
# Múltiplas ontologias do ser hacker: experiências da CryptoRave

*Daniela Albini Pinheiro*[1]

**Resumo:** O que é ser hacker está em constante transformação e disputa. Ainda que em alguns espaços de prática e discussão algumas formas do ser hacker se configuraram hegemônicas – como a do hacker como um jovem com conhecimento técnico-científico que programa, constrói e se diverte transformando tecnologias eletrônicas e digitais para sua satisfação – tantas outras formas coexistem, convergem e divergem entre si. A CryptoRave é um dos espaços onde várias formas do ser hacker coexistem e entram em disputa. Neste trabalho, proponho refletir sobre a existência de múltiplas ontologias do ser hacker a partir das observações e vivências em duas edições brasileiras da CryptoRave (2017 e 2018), buscando considerar como essas formas se reafirmam e se contrapõem entre si e se relacionam àquelas identificadas na literatura dos estudos hackers.

**Palavras-chave:** hackers; CryptoRave; múltiplas ontologias

## Introdução

A proposta deste trabalho é trazer para a discussão a possibilidade da existência de múltiplas ontologias do ser hacker[2] no contexto de duas diferentes edições da CryptoRave

[1] Mestre e doutoranda pelo Programa de Pós-Graduação em Política Científica e Tecnológica da Universidade Estadual de Campinas (Unicamp).

[2] Neste documento, o termo hacker e suas derivações não serão grafados em itálico porque serão utilizadas massivamente e em conjunto a outras palavras em português. Outros termos em língua estrangeira continuarão sendo grafados em itálico, como exige a norma para trabalhos acadêmicos.

no Brasil a partir de vivências e anotações em mesas de discussão em que os palestrantes identificaram a si mesmos ou às suas atividades como hackers ou afirmaram discutir temáticas relacionadas. O exercício aqui realizado foi de tentar identificar convergências e divergências entre práticas e discussões como forma de entender o ordenamento de realidades dentro daquele espaço de onde emergem várias formas do ser hacker, relacionando-as, quando possível, àquelas identificadas na literatura dos estudos hackers.

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, conta com diversos espaços de discussão e oferece palestras e oficinas, *installfests*, entre outras atividades. 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[3].

A CryptoRave não deve ser compreendida 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, segurança e liberdade na Internet. Nesse sentido, ainda que que preenchido de discussões mais técnicas e especialistas em tecnologias da informação, o evento se configura como um espaço para identificação de discussões entre aqueles que, de alguma forma, estão envolvidos ou interessados nos desdobramentos do movimento hacker.

A proposta de trazer as múltiplas ontologias a este exercício permite entender que não existe apenas uma realidade e sua diferentes representações, mas que a realidade é múltipla e as entidades, situadas em algum lugar e tempo, emergem de práticas, discursos, eventos, materialidades e associações entre elementos heterogêneos (Mol, 2002; Souza, 2015). Especificamente sobre a CryptoRave, a noção das múltiplas ontologias se configurou como uma maneira de ordenar o que foi observado: que diferentes formas do ser hacker emergem e estabelecem diferentes relações entre si. Nesse sentido, a CryptoRave se torna uma arena de conflito em que o ser hacker é colocado em disputa em mesas de discussão, espaços livres e formas com que os diferentes grupos se engajam com as materialidades e práticas relacionadas à criptografia.

[3] Em 2017, houve a quarta edição da CryptoRave no Brasil, que aconteceu na Casa do Povo, na cidade de São Paulo (Brasil), 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.

Nas duas edições da CryptoRave foi possível identificar que o ser hacker esteve em constante transformação e disputa. Uma das formas do ser hacker, que despontou como hegemônica (Yates, Harris e Wilson, 2017), reforça a imagem de um jovem com conhecimento técnico-científico que programa, constrói e se diverte transformando tecnologias eletrônicas e digitais para sua satisfação. É principalmente com esta forma que outras entram em conflito tanto na CryptoRave quanto na literatura dos estudos hackers.

Tendo isso em consideração, primeiro busco esclarecer as origens desta forma hegemônica do ser hacker e, em seguida, apresento algumas das contestações existentes na literatura. Sigo, então, para as reflexões acerca de como formas do ser hacker emergem, se reafirmam e se contrapõem entre si no contexto da CryptoRave.

## Literatura e os verdadeiros 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 (*Massachusets 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 (Himanen, 2001; Castells, 2003; Levy, 2010). 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.

No livro de 1984 "*Hackers*", o autor Steven Levy os caracteriza como um grupo de indivíduos com história compartilhada ou engajamento em práticas comuns e, ainda que pertencentes a diferentes décadas e grupos de prática, apresentam elementos em comum: a materialidade concentrada no computador, suas redes e estruturas e a filosofia do compartilhamento, abertura e do fazer – chamada ética hacker, amplamente discutida, quando não reformulada ao longo dos anos por outros autores[4].

As primeiras literaturas sobre hackers, de acordo com Söderberg (2017), abriram frestas para o público espiar um universo desconhecido, exótico e contido em si mesmo

[4] Evangelista (2010) discute extensamente semelhanças e diferenças entre as éticas hacker apresentadas por diferentes autores (Raymond, 1996; 1999; Himanen, 2001; Levy, 2010) e quais suas implicações para o ser hacker.

e a apresentação dos magos dos computadores, objetivo explícito da obra de Steven Levy, é exemplo. "*Hackers*" é um livro de cunho jornalístico que 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).

Dentro dos primeiros autores dos estudos hackers, um dos principais é Eric Raymond. Seus textos são pervasivos 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 de 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 de Steve Levy que escreve uma narrativa, Eric Raymond parece assumir o lugar de porta-voz deste grupo de hackers e seus textos funcionam como manuais com prescrições para os indivíduos que queiram participar dessa comunidade[5]. Nesse

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

sentido, hackers são tecnicamente habilidosos, resolvem problemas, constroem coisas e acreditam na liberdade e na ajuda voluntária e apenas alguém que segue e acredita nisso pode ser reconhecido como um hacker (Raymond, 1996, revisão 1.51 out. 2017). Tão importante quanto, Raymond também demarca quem não deve ser considerado hacker: aqueles que se autodenominam assim ou invadem computadores e sistemas telefônicos, porque esses crimes não demandam nenhum conhecimento excepcional em tecnologia. Estes, segundo Raymond, são vistos com maus olhos e chamados de *crackers* pelos verdadeiros hackers.

Desta caracterização é possível extrair duas questões explicitadas por todo o texto e relevantes para entender a proposta de Raymond do ser hacker.

Primeiro, de 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.

Segundo, em relação a posicionamentos políticos, questão ilustrada pela história da disputa entre código aberto e *software* livre como apresentada por Eric Raymond (1996, revisão 1.51 out. 2017; 1999) que traz muito de sua perspectiva. 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. Ao mesmo tempo em que abre caminho para certas associações, Raymond encerra outros que envolvem o posicionamento político explícito, como defendido pelos movimentos relacionados 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.

Dessa forma, ao descrever como deve ser um hacker para 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), Raymond cria critérios

bastante restritos de inclusão e exclusão na comunidade. Isso tem implicações tanto para os estudos hackers, quanto para o campo empírico. No caso dos estudos hackers, Coleman (2016) aponta como principal implicação o fato de as pesquisas costumarem ter como o ponto de partida o estereótipo do hacker libertário e apolítico. Isso acontece 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 específicos circulam muito mais rápido que os de outras formas do ser hackers em decorrência da quantidade de recursos envolvidos. Segundo, porque existe uma escassez de estudos históricos sobre as múltiplas genealogias hacker e de pesquisas contemporâneas sobre diferenças regionais. A literatura identificada como pertencente ao segundo momento dos estudos hackers faz um esforço em expandir o conhecimento nos temas que Coleman (2016) considera incipientes.

Quanto ao campo empírico, existe uma persistência na recuperação e manutenção da proposta de Raymond. Evangelista (2010), ao tratar do Movimento do Software Livre[6] no Brasil em sua tese, mostra que apesar de ser possível identificar diferentes agendas, as discussões em fóruns virtuais e no Fórum Internacional de Software Livre (FISL) de 2008 reproduziam a disputa entre os grupos do *software* livre e código aberto. Tanto no movimento quanto no evento, notou-se algumas subdivisões entre o público: burocratas/ativistas e nerds/empresários, confundidos muitas vezes com pessoas com menos ou mais conhecimento técnico, respectivamente. Ainda que essas categorias se entrelacem de diversas formas, de acordo com Evangelista (2010) mesmo na organização do evento existe 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 subdivisões criadas pelos participantes do Movimento do Software Livre e do FISL ressoam diretamente as características que os "verdadeiros hackers" deveriam ter

[6] Evangelista (2010: 27) entende "*o movimento software livre como o conjunto de pessoas e instituições, públicas e privadas, que promovem publicamente e manifestam-se em favor da adoção maciça ou parcial de softwares livres e/ou do modelo de desenvolvimento aberto proporcionado pelas licenças livres*".

para o grupo de hackers sobre quem Raymond escreve: tecnicamente habilidoso e que entendem que a política é um obstáculo para as melhores soluções. Mas essa não é a única semelhança. Evangelista (2010) 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[7].

## A multiplicidade de origens e gêneros hackers

Existe um esforço na literatura mais recente dos estudos hackers de recuperação de 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.

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*

[7] A importância em trazer estes relatos e análises sobre o FISL ao se falar da CryptoRave porque parte do público e dos interesses são compartilhados. Os *softwares* livres são mais seguros que os proprietários porque é possível saber se e onde dados dos usuários são armazenados. Nos *softwares* proprietários e armazenagem em servidores privados, os dados ficam abertos à empresa ou governo ao qual o *software* ou servidor pertencem e os dados podem ser utilizados, compartilhados ou vendidos a quem interessar. Portanto, *softwares* e ferramentas livres são parte da tecnologia defendida e preferida também na CryptoRave.

> *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, 2013:17).

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. Faça-você-mesmo, rádios livres e piratas, bricolagem, MetaReciclagem, entre tantas outras são trazidas para compor os hackerismos. 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.

A América Latina também se torna local de recuperação de diferentes formas do ser hacker. Algumas das histórias datam os anos 1980 e 1990, como a dos ativistas culturais maias na Guatemala nas décadas que se recusavam a ser absorvidos pela cultura hegemônica e foram chamados de hackers maias por se apropriarem de tecnologias da informação e conhecimentos modernos normalmente não associados à sua cultura e os utilizaram para construir redes de comunicação e compartilhamento que se tornaram chave nas lutas do movimento de direitos culturais tradicionais (Nelson, 1996).

Os acontecimentos entrelaçados com o levante do Exército Zapatista de Libertação Nacional, que em 1994 ocupou uma série de cidades em Chiapas (México) são outro exemplo. Em resposta à ação violenta do governo mexicano ao movimento zapatista e em solidariedade com sua agenda política[8], dezenas de Organizações Não Governamentais (ONGs) e ativistas de direitos humanos de vários lugares do mundo invadiram eletronicamente o México e as Chiapas, utilizando a Internet como campo de batalha para

[8] A agenda política do movimento zapatista demandava respeito aos povos tradicionais, a renúncia do presidente atuante e a garantia de eleições justas, a realização de reformas sociais e econômicas (que implicariam na reversão do Tratado Norte-Americano de Livre Comércio) e o engajamento político da população (Ronfeldt e Martínez, 1997).

pressionar o governo mexicano a cessar-fogo, retirar as forças militares, abrir negociação com o movimento zapatistas e agilizar sua agenda política. De acordo com Ronfeldt e Martínez (1997), o levante zapatista e o engajamento de militante pela Internet foram um dos primeiros exemplos da capacidade de mobilização e utilização de táticas de guerra na rede para afetar conflitos sociais e ajudaram a posicionar hackers como atores políticos em nível transnacional.

O que torna possível diferenciar esse momento em relação ao anterior não é só o reconhecimento da alteridade, mas também a impossibilidade ignorar as diversas agendas e implicações políticas das práticas hacker (*hacker politics* em inglês) e sua influência nas políticas do dia-a-dia.

Söderberg (2017), nessa direção, retoma o ser hacker propagado por Eric Raymond e demanda que a comunidade acadêmica não ignore esse estereótipo ao tratar da política dos hackers porque mesmo em suas práticas e ética tecnologicamente deterministas existe engajamento político: a escolha por não engajar politicamente também é uma escolha política. Além disso, Söderberg (2017) insiste que ainda que hackers entendam que a mudança social depende do desenvolvimento tecnológico, sua tecnofilia não necessariamente minaria o potencial emancipatório dos hackerismos.

Ainda assim, houve uma passagem massiva dos hackers para a arena política na última década. Ao questionar sobre quais condições históricas, culturais e sociológicas impulsionaram esse movimento, Coleman (2017) argumenta que grandes acontecimentos críticos como os *Wikileaks*, a intensificação da ação do *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, que historicamente se unem e direcionam suas políticas por dois motivos: o compromisso compartilhado em preservar a autonomia dos indivíduos em pensar, agir e ser e a desconfiança em relação a instituições, governos e outras formas de poder centralizado.

Neste ponto entra o papel central da criptografia. Coleman (2017) defende que os atos de denúncia de Snowden 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 nos últimos cinco anos. As CryptoParties e as CrytoRaves surgem e se situam em um contexto de intensificação da vigilância massiva, em que Estados compram e consomem tecnologias cada vez mais complexas

para garantir controle da população, enquanto buscam encontrar formas de proibir e criminalizar resistências à invasão de privacidade (PITA, 2017).

## CryptoRave, políticas e o ser hacker

Como apontado anteriormente, a CryptoRave é um evento aberto e gratuito voltado para a disseminação da cultura e das ferramentas de privacidade, segurança, criptografia, hacking e liberdade na Internet que conta com diversos espaços de discussão e oferece palestras e oficinas, *installfests*, entre outras atividades.

Os indivíduos e grupos que propuseram e apresentam as atividades na CryptoRave das quais participei eram de uma grande diversidade 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.

A apresentação das pessoas no evento remeteu às descrições de Evangelista (2010) sobre a FISL. Roupas confortáveis, normalmente calças jeans, tênis, camisetas, muitas vezes com temática do Star Wars, Game of Thrones, Marvel, DC e outras referências à cultura pop. Algumas camisetas tinham estampas indicando alguma preferência específica por *software* e linguagem de programação e normalmente eram utilizadas por homens ali presentes. As mochilas também eram bastante comuns. Muitas pessoas levam seus computadores tanto para a *installfest* quanto para anotação e compartilhamento de arquivos.

Dentre as atividades disponíveis para as edições de 2017 e 2018 estavam palestras, mesas de debate em diversas 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 que a de 2017. A Cinemateca Brasileira em São Paulo é repleta de salas e auditórios com janelas amplas 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 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[9] e doze mesas de discussão[10]. No exercício de trazer as vivências e anotações da CryptoRave, procurei identificar fatores convergentes e divergentes que pudessem ajudar a entender o ordenamento de realidades dentro daquele espaço de onde emergem as várias formas do ser hacker, relacionando-as, quando possível, àquelas identificadas na literatura dos estudos hackers. Nessa direção, duas questões se entrelaçam: por que usar criptografia e por que estar na CryptoRave.

[9] 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.

[10] Às mesas seguem a trilha e ano da edição: "De volta ao cyberfeminismo" (gênero, 2017), "Criptografia e agroecologia" (política, 2017), "(Cyber)espaços seguros: redes autônomas feministas" (gênero, 2017), "A GDPR chegou!! Como se preparar?" (privacidade, 2018), "*Investigación y desarrollo del proyecto Tor*" (anonimato, 2018), Criptografia, privacidade e política (política, 2018), SaferManas (gênero, 2018), Ciberseguras (gênero, 2018), "Cidadão quem? Usos e abusos da biometria no Brasil" (privacidade, 2018), "*Whatsapp y comunidades vulnerables*" (segurança, 2018), "*Leakydata*" (hacking, 2018) e "A economia psíquica dos algoritmos" (política, 2018).

## Por que usar 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 em comum da prática e do interesse dos grupos presentes na CryptoRave de onde emergiram dois temas constantemente discutido durante as mesas: o contexto que levou à necessidade crescente em utilizar criptografia e as tecnologias devem ser utilizadas.

Em termos de contexto, houve grande convergência no reconhecimento da existência de uma disparidade de poder entre os indivíduos e o Estado/grandes corporações em se tratando da privacidade, que toma formas específicas no contexto de vigilância em massa, uma vez que a centralização de informações pelo Estado e controle da conectividade por grandes corporações podem rapidamente se tornar formas de bloquear livre expressão de pensamento e dificultar organização política. Isso corrobora, particularmente, com a perspectiva de Coleman (2017) de que a intensificação da mobilização política dos hackers e do uso de ferramentas de criptografia vêm com o compromisso compartilhado de preservar formas de pensar, ser e interagir autonomamente.

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).

Como exemplo, a discussão da mesa "Criptografia e agroecologia" (trilha política, 2017) reforçou 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. Quando a circulação de informação sobre pessoas, protestos, ativismos e outras lutas são cerceadas e ficam centralizadas e sob controle das empresas capitalistas e governos conservadores, a população se torna cada vez mais vulnerável e sob controle das empresas capitalistas e governos, 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).

A importância da manutenção da liberdade do indivíduo e da circulação de informação é um dos pontos de intersecção com a forma do ser hacker já apresentada (Raymond, 1996, revisão 1.51 out. 2017; Coleman, 2016). Porém, ainda que existam na CryptoRave lugares e atividades em que liberdade significa a exploração livre de habilidades técnicas (como as mesas com foco em tecnologia e o *installfest*), percepção conectada ao hacker libertário, ao contrário dos relatos sobre o FISL de Evangelista (2010), na CryptoRave parece ser impossível desassociar a criptografia das questões políticas. Todas as discussões serviram de espaço para denúncias de invasão de privacidade e violências contra direitos individuais e para o compartilhamento do sentimento de urgência em difundir e utilizar ferramentas de criptografia e segurança.

Na mesa "*Whatsapp y comunidades vulnerables*", especificamente, a criptografia e os movimentos sociais foram conectados. Representando os *Derechos Digitales* – organização latino-americana independente e sem fins lucrativos que busca desenvolver, defender e promover os direitos humanos no meio digital – a discussão ocorreu entorno da *Operación Huracán* em 2017, em que oito líderes mapuches foram detidos pela polícia chilena sob pretexto de envolvimento em terrorismo captado em mensagens de WhatsApp interceptadas por um *software* forense. Em realidade, na tentativa de impedir mais protestos, as provas foram forjadas utilizando arquivos .txt e num momento em que o WhatsApp já utilizava o Protocolo Signal para criptografia ponta a ponta, o que dificulta a obtenção das conversas entre usuários.

Um dos exemplos mais interessantes de denúncia sobre a concentração de informações nas mãos de governos veio da mesa "*Leakydata*" (trilha hacking, 2018), em que o palestrante contou sua brincadeira em testar quais informações seriam possíveis de extrair com o *Freedom of Information Act* (FOIA) de um documento do governo estadunidense mesmo quando ele já foi vazado. A obtenção do FOIA de um *wikileak* levou meses, primeiro porque o pedido foi repetidamente negado e, segundo, porque veio quase completamente rasurado devido ao alto nível de segurança da informação requerida.

Na CryptoRave, foi possível observar que liberdade ganhou outros sentidos além daqueles relacionados a livre circulação de informação e ao direito de transformar códigos e tecnologias: os de proteção e de direito de existir. Nesse ponto surgiram algumas divergências entre os participantes da CryptoRave tanto em relação às ferramentas quanto ao que significa proteger e existir, principalmente nas intersecções com movimentos sociais e coletivos feministas.

Sasha Costanza-Chock[11] 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 por exposição de dados pessoais, invasão de privacidade, perseguição e outras práticas abusivas de parceiros através de aplicativos, identificação de pessoas nos protestos por meio de torres policiais disfarçadas de pontos de Internet, entre outros exemplos.

Essa perspectiva foi reforçada também pelo coletivo feminista MariaLab e o projeto Vedetas, em "(Ciber)espaços seguros: redes autônomas feministas" (trilha gênero, 2017). É dessa problematização que surgem outros motivos para usar criptografia, *software* livre e outras ferramentas. Como os corpos femininos vivenciam de outra forma a vigilância, é essencial que mulheres tenham conhecimento sobre segurança da informação e autonomia em relação à infraestrutura de redes para se protegerem e, se necessário, contra-atacarem. O argumento é que quando as tecnologias são autônomas e comunitárias, como a infraestrutura que propuseram, são as próprias mulheres que dominam o técnico e controlam o funcionamento da rede e gerenciam seu conteúdo, diminuindo sua vulnerabilidade em relação à dependência de aliados masculinos, à dominação das corporações capitalistas e ao controle do Estado.

Isso evidencia, portanto, que ainda que possa haver posicionamentos tecnologicamente deterministas nas mesas e discussões, eles são inerentemente políticos (Söderberg, 2017). Para esses coletivos e indivíduos a tecnologia não é neutra: os interesses, valores e visões de mundo de quem as desenvolve está incorporado na tecnologia e emergem de sua utilização e implica em diferentes soluções e associações. A proposta tecnológica da MariaLab seria, portanto, uma forma de forjar relações que emergem do desenvolvimento e da utilização da tecnologia que vão além daquelas mercantis e a luta está em participar na construção das próprias tecnologias de proteção.

A discussão sobre associações entre tecnologias e desenvolvedores/usuários e a não neutralidade da tecnologia não ficou circunscrita aos debates feministas. Foi bastante

[11] 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.

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 criptografia ponta-a-ponta para mensagem para escrita, voz e vídeo bastante segura. Os posicionamentos sobre o protocolo mudaram 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. A própria criptografia como ferramenta foi colocada em xeque algumas vezes quando surgiam assuntos 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).

Portanto, ainda que haja concordância sobre um contexto mais amplo e sobre a necessidade do uso da criptografia, os motivos divergiram para cada grupo, dependendo de sua identificação dentro desse contexto. O mesmo aconteceu em relação ao porquê estar na CryptoRave.

## Por que estar na CryptoRave?

A experiência na CryptoRave começou com um causo: chegando na Casa do Povo, fui informada de que um garoto 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, 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. A escolha das integrantes do projeto Vedetas em utilizar apenas artigos, pronomes e substantivos no feminino para suas tecnologias também é um exemplo. Brincar com os nomes das coisas é muito comum na cultura hacker 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 e a parte técnica ser comumente atribuída aos homens tanto em terminologia quanto em imaginário ("o técnico", "o cara da manutenção").

Estar na CryptoRave é dividir espaço e tempo com todos os interessados em denunciar quem utiliza das mais variadas tecnologias da informação para ameaçar a privacidade e a segurança de diferentes indivíduos, em defender o uso da criptografia e outras ferramentas e em difundir conhecimentos sobre essas tecnologias (Pita, 2017), sejam eles hackers, desenvolvedores, acadêmicos, ativista, gestores, etc.

As justificativas para estar na CryptoRave, em sua maioria, entrelaçaram-se de alguma forma com o sentimento de que todos ali precisavam arregimentar tecnologias da informação porque eram afetados pela vigilância em massa e centralização da informação nas mãos de governos e grandes corporações, portanto, uma resposta ao contexto amplamente discutido nas mesas. Dois casos se mostraram divergentes neste aspecto.

O primeiro caso, a mesa "Criptografia e agroecologia" (trilha política, 2017), divergiu dos outros por tirar o foco das tecnologias da informação. Grande parte do tempo de fala de uma das integrantes da mesa, pertencente a Sempreviva Organização Feminista (SOF), foi utilizado para justificar porque uma atividade como a agroecologia pertencia a um evento como a CrytoRave 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 e o digital acabam se esquecendo de que outras práticas também carregam conhecimento sobre tecnologias. A agroecologia é um exemplo, uma vez que suas práticas são derivadas de conhecimentos tradicionais passados por gerações e 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. 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. 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 comparada ao movimento hacker, que existe para criar alternativas para proteção de dados e mediações de suas relações através da utilização de criptografia e *software* livre, desenvolvidos de forma diferente daquela capitalista, com base na liberdade, solidariedade e colaboração.

O segundo caso divergiu dos demais por refletir um comportamento específico entre pessoas sem ou com pouco conhecimento técnico. Ainda que fosse reforçado constantemente a necessidade de toda sociedade civil de resistir à vigilância e utilizar ferramentas de criptografia, em todas as atividades que participei, sempre que alguém se colocava para desconhecidos, acabava incluindo em sua apresentação o comentário "não sou da área de tecnologias", principalmente nos casos de acadêmicos ou interessados na cultura hacker, porém nunca os ativistas. Jargões e outros termos técnicos eram usados livremente durante as mesas e não havia questionamento sobre seus significados, propriedades ou objetivos. O sentimento de não-pertencimento parecia emergir do medo de ser identificado como intruso.

Os dois casos mostram que formas do ser hacker coexistem, mas entram em conflito quando precisam se reafirmar, combater ou reproduzir algumas características para ganhar espaço junto de outras formas que buscam delimitar o que pode ou não ser considerado hacker ou hackear. No caso da CryptoRave, ao analisar as falas e como foram feitas, outras formas do ser hacker tomaram como interlocutora 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).

No primeiro caso houve um combate entre formas do ser hacker: quando as práticas solidárias e colaborativas são resistência e subversão a um sistema que controla e oprime, ali existe um movimento hacker. Nesta realidade, é contraditório ao ser hacker criar limites apenas porque são outros conhecimentos e tecnologias utilizados nas práticas. Ser hacker é criar alternativas para sobreviver e subverter a lógica de mercado, pro-

curando novos espaços para existir. Já no segundo houve uma reprodução do estereótipo e do preconceito dos "verdadeiros hackers" foi imposto aos não-especialistas em tecnologia da informação em si mesmos, refletido no sentimento de não pertencimento. Ainda assim, há invasão de espaço: os intrusos surgem para ocupar lugar junto dos "verdadeiros hackers" nas discussões e mesas, tornando a CryptoRave um espaço aberto de fato.

## Considerações finais

O exercício de pensar com a CryptoRave e a existência de múltiplas ontologias do ser hacker mostrou-se bastante complexo. A CryptoRave se configurou como uma arena de conflito em que o ser hacker foi colocado em disputa a todo momento, principalmente em relação às formas com que os diferentes grupos se engajam com as materialidades e práticas relacionadas à criptografia. Com esse exercício, foi possível identificar uma série de outras temáticas e relações que emergem da CryptoRave, como o determinismo tecnológico, a neutralidade da tecnologia, questões de gênero e diferentes políticas que também estão sendo discutidas na literatura dos estudos hackers

Ao buscar identificar convergências e divergências entre práticas e discussões para entender o ordenamento de realidades nas edições de 2017 e 2018 da CryptoRave, foi possível observar a emergência de diferentes formas do ser hacker e o estabelecimento de diferentes relações entre elas.

Entre as principais convergências observadas estão a concordância sobre a existência de um contexto mais amplo de vigilância em massa e centralização da informação nas mãos de governos e grandes corporações que torna necessário o uso da criptografia, o compromisso de preservar formas de pensar, ser e interagir autonomamente e o caráter político dos posicionamentos ali declarados, ainda que tecnologicamente deterministas.

As divergências, porém, evidenciaram a multiplicidade de formas do ser hacker e a complexidade das relações entre elas. Questões que poderiam ser consideradas como estabelecidas naquele espaço, como a liberdade de expressão e de fazer ganham outros significados nas intersecções com movimentos sociais e coletivos feministas, assim como materialidades e práticas são colocados no centro do conflito quando grupos de leigos em tecnologias da informação começam a ocupar e se apropriar do espaço da CryptoRave.

## Referências


CASTELLS, Manuel. 2003. **A galáxia da Internet**: reflexões sobre a Internet, os negócios e a sociedade. Rio de Janeiro: J. Zahar.

COLEMAN, Gabriella. 2013. **Coding freedom**: the ethics and aesthetics of hacking. Princeton: Princeton University Press.

_____. 2016. Hacker. In: PETERS, Benjamin (Ed.). **Digital Keywords**: a vocabulary of information society and culture. Princeton: Princeton University Press, pp. 158-172.

_____. 2017. From Internet Farming to Weapons of the Geek. **Current Anthropology**, 58 (15): S91-S102.

COLEMAN, Gabriella, GOLUB, Alex. 2008. Hacker practice: moral genres and the cultural articulation of liberalism. **Anthropological Theory**, 8(3): 255-277.

EVANGELISTA, Rafael de Almeida. 2010. **Traidores do movimento**: política, cultura, ideologia e trabalho no software livre. Campinas: Unicamp, 2010. 240 p.

HIMANEN, Pekka. 2001. **A ética dos hackers e o espírito da era da informação**. Tradução Fernanda Wolff. Rio de Janeiro: Campus.

KELTY, Christopher. 2005. Geeks, Social Imaginaries, and Recursive Publics. **Cultural Anthropology**, 20(2): 185-214.

LEVY, Steven. 2010. **Hackers**: heroes of the computer revolution. Sebastopol: O'Reilly Media (Trabalho originalmente publicado em 1984).

MOL, Annemarie. 2002. **The body multiple**: ontology in medical practice. Durham e Londres: Duke University Press.

NELSON, Diana M. 1996. Maya Hackers and the Cyberspatialized Nation-State: Modernity, Ethnostalgia, and a Lizard Queen in Guatemala. **Cultural Anthropology**, 11(3): 287-308.

PITA, Marina. 2017. 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. 1996 (revisão 1.51 out. 2017). **How To Become A Hacker**. Disponível em: <http://catb.org/~esr/faqs/hacker-howto.html>. Último acesso em: 7 nov. 2018.

_____. **The Cathedral and the Bazaar**. 1999. Disponível em: < http://www.unterstein.net/su/docs/CathBaz.pdf >. Último acesso em: 7 nov. 2018.

RONFELDT, David, MARTÍNEZ, Armando. 1997. A Comment on theZapatista "Netwar". In: ARQUILLA, John, RONFELDT, David. (Eds.) **In Athena's Camp**: preparing for conflict in the information age. Santa Monica: RAND Corporation, pp.369-391.

SÖDERBERG, Johan. 2013. Determining social change: The role of technological determinism in the collective action framing of hackers. **New media & society**, 15(8): 1277-1293.

_____. 2017. Inquiring Hacking as Politics: A New Departure in Hacker Studies? **Science, Technology, & Human Values**, 42(5): 969-980.

SOUZA, Iara M. A. 2017. A noção de ontologias múltiplas e suas consequências políticas. **ILHA**, 17(2): 49-73.

YATES, Julian. S., HARRIS, Leila. M., WILSON, Nicole. J. 2017. Multiple ontologies of water: Politics, conflict and implications for governance. **Environment and Planning D: Society and Space**, 35(5): 797-815.