press, 2016, p. 158-172.

COLEMAN, Gabriella. From Internet Farming to Weapons of the Geek. **Current Anthropology**, v. 58, n. 15, 2017.

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

DAGNINO, Renato. **Neutralidade da ciência e determinismo tecnológico**: um debate sobre a tecnociência. Campinas: Unicamp, 2008.

DELFANTI, Alessandro; SÖDERBERG, Johan. Repurposing the hacker: three cycles of recuperation in the Evolution of hacking and capitalism. Ephemera, v. 18, n. 3, p. 457-476, 2018.

DUNBAR-HESTER, Christine. Geeks, Meta-Geeks, and Gender Trouble: Activism, Identity, and Low-power FM Radio. **Social Studies of Science**, v. 38, n. 2, p. 201-231, 2008.

EVANGELISTA, Rafael Aalmeida. **Traidores do movimento**: política, cultura, ideologia e trabalho no *software* livre. Campinas: Unicamp, 2010. 240 p.

FEENBERG, Andrew. The politics of meaning: modernity, technology, and rationality**. Radical Philosophy Review**, mar., 2016. Disponível em <https://www.pdcnet.org/radphilrev/ content/radphilrev_2016_0999_3_9_49>. Acesso em: 22 jan. 2017.

FONSECA, Felipe. S. **Redelabs**: laboratórios experimentais em rede. Campinas: Unicamp, 2014. 120 p.

GRENZFURTHNER, Johannes; SCHNEIDER, Frank A. Hacking the spaces. **Monochrom**, 2009. Disponível em: <http://www.monochrom.at/hacking-the-spaces/>. Acesso em: 9 jan. 2017.

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

KELTY, Christopher. Geeks, Social Imaginaries, and Recursive Publics. **Cultural Anthropology**, v. 20, n. 2, p. 185-214, 2005.

KELTY, Christopher. **Two bits**: the cultural significance of free sofware. Durham: Duke University Press, 2008.

KNORR-CETINA, Karin D. The Ethnographic Study of Scientific Work: Towards a Constructivist Interpretation of Science. In: KNORR-CETINA, K. D. (Ed.). **Science Observed**: Perspectives on the Social Study of Science. Londres: Sage, 1983, p. 115-140.

LEVY, Steven. **Hackers**: heroes of the computer revolution. Sebastopol: O'Reilly Media, 2010 [1984].

LEVY, Yair.; ELLIS, Timothy. J. A Systems Approach to Conduct na Effective Literature Review in Support of Information Systems Research. **Informing Science Journal**, v. 9, p. 181-212, 2006.

LUND, Arwid. A critical political economic framework for peer production's relation to capitalismo. **Journal of Peer Production**, v. 10, 2017. Disponível em: < http://peerproduction.net/issues/issue-10-peer-production-and-work/peer-reviewed-papers/a-critical-political-economic-framework-for-peer-productions-relation-to-capitalism/ >. Acesso em: 13 jun. 2017.

MATTOS, Erica. A. C. **Ethos hacker e hackerspaces**: práticas e processos de aprendizagem, criação e intervenção. Florianópolis, UFSC, 2014. 144 p.

MAXIGAS. Hacklabs and hackerspaces: tracing two genealogies. **Journal of Peer Production**, v. 2, 2012. Disponível em: http://peerproduction.net/issues/issue-2/peer-reviewed-papers/hacklabs-and-hackerspaces/. Acesso em: 31 ago. 2016.

MAXIGAS. Hackers against technology: Critique and recuperation in technological cycles. **Social Studies of Science**, v. 47, n. 6, p. 841-860, 2017.

MOROZOV, Evgeny. Making it: pick up a spot welder and join the revolution. **The New Yorker**, 13 jan. 2014. Disponível em: < http://www.newyorker.com/magazine/2014/01/13/making-it-2 >. Acesso em: 31 ago. 2016.

NASCIMENTO, Susana. Critical notions of technology and the promises of empowerment in shared machine shops. **Journal of Peer Production**, v. 5, 2014. Disponível em: < http://peerproduction.net/issues/issue-5-shared-machine-shops/editorial-section/critical-notions-of-technology-and-the-promises-of-empowerment-in-shared-machine-shops/ >. Acesso em: 24 fev. 2017.

PFAFFENBERG, Bryan. Technological dramas. Science, **Technology & Human Values**, v. 17, n. 3, pp. 282-312, 1992.

PITA, Marina. Por que precisamos da criptografia. **Blog da Redação**, 2017. Disponível em: < https://outraspalavras.net/blog/2017/04/24/por-que-precisamos-da-criptografia/ >. Acesso em 17 de maio de 2017.

RAYMOND, Eric. S. **How To Become A Hacker**. 1996 (revisão 1.51 out. 2017). Disponível em: <http://catb.org/~esr/faqs/hacker-howto.html>. Último acesso em: 7 nov. 2018.

RAYMOND, Eric. S. **The Cathedral and the Bazaar**. 1999. Disponível em: < http://www.unterstein.net/su/docs/CathBaz.pdf >. Último acesso em: 7 nov. 2018.

SAMPAIO, R. F.; MANCINI, M. C. Estudos de revisão sistemática: um guia para síntese criteriosa da evidência científica. **Revista Brasileira de Fisioterapia**, v. 11, n. 1, p. 83-89, jan/fev, 2007.

SCHROCK, Andrew R. Education in disguise: culture of a hacker and maker space. **InterActions**, v. 10, n. 1, 2014.

SANCHO, Guiomar Rovina. Multidões conectadas e movimentos sociais: dos zapatistas e do hacktivismo à tomada das ruas e das redes. Tradução Lucas Melgaço. In: BRUNO, F. et al (orgs.) **Tecnopolíticas da vigilância**: perspectivas da margem. São Paulo: Boitempo, 2018, p. 355-376.

SELLTIZ, Claire et al. **Métodos de pesquisa nas relações sociais**. Tradução Dante Moreira Leite. São Paulo: Editora da Universidade de São Paulo, 1975, cap. 3-4.

SÖDERBERG, Johan. Determining social change: The role of technological determinismo in the collective action framing of hackers. **New media & society**, v. 15, n. 8, p. 127-1293, 2013.

SÖDERBERG, Johan. Inquiring Hacking as Politics: A New Departure in Hacker Studies? **Science, Technology, & Human Values**, v. 42, n. 5, p. 969-980, 2017.

TOUPIN, Sophie. Feminist hackerspaces: the synthesis of feminist and hacker cultures. **Journal of Peer Production**, v. 5, 2014. Disponível em: < http://peerproduction.net/issues/issue-5-shared-machine-shops/peer-reviewed-articles/feminist-hackerspaces-the-synthesis-of-feminist-and-hacker-cultures/ >. Acesso em: 24 fev. 2017.

TRANFIELD, David; DENYER, David. SMART; Palminder. Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. **British Journal of Management**, v. 14, p. 207-222, 2003.

TROXLER, Peter.; MAXIGAS. We now have the means of production, but where is my revolution? **Journal of Peer Production**, v. 5, 2012. Disponível em: < http://peerproduction.net/issues/issue-5-shared-machine-shops/editorial-section/editorial-note-we-now-have-the-means-of-production-but-where-is-my-revolution/ >. Acesso em: 24 fev. 2017.

VELHO, Lea. Conceitos de Ciência e a Política Científica, Tecnológica e de Inovação. **Sociologias**, ano 13, n. 26, p.128-153, 2011.

WINNER, Langdom. Do Artifacts Have Politics?. **Daedalus**, v. 109, n. 1, p. 121-136, 1980.

WRAY, Stefan. On eletronic civil disobedience. **Peace Review: A Journal of Social Justice**, v. 11, n. 1, p.107-111, 1999.

ZUBOFF, Shoshana. Big other: Surveillance capitalism and the prospects of an information civilization. **Journal of Information Technology**, n. 30, pp. 75–89, 2015.

ANEXO A - Referências bibliográficas do conjunto de publicações selecionadas

ALCÍVAR T., Carlos; BLANC P.; Glenda; CALDERÓN C., Juan. Aplicación de la ciencia forense en los delitos informáticos en el Ecuador y su punibilidade. **Revista Espacios**, v. 39, n. 42, p. 1-10, 2018.

ALMEIDA, Marco Antonio. Políticas culturais e redes sociotécnicas: reconfigurando o espaço público. **Ciências Sociais Unisinos**, v. 50, n. 1, p. 54-64, 2014.

ARAUJO, Daniela; GITAHY, Leda. Mulheres e a segurança da informação: a trajetória de um hackerspace feminista no Brasil. In: SIMPÓSIO INTERNACIONAL LAVITS, 4, 2017, Buenos Aires. **Anais...** Buenos Aires, 2017, p. 1-9.

AROCENA, Gustavo. A. La regulación de los delitos informáticos en el código penal argentino. Introducción a la ley nacional núm. 26.388. **Boletín Mexicano de Derecho Comparado**, v. 45, n. 135, p. 945- 988, 2012.

BARON, Anton P. Práctica y motivación en el entorno hacker: un análisis empírico. **Revista Científica Internacional**, v. 1, n. 1, p. 61-92, 2014.

BORGES, Fabiana Morais. Questionário sobre tecnoxamanismo. **Revista Metamorfose**, v. 3, n. 1, setembro, p. 104-120, 2018.

BROWN, J. Andrew. Hacking the past: Edmundo Paz Soldán's "El delirio de Turing" and Carlos Gamerro's "Las Islas". **Arizona Journal of Hispanic Cultural Studies**, v. 10, p. 115-129, 2006.

BUNKER, Robert J. The growing Mexican Cartel and vigilante war in cyberspace: information offensives and counter-offensives. **Small Wars Journal**, 2011. Disponível em: < https://smallwarsjournal.com/index.php/jrnl/art/growing-mexican-cartel-and-vigilante-war-cyberspace >. Último acesso em 17 de julho de 2019.

CERQUEIRA, Silvio Castro; ROCHA, Claudionor. Crimes cibernéticos: desafios da investigação. **Cadernos ASLEGIS**, n. 49, mai/ago, p. 133-161, 2013.

CHAN, Anita Say. Balancing Design: OLPC Engineers and ICT Translations at the Periphery. In: MEDINA, E.; MARQUES, I. C.; HOLMES, C. (Eds.) **Essays on Science, Technology, and Society in Latin America**. Cambridge: MIT Press, 2014, p. 181-205.

CHIESA, Carolina Dalla.; CAVEDON, Neusa. Rolita. Elementos Anarquistas no Cotidiano de Uma Organização Contemporânea: o Caso da Casa da Cultura Digital de Porto Alegre. **Revista Gestão Organizacional**, v. 13, n. 1, p 11-23, 2015.

CLEAVER, Harry. The Zapatistas and the Electronic Fabric of Struggle. In: HOLLOWAY, J.; PELÁEZ, E. (Eds.) **Zapatista!: Reinventing Revolution in Mexico**. London: Pluto Press, 1998. Disponível em: < https://la.utexas.edu/users/hcleaver/zaps.html >. Último acesso em 17 de julho de 2019.

COLEMAN, Gabriella. Conference: A Ritual Condensation and Celebration of a Lifeworld. **Anthropological Quarterly**, v. 83, n. 1, p. 47-72, 2010.

DÍAZ, Germán Alejandro M.; SEGURA, Felipe T. Análisis sistémico en la generación cultural de uma comunidad virtual de aprendizaje. REDIE. **Revista Electrónica de Investigación Educativa**, v. 15, n. 1, p. 1-16, 2013.

DONAS, Javier. B. Los nuevos derechos humanos: gobierno electrónico e informática comunitária. Enl@ce: **Revista Venezolana de Información, Tecnología y Conocimiento**, v. 4, n. 2, p. 13-27, 2007.

ENTEEN, Jillana. "On the Receiving End of the Colonization": Nalo Hopkinson's 'Nansi Web. **Science Fiction Studies**, v. 34, n. 2, p. 262-282, 2007.

EVANGELISTA, Rafael. O movimento *software* livre do Brasil: política, trabalho e hacking. **Horizontes Antropológicos**, Porto Alegre, a. 20, n. 41, p. 173-200, 2014.

FERNÁNDEZ, Rubén F. El arte hacker: el activismo en la era digital. **Ábaco**, v.2, n. 68/69, p. 88-97, 2011.

FRANÇA FILHO, Genauto C.; AGUIAR, Vicente M. Um trabalho a troco de nada? A ação de uma comunidade de hackers à luz da teoria da dádiva. **Sociologias**, v. 16, n. 36, p. 104-142, 2014.

GACHARNÁ G. Federico Iván. Hacker ético vs. delincuente informático: Una mirada en el contexto colombiano. **Inventum**, n.6, p. 46-49, 2009.

GAINZA C, Carolina. Literatura chilena en digital: mapas, estéticas y conceptualizaciones. **Revista Chilena de Literatura**, n. 94, p. 233-256, 2016.

GARCÍA Hernán Manuel. Tecnociencia y cibercultura em México: hackers em el cuento cyberpunk mexicano. **Revista Iberoamericana**, v. 78, ns. 238-239, jan/jun, p. 329-348, 2012.

GARCÍA, Miguel. Urbes corruptoras y visiones apocalípticas en dos novelas ciberpunk latino-americanas. **Chasqui**, v. 44, n. 2, novembro, p. 138-148, 2015.

GRAVANTE, Tommaso. Ciberactivismo y apropiación social. Un estudio de caso: la insurgencia popular de Oaxaca. **Sociedade e Cultura**, v. 15, n. 1, jan/jun, p. 51-60, 2012.

GUIZARDI, Francini Lube et al.. Maratonas hackers no Brasil com desafios no campo da saúde. **Interface**, Botucatu, v. 22, n. 65, p.447-459, 2018.

GUTIÉRREZ, Bernardo. Criptopunks y América Latina: de la soberanía tecnológica a la era de las filtraciones. **Revista Teknokultura**, v. 12, n. 3, p. 549-576, 2015.

HERNÁNDEZ, Miguel; BAQUERO, Luis; GIL, Celio. Approach to the State of the Art of Ciberdelincuence in Colombia. **International Journal of Applied Engineering Research**, v. 13, n. 23, p. 16648-16655, 2018.

HERRERA, Antonio Del Rivero; GARRIDO, Edith Aurora R. Arte y TIC: ¿Predominio de la técnica o la cognición?. **Versión Nueva Época**, n. 27, setembro, p. 1-12, 2011.

ISLAS, Octavio; ARRIBAS, Amaia; MINERA, Ericka. El empleo propagandístico de Internet 2.0 en campañas a puestos de elección ciudana, estado de México, julio 2009. **Razón y Palabra**, v. 14, n. 70, nov/jan, 2009.

JOLÍAS, Lucas; PRINCE, Alejandro. El ecossistema argentino de los datos abiertos. In: PANDO, D.; ARROYO, N. F. (Orgs.) **El gobierno electrónico a nível local**. Buenos Aires: Fundació CIPPEC, 2013, p. 110-131.

JORZA, Diana R. La figuración de una utopía política en El delirio de Turing de Edmundo Paz Soldán. **Revista Hispánica Moderna**, a. 65, n. 1, p. 47-64, 2012.

LEDESMA, Eduardo. The Poetics and Politics of Computer Code in Latin America: Codework, Code Art, and Live Coding. **Revista de Estudios Hispánicos**, v. 49, n. 1, março, p. 91-120, 2015.

LIMA, Carlos Henrique M. A cidade em movimento: práticas insurgentes no ambiente urbano. **Oculum Ensaios**, v. 12, n. 1, p. 39-48, 2015.

MACHADO, Murilo Bansi. Entre o controle e o ativismo hacker: a ação política dos Anonymous Brasil. **História, Ciências, Saúde – Manguinhos**, Rio de Janeiro, v. 22, dez., p.1531-1549, 2015.

MAGUIRE, Emily A. El hombre lobo en el espacio: el hacker como monstruo en el cyberpunk cubano. **Revista Iberoamericana**, v. 75, n. 227, abr/jun, p.505-521, 2009.

MENDOZA, Jorge Lizama. Hackers: de piratas a defensores del *software* libre. **Revista Mexicana de Ciencias Políticas y Sociales**, v. 45, n. 185, mai/ago, p. 91-108, 2002.

MILLS, Alan. Literatura hacker y la creación del nahual del lector. **Cuadernos Hispanoamericanos**, n. 744, jun, p.13-30, 2012.

MOTA, Bárbara M. F.; FIGUEIREDO FILHO, Dalson B. Quem controla a política de ninguém? Anonymous Brasil e o ativismo hacker nas redes de comunicação. **Emancipação**, Ponta Grossa, v. 15, n. 2, p. 299-315, 2015.

MOTA, Bárbara M. F.; HAYASHI, Renato. T.; FERNANDES, Antônio. A. Hacking político: crime cibernético ou manifestação legal de protesto?. **Argumentum**, v. 8, n. 3, p. 122-132, 2016.

NATANSOHN, Graciela. Cuidados digitais em perspectiva ciberfeminista. In: CONGRESSO BRASILEIRO DE CIÊNCIAS DA COMUNICAÇÃO (INTERCOM), 41, 2018, Joinville. **Anais...** Joinville: Universidade da Região de Joinville, 2018, p. 1-18.

NATANSOHN, Graciela; PAZ, Mônica. Entre usos y apropiaciones de tecnología digital: ciberfeminismos contemporâneos. In: Encontro Anual da Compós, 27, 2018, Belo Horizonte. **Anais...** Belo Horizonte: PUC-MG, 2017, p. 1-20.

NELSON, Diana M. Maya Hackers and the Cyberspatialized Nation-State: Modernity, Ethnostalgia, and a Lizard Queen in Guatemala. **Cultural Anthropology**, v. 11, n. 3, p. 287-308, 1996.

NÚÑEZ, Alma Celia Galindo. Hackmitin 2016: jóvenes y practicas digitales. In: TOLEDO, D. B.; YAÑEZ, C. E. J.; HUERTA, C. A. F. **Cultura em América Latina: práticas, significados, cartografias y discusiones**. Mexicali: Instituto de Investigaciones Culturales-Museo, 2017, p. 81-93.

OJEDA-PÉREZ, Jorge Eliéses et al. Delitos informáticos y entorno jurídico vigente en Colombia. **Cuadernos de Contabilidad**, v. 11, n. 28, p. 41-66, 2010.

OVIEDO, César E. S. El delírio de la globalizacion: la literatura tras el caminho y los caminhantes. **IUS ET VERITAS**, n. 27, p. 389-395, 2003.

PARRA, Henrique. Controle social e prática hacker: tecnopolítica e ciberpolítica em redes digitais. **Sociedade e Cultura**, v. 15, n. 1, jan/jun, p. 109-120, 2012.

PAZ, Mônica de Sá Dantas. A divisão digital de gênero no movimento *software* livre do Brasil. In: NATANSOHN, G. **Internet em código feminino: teorias e práticas**. Buenos Aires: La Crujía, 2013, p. 151-162.

PEDERSON, Claudia Costa. Situating making in contemporary Latin American feminist art. **Journal of Peer Production**, 2016. Disponível em: < http://peerproduction.net/issues/issue-8-feminism-and-unhacking-2/peer-reviewed-papers/issue-8-feminism-and-unhackingpeer-reviewed-papers-2situating-making-in-contemporary-latin-american-feminist-art/ >. Último acesso em 17 de julho de 2017.

PÉREZ-BUSTOS, Tania. Construyendo espacios de exclusividade: uma aproximación etnográfica al papel y la experiencia de mujeres índias y colombianas em lascomunidades locales de *Software* Libre. **Universitas Humanística**, n. 69, p. 115-137, 2010a.

PÉREZ-BUSTOS, Tania. Reflexiones sobre una etnografía feminista del *Software* Libre en Colombia. **Revista Estudos Feministas**, v. 18, n. 2, mai/ago, p. 385-405, 2010b.

PINO, Edixela. K. B. El hacktivismo: entre la participación política y las tácticas de subversión digital. **Razón y Palabra**, v. 18, n. 88, 2014.

PITMAN, Thea. Latin American Cyberprotest: Before and After the Zapatistas. In: TAYLOR, C.; PITMAN, T (Eds.) **Latin American Cyberculture and Cyberliterature**. Liverpool: Liverpool University Press, 2007, p. 86-110.

PRETTO, N. Redes colaborativas, ética hacker e educação. **Educação em Revista**, v. 26, n. 3, p. 305-316, 2010.

REDONDO, Juan C. T. From Socialist Realism to Anarchist Capitalism: Cuban Cyberpunk. **Science Fiction Studies**, v. 32, n. 3, p. 442-466, 2005.

RENNO, Raquel. Activism in Brazil: hacker spaces as spaces of resistance and free. **Medien Impulse**. Disponível em: <http://www.medienimpulse.at/articles/view/648>. Último acesso em 17 de julho de 2019.

ROCHA, C. T. C. Expressões do ciberfeminismo na contemporaneidade. **Tecnologia e Sociedade**, v. 2, n. 3, p. 43-61, 2006.

RODRÍGUEZ, Juan Antonio; ODUBER, Jesús; MORA, Endira. Actividades rutinarias y cibervictimización en Venezuela. **Revista Latinoamericana de Estudios de Seguridad**, n. 20, junho, p. 63-79, 2017.

RONFELDT, David; MARTÍNEZ, Armando. A Comment on theZapatista "Netwar". In: ARQUILLA, J.; RONFELDT, D. (Eds.) **In Athena's Camp: preparing for conflict in the information age**. Santa Monica: RAND Corporation, 1997, p. 369-391.

RUIZ, Patricia. T.; SEGURA, Jessica. D.; QUESADA, Vania. T. Violencia en internet: nuevas víctimas, nuevos retos. **Liberabit Revista de Psicología**, v. 15, n. 1, p. 7-19, 2009.

SCHÄFER, Camila. Hackers e sua relação com o surgimento e desenvolvimento da chipmusic. **Mediação**, Belo Horizonte, v. 17, n. 20, jan/jun, p. 85-98, 2015.

SOLÓRZANO, Sofía. F. Las comunidades de *software* libre de costa rica. **Revista de Ciencias Sociales**, v. 4-1, n. 126-127, p. 143-152, 2009.

SUAZA, Luz Marina. Hackeando el patriarcado: metáforas y prácticas sociales de mujeres com tecnologias. In: ORTIZ, R. R.; DÍAZ, A. D. F.; SIERRA, L. M. R. (Eds.) **Ciberciudadanías, cultura política y creatividad social**. Bogotá: Universidad Pedagógica Nacional, 2013, p. 139-186.

SUAZA, Luz Marina; ORTIZ, Rocío Rueda. Cibercultura, género y política: Hacia uma emergente creatividad social y educativa. **Educació i Cultura**, n. 22, p. 21-36, 2011.

TAVARES, Luis Eduardo. Ágoras on-line: a participação cidadã no contexto da cultura digital. In: Congresso Latino Americano de Opinião Pública da WAPOR, 4, 2011, Belo Horizonte. **Anais...** Belo Horizonte, 2011, p. 1-36.

TRÄSEL, Marcelo. Hacks and hackers: the ethos and beliefs of a group of Data-Driven Journalism professionals in Brazil. **Revista FAMECOS: mídia, cultura e tecnologia**, v. 25, n. 1, jan/abr, p. 1-14, 2018.

VÁZQUEZ, Daniel. En la web, 'un actor mucho más importante es la gente sin organización'. Chasqui. **Revista Latinoamericana de Comunicación**, n. 123, setembro, p. 48-54, 2013.

VILLANUEVA-MANSILLA, Eduardo; OLIVERA, Paz. Barreras Institucionales para el Desarrollo de una Innovación: Evaluando la Implementación de las Computadoras XO-1 en dos Escuelas Periurbanas del Perú. **Information Technologies & International Development**, v. 8, n. 4, p. 191-203, 2012.

VON WERDER, Sophie Dorothee. Control y fugas en la era digital, en El delirio de Turing, de Edmundo Paz Soldán. **Alea: Estudos Neolatinos**, v. 18, n. 1, jan/abr, p. 54-64, 2016.

ZANOTTI, Agustín. Comunidades de *software* libre en Argentina: motivaciones, participación, militância. **Perspectivas de la Comunicación**, v. 7, n. 2, p. 55-74, 2014.

ZANOTTI, Agustín. Reescribiendo tecnologías: aproximaciones al movimiento *software* libre y su difusión en Argentina. **Intersticios: Revista Sociológica de Pensamiento Crítico**, v. 5, n. 2, p.145-159, 2011.

ANEXO B – Agrupamentos e categorias de análise por publicação

Referência	Objeto de estudo	Definição de hackers	Políticas hackers
Alcívar, Blanc & Calderón (2018)	Hackers + outros atores	Práticas – cibercrime	Violência e ilegalidade
Almeida (2014)	Hackers + outros atores	Práticas – características do trabalho hacker	Políticas do dia-a-dia
Araujo & Gitahy (2017)	Comunidade/grupo/coletivo	Práticas – características do trabalho hacker	Políticas do dia-a-dia + Resistências
Arocena (2012)	Hackers + outros atores	Práticas – cibercrime	Violência e ilegalidade
Baron (2014)	Representações hackers	Entusiasmo com tecnologias da informação	Políticas do dia-a-dia
Borges (2018)	Representações hackers	Relação com ferramentas e tecnologias da informação	Políticas do dia-a-dia
Brown (2006)	Representações hackers	Relação com ferramentas e tecnologias da informação	Resistências
Bunker (2011)	Hackers + outros atores	Práticas – características do ser hacker	Outras formas de fazer política pública, influenciar na tomada de decisões, expressar politicamente
Cerqueira & Rocha (2013)	Hackers + outros atores	Práticas – características do trabalho hacker	Violência e ilegalidade
Chan (2014)	Hackers + outros atores	Práticas – características do trabalho hacker	Outras formas de fazer política pública, influenciar na tomada de decisões, expressar politicamente
Chiesa & Cabedon (2015)	Potencialidades	Práticas – características do ser hacker	Transposição do ser hacker para outros meios
Cleaver (1998)	Hackers + outros atores	Relação com ferramentas e tecnologias da informação	Resistências + Outras formas de fazer política pública, influenciar na tomada de decisões, expressar politicamente
Coleman (2010)	Comunidade/grupo/coletivo	Entusiasmo com tecnologias da informação	Políticas do dia-a-dia
Díaz & Segura	Comunidade/grupo/coletivo	Práticas – características do	Transposição do ser hacker para outros meios

(2013)		trabalho hacker	
Donas (2007)	Hackers + outros atores	Práticas – características do ser hacker	Outras formas de fazer política pública, influenciar na tomada de decisões, expressar politicamente
Enteen (2007)	Hacking em outros meios	Práticas – características do ser hacker	Transposição do ser hacker para outros meios
Evangelista (2014)	Comunidade/grupo/coletivo	Práticas – características do ser hacker	Políticas do dia-a-dia
Fernández (2011)	Hacking em outros meios	Relação com ferramentas e tecnologias da informação	Transposição do ser hackers para outros meios + Outras formas de fazer política pública, influenciar na tomada de decisões, expressar politicamente
França Filho & Aguiar (2014)	Potencialidades	Práticas – características do trabalho hacker	Políticas do dia-a-dia
Gacharná G. (2009)	Representações hackers	Entusiasmo com tecnologias da informação	Violência e ilegalidade
Gainza C. (2016)	Hacking em outros meios	Relação com ferramentas e tecnologias da informação	Transposição do ser hacker para outros meios
García (2012)	Hacker + contexto	Práticas – características do ser hacker	Transposição do ser hacker para outros meios
García (2015)	Hacker + contexto	Relação com ferramentas e tecnologias da informação	Políticas do dia-a-dia
Gravante (2012)	Potencialidades	Práticas – características do ser hacker	Resistências + Outras formas de fazer política pública, influenciar na tomada de decisões, expressar politicamente
Guizardi et al. (2018)	Potencialidades	Práticas – características do trabalho hacker	Transposição do ser hacker para outros meios
Gutiérrez (2015)	Hackers + outros atores	Relação com ferramentas e tecnologias da informação	Resistências + Outras formas de fazer política pública, influenciar na tomada de decisões, expressar politicamente
Hernández, Baquero & Gil (2018)	Hackers + outros atores	Relação com ferramentas e tecnologias da informação	Violência e ilegalidade
Herrera & Garrido	Hacking em outros meios	Relação com ferramentas e	Transposição do ser hacker para outros meios

(2011)		tecnologias da informação	
Islas, Arribas & Minera (2009)	Hackers + outros atores	Práticas – características do ser hacker	Outras formas de fazer política pública, influenciar na tomada de decisões, expressar politicamente
Jolías & Prince (2013)	Hackers + outros atores	Práticas – características do trabalho hacker	Outras formas de fazer política pública, influenciar na tomada de decisões, expressar politicamente
Jorza (2012)	Hacker + contexto	Práticas – características do ser hacker	Resistências + Outras formas de fazer política pública, influenciar na tomada de decisões, expressar politicamente
Ledesma (2015)	Hacking em outros meios	Práticas – características do ser hacker	Transposição do ser hacker para outros meios
Lima (2015)	Comunidade/grupo/coletivo	Práticas – características do ser hacker	Transposição do ser hacker para outros meios
Machado (2015)	Comunidade/grupo/coletivo	Relação com ferramentas e tecnologias da informação	Resistências + Outras formas de fazer política pública, influenciar na tomada de decisões, expressar politicamente
Maguire (2009)	Representações hackers	Relação com ferramentas e tecnologias da informação	Resistências
Mendoza (2002)	Potencialidades	Práticas – características do trabalho hacker	Outras formas de fazer política pública, influenciar na tomada de decisões, expressar politicamente
Mills (2012)	Hacking em outros meios	Relação com ferramentas e tecnologias da informação	Transposição do ser hacker para outros meios
Mota & Figueiredo Filho (2015)	Comunidade/grupo/coletivo	Relação com ferramentas e tecnologias da informação	Resistências
Mota, Hayashi & Fernandes (2016)	Hackers + outros atores	Relação com ferramentas e tecnologias da informação	Outras formas de fazer política pública, influenciar na tomada de decisões, expressar politicamente
Natansohn & Paz (2018)	Hacker + contexto	Práticas – características do trabalho hacker	Políticas do dia-a-dia
Natansohn (2018)	Representações hackers	Relação com ferramentas e tecnologias da informação	Políticas do dia-a-dia + Resistências
Nelson (1996)	Hackers + outros atores	Relação com ferramentas e tecnologias da informação	Resistências + Outras formas de fazer política pública, influenciar na tomada de decisões, expressar politicamente

Núñez (2017)	Comunidade/grupo/coletivo	Práticas – características do trabalho hacker	Políticas do dia-a-dia
Ojeda-Pérez et al. (2010)	Hackers + outros atores	Práticas – cibercrime	Violência e ilegalidade
Oviedo (2003)	Hacker + contexto	Relação com ferramentas e tecnologias da informação	Resistências + Outras formas de fazer política pública, influenciar na tomada de decisões, expressar politicamente
Parra (2012)	Hacker + contexto	Entusiasmo com tecnologias da informação	Outras formas de fazer política pública, influenciar na tomada de decisões, expressar politicamente
Paz (2013)	Comunidade/grupo/coletivo	Relação com ferramentas e tecnologias da informação	Políticas do dia-a-dia
Pederson (2016)	Hacking em outros meios	Relação com ferramentas e tecnologias da informação	Transposição do ser hacker para outros meios + Outras formas de fazer política pública, influenciar na tomada de decisões, expressar politicamente
Pérez-Bustos (2010a)	Comunidade/grupo/coletivo	Práticas – características do ser hacker	Políticas do dia-a-dia
Pérez-Bustos (2010b)	Comunidade/grupo/coletivo	Práticas – características do ser hacker	Políticas do dia-a-dia
Pino (2014)	Hacker + contexto	Relação com ferramentas e tecnologias da informação	Resistências
Pitman (2007)	Hackers + outros atores	Relação com ferramentas e tecnologias da informação	Resistências + Outras formas de fazer política pública, influenciar na tomada de decisões, expressar politicamente
Pretto (2010)	Potencialidades	Entusiasmo com tecnologias da informação	Transposição do ser hacker para outros meios
Redondo (2005)	Hacking em outros meios	Práticas – cibercrime	Resistências
Renno (2015)	Potencialidades	Práticas – características do trabalho hacker	Políticas do dia-a-dia
Rocha (2006)	Comunidade/grupo/coletivo	Entusiasmo com tecnologias da informação	Políticas do dia-a-dia
Rodríguez, Oduber & Mora (2017)	Representações hackers	Práticas – cibercrime	Violência e ilegalidade

Ronfeldt & Martínez (1997)	Hackers + outros atores	Práticas – características do ser hacker	Resistências + Outras formas de fazer política pública, influenciar na tomada de decisões, expressar politicamente
Ruiz, Segura & Quesada (2009)	Representações hackers	Práticas – cibercrime	Violência e ilegalidade
Schäfer (2015)	Hackers + outros atores	Práticas – características do ser hacker	Transposição do ser hacker para outros meios
Solórzano (2009)	Comunidade/grupo/coletivo	Práticas – características do trabalho hacker	Políticas do dia-a-dia
Suaza & Ortiz (2011)	Hacker + contexto	Práticas – características do trabalho hacker	Políticas do dia-a-dia
Suaza (2013)	Hacker + contexto	Práticas – características do trabalho hacker	Políticas do dia-a-dia
Tavares (2011)	Hackers + outros atores	Práticas – características do trabalho hacker	Outras formas de fazer política pública, influenciar na tomada de decisões, expressar politicamente
Träsel (2018)	Potencialidades	Práticas – características do trabalho hacker	Transposição do ser hacker para outros meios
Vasquéz (2013)	Hacker + contexto	Relação com ferramentas e tecnologias da informação	Outras formas de fazer política pública, influenciar na tomada de decisões, expressar politicamente
Villanueva & Olivera (2012)	Hackers + outros atores	Práticas – características do trabalho hacker	Outras formas de fazer política pública, influenciar na tomada de decisões, expressar politicamente
von Werder (2016)	Hackers + outros atores	Práticas – cibercrime	Resistências
Zanotti (2011)	Comunidade/grupo/coletivo	Práticas – características do trabalho hacker	Políticas do dia-a-dia
Zanotti (2014)	Comunidade/grupo/coletivo	Práticas – características do trabalho hacker	Políticas do dia-a-dia

Fonte: elaboração própria com base no conjunto de publicações selecionadas.