

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL  
INSTITUTO DE FILOSOFIA E CIÊNCIAS HUMANAS  
DEPARTAMENTO DE SOCIOLOGIA

EMÍLIO FREGAPANI TOSCANI

**CRYPTORAVE 2016/2017: A POLITIZAÇÃO DA PRIVACIDADE NO MAIOR  
EVENTO SOBRE PRIVACIDADE, SEGURANÇA E ANONÍMIA DO BRASIL**

Porto Alegre

2017

EMÍLIO FREGAPANI TOSCANI

**CRYPTORAVE 2016/2017: A POLITIZAÇÃO DA PRIVACIDADE NO MAIOR  
EVENTO SOBRE PRIVACIDADE, SEGURANÇA E ANONÍMIA DO BRASIL**

Trabalho de Conclusão de Curso de Ciências Sociais apresentado ao Departamento de Sociologia do Instituto de Filosofia e Ciências Humanas da Universidade Federal do Rio Grande do Sul como requisito para a obtenção do grau de Bacharel em Ciências Sociais.

Orientador: Profº Drº Marcelo Kunrath Silva  
Coorientador: Eduardo Georjão Fernandes

Porto Alegre

2017

### CIP - Catalogação na Publicação

Toscani, Emílio Fregapani

CryptoRave 2016/2017: A politização da privacidade no maior evento brasileiro sobre privacidade, segurança e anonimidade do Brasil / Emílio Fregapani Toscani. -- 2017.

66 f.

Orientador: Marcelo Kunrath Silva.

Coorientador: Eduardo Georjão Fernandes.

Trabalho de conclusão de curso (Graduação) -- Universidade Federal do Rio Grande do Sul, Instituto de Filosofia e Ciências Humanas, Bacharelado em Filosofia, Porto Alegre, BR-RS, 2017.

1. Internet. 2. Ciberativismo. 3. Tecnopolítica. 4. Privacidade. 5. Criptografia. I. Silva, Marcelo Kunrath, orient. II. Fernandes, Eduardo Georjão, coorient. III. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da UFRGS com os dados fornecidos pelo(a) autor(a).

## **AGRADECIMENTOS**

Dedico este trabalho aos meus pais, Humberto Toscani e Marisa Fregapani, que apoiaram desde o primeiro momento a minha decisão em cursar ciências sociais. Agradeço aos organizadores da *CryptoRave*, ao grupo de pesquisa GPACE, aos meus colegas de faculdade e aos meus amigos, seja pelas conversas, pelo tempo dedicado a mim ou por qualquer outro motivo que venha a calhar.

## RESUMO

O presente trabalho tem como objeto central a análise da *CryptoRave*, com foco nas edições ocorridas nos anos de 2016 e 2017. Faz-se importante a análise da *CryptoRave* pelo fato da mesma servir como um exemplo para uma forma diferenciada de ativismo, onde o foco é no empoderamento do indivíduo via criptografia e na politização de questões como privacidade e vigilância. A *CryptoRave* é um evento realizado anualmente em São Paulo de forma coletiva por doações de interessados. Neste evento, via palestras, *workshops* e aulas abertas, questões relacionadas com privacidade, luta por direitos na Internet, criptografia e luta contra a vigilância *on-line* são apresentadas de forma a ampliar o debate sobre o direito da privacidade e o uso das tecnologias no Brasil. A metodologia utilizada para a pesquisa envolveu o estudo de textos publicados sobre as temáticas tratadas pelo evento, entrevista com os organizadores e participação no evento com um estudo de caso na edição de 2017. A entrevista foi realizada em 2016 via e-mail e foi recolhido material oficial divulgado pelo coletivo organizador. Após a análise da história da luta pela privacidade, do ciberativismo e de suas manifestações, temos como conclusão que a *CryptoRave* cumpre seu papel de evento educativo e politizador ao transformar a privacidade em problema social e focar no ensino de forma individual. Ao sugerir a tecnopolítica como solução e mostrar como a criptografia pode ajudar pessoas na sua proteção, o objetivo do evento se cumpre seguindo dogmas ciberativistas para o empoderamento dos participantes.

**Palavras-chave:** Internet, Tecnopolítica, Ciberativismo, Privacidade, Criptografia, Eventos, Educação.

## ABSTRACT

The main objective of this work is the analysis of *CryptoRave*, focusing on the editions that took place in the years 2016 and 2017. The *CryptoRave* analysis is important because it serves as an example for a differentiated form of activism, where the focus is on the individual's empowerment through cryptography and the politicization of issues such as privacy and surveillance. *CryptoRave* is an event held annually in São Paulo collectively by donations of interested parties. In this event, via lectures, workshops and open classes, issues related to privacy, fight for rights on the Internet, encryption and fight against *on-line* surveillance are presented in order to broaden the debate on the right of privacy and the use of technologies in the Brazil. The methodology used for the research involved the study of published texts on the themes dealt with by the event, interview with the organizers and participation in the event with a case study in the 2017 edition. The interview was conducted in 2016 via e-mail and official material released by the collective organizer was collected. After analyzing the history of the struggle for privacy, cyber-activism and its manifestations, we conclude that *CryptoRave* fulfills its role as an educational and politicizing event by transforming privacy into a social problem and focusing on teaching individually. By suggesting technopolitics as a solution and showing how encryption can help people in their protection, the purpose of the event is met by following cyber-security dogmas for the empowerment of participants.

**Keywords:** Internet, Technopolitics, Cyber-activism, Privacy, Cryptography, Events, Education.

## **LISTA DE ABREVIATURAS E SIGLAS**

ARPA – Advanced Research Projects Agency Network

BR – Brasil

ECT – Estudos de Ciência e Tecnologia

EUA – Estados Unidos da América

FISL – Fórum Internacional do Software Livre

STS – Science and Technology Studies

TOR – The Onion Router

URSS – União das Repúblicas Socialistas Soviéticas

WWW – World Wide Web

## SUMÁRIO

1. INTRODUÇÃO.....	8
2. POLÍTICA, PRIVACIDADE E INTERNET.....	12
3. CIBERATIVISMO, MANIFESTAÇÕES E EVENTOS BRASILEIROS – BASES DA <i>CRYPTORAVE</i> .....	17
4. <i>CRYPTORAVE</i> – SEGURANÇA, CRIPTOGRAFIA, <i>HACKING</i> , ANONIMATO, PRIVACIDADE E LIBERDADE NA REDE.....	23
4.1 Espaço Aaron Swartz: Regulamentação da Internet, anonimia e direitos humanos.....	28
4.2 Espaço Chelsea Manning: limites e novidades da criptografia.....	34
4.3 Espaço Edward Snowden: mergulhando nas fronteiras da Internet.....	38
4.4 Espaço Alan Turing: ferramentas e oficinas necessárias para a segurança na rede.....	40
4.5 Espaço Ada Lovelace: Gênero, sexualidade e feminismo na <i>CryptoRave</i> .....	41
4.6 Espaço Ian Murdock: segurança digital pessoal.....;	45
5. ANÁLISE DA <i>CRYPTORAVE</i> .....	48
6. CONSIDERAÇÕES FINAIS.....	56
REFERÊNCIAS.....	59
APÊNDICE “A”: Entrevista sobre a <i>CryptoRave</i> para o coletivo organizador realizada em 2016. ....	61



## 1. INTRODUÇÃO

Este trabalho de conclusão de curso em Ciências Sociais tem como o objetivo central a análise de como a *CryptoRave* - um evento onde a técnica e a política são mobilizadas em conjunto para a luta contra a vigilância - politiza a questão da privacidade ao apresentar para seu público diversas temáticas que abordam o estudo da criptografia, a luta contra a vigilância do Estado e o direito à privacidade<sup>1</sup>.

A politização será entendida e abordada neste trabalho em dois sentidos, o primeiro relacionado a como um objeto se transforma em problema sócia/público/político, na aceção de quais ocorrências históricas e mecanismos são trazidos a tona para fazer com que os participantes do evento entendam seus temas problemáticos centrais – como a falta de privacidade na Internet – como algo a ser estudado, entendido e, com a criação de novas ideias, superado. E o segundo sentido tem como foco a criação de métodos para agir frente às tais temáticas problemáticas.

A noção de privacidade, como direito à reserva de informações pessoais e da própria vida privada, é algo que se manifesta como uma questão que foi discutida primeiramente entre os séculos XVII e XVIII desde então sofreu drásticas transformações em sua essência; mudando de uma quase inexistência, para uma das questões mais debatidas no século XXI. (SILVEIRA, 2011, p. 4)

Neste trabalho também é explorado como a evolução da privacidade ocorre e como ela é apropriada para discussões sobre temáticas da Internet. Conceito que será considerado pauta política na *CryptoRave*, um dos maiores eventos sobre criptografia, luta contra a vigilância e segurança digital do mundo, entendida neste trabalho.

Esse evento nasceu em 2013 sob o nome apenas de *CryptoParty* São Paulo e desde então contou com edições anuais, assumindo o nome de *CryptoRave* em 2014. Sua última edição ocorreu entre o dia 5 e 6 de maio de 2017, na Casa do Povo<sup>2</sup> em São Paulo; e tanto esta quanto as prévias edições seguem um modelo

---

<sup>1</sup> A luta pelo direito à privacidade, que será citada neste trabalho diversas vezes, será tomada aqui por como as pessoas podem resistir à interferência, muitas vezes negativa, que a Internet pode ter na vida delas, principalmente no que diz respeito à coleta e comercialização de dados pessoais. (BRUNO, 2013, p. 01)

<sup>2</sup> Disponível em: <[casadopovo.org.br/](http://casadopovo.org.br/)> Acesso em 08 de abril de 2017.

que envolve na maioria das vezes: horizontalidade do saber<sup>3</sup>, financiamento coletivo do evento, trilhas de discussão, palestrantes do Brasil e do mundo, *workshops*, festa na madrugada e muitas outras atividades. Neste trabalho o foco será direcionado para as edições de 2016 e a de 2017 principalmente pelo fato delas possuírem maior quantidade de informações disponíveis.

Devido ao número oficial dos participantes de cada ano não ser divulgado pelo coletivo, temos como dados apenas as pessoas que confirmaram presença no evento do Facebook e quem colaborou com o financiamento coletivo. Em 2016 foram quinhentos e quarenta e sete apoiadores e mais de mil confirmados no evento, e no ano de 2017 foram seiscentos e um apoiadores e mais de mil e duzentos no evento confirmados.

Considerado pelos organizadores um esforço coletivo, sua última edição possuiu cinco coletivos centrais organizadores e muitos ajudantes voluntários. Os coletivos envolvidos foram os Actantes<sup>4</sup>, a Escola de Ativismo<sup>5</sup>, o Intervozes<sup>6</sup>, o Saravá e o Encripta<sup>7</sup>. Além disso, todo o dinheiro relacionado ao evento e seus custos periféricos foi coletado em um financiamento coletivo *on-line*.

Nesse sentido, esta pesquisa será organizada de modo a dividir a temática em quatro tópicos centrais para os conteúdos que aqui serão tratados, de forma que o leitor se situará na realidade da Internet e de suas relações com a sociedade, antes de mergulhar no evento. São as divisões: capítulo 2, onde tratamos sobre questões relacionadas à política, privacidade e Internet. Dentro disso, os fundamentos da concepção e evolução do conceito de “privacidade”, suas implicações e sua relação direta com a criação e expansão da Internet. Também, como a privacidade se tornou “politizada” e de que maneira esta discussão percorre o Brasil; capítulo 3, no qual examinamos a cibercultura e suas manifestações como instrumento de mobilização política da técnica para uma luta contra a vigilância *on-line*; capítulo 4, que explora o evento em si e seus encadeamentos para a discussão sobre privacidade e vigilância *on-line*; capítulo 5, com o foco na análise do evento e suas implicações.

---

<sup>3</sup> O saber não deve ser hierarquizado, o conhecimento deve ser livre e igualmente distribuído a todos.

<sup>4</sup> Disponível em: <<http://actantes.org.br/>> Acesso em 30 de novembro de 2016.

<sup>5</sup> Disponível em: <<https://ativismo.org.br/>> Acesso em 30 de novembro de 2016.

<sup>6</sup> Disponível em: <<http://intervozes.org.br/>> Acesso em 30 de novembro de 2016.

<sup>7</sup> Disponível em: <<https://encripta.org/>> Acesso em 10 de janeiro de 2017.

A abordagem encontrada para melhor trabalhar essa temática, que envolve um estudo de questões históricas, políticas e um evento organizado coletivamente que relaciona as ciências humanas e sociais com a tecnologia e o virtual foi utilizar diversos textos sobre questões relacionadas à vigilância, à privacidade e à liberdade *on-line* para obter uma construção histórica de como as bases e a evolução da discussão dos tópicos citados se deram para então chegar ao evento explorado.

A metodologia para a realização do texto foi realizada em quatro partes centrais: na primeira parte, ocorreu o recolhimento de informações sobre criptografia, história da luta contra a vigilância e a favor da privacidade e o evento em si, sendo utilizados livros, artigos e notícias *on-line* e *off-line* em fontes documentais.

Durante a segunda parte foi realizada uma entrevista via e-mail em 2016 com os organizadores do evento. Esta entrevista versou as mais diversas questões, desde como é feita a organização do evento até perguntas sobre os participantes e palestrantes e esta disponível no anexo “A” do trabalho.

Os dados sobre a *CryptoRave* de 2016 foram recolhidos mediante à supracitada entrevista e pesquisa em textos, notícias e vídeos sobre o evento. Todas as informações sobre palestras de 2016 abordadas no trabalho são frutos de pesquisa em fontes relacionadas diretamente aos organizadores e com aprovação dos mesmos.

Na terceira parte os dados da *CryptoRave* de 2017 foram recolhidos durante o evento, o qual participei e nele assisti seis palestras, todas serão citadas mais a frente. Na última parte, foi feita a elaboração da escrita, com foco nos artigos lidos e estudos realizados.

Como objetivo central do trabalho temos a análise de como a *CryptoRave*, um evento onde a técnica e a política são mobilizadas em conjunto para a luta contra a vigilância, politiza a questão da privacidade.

Dentro dos objetivos específicos, podemos denotar alguns, como:

a. Por meio da identificação dos espaços de discussão construídos, das temáticas propostas e dos palestrantes convidados, verificar como a *CryptoRave* aborda a questão da privacidade.

b. Com base na observação *in loco* de uma edição da *CryptoRave*, verificar como se dão a organização dos espaços de discussão e a interação entre organizadores e participantes no curso do evento.

c. Via entrevista, identificar as motivações dos organizadores, quais seus objetivos e a avaliação que eles fazem dos impactos do evento.

A maior dificuldade na elaboração deste texto foi o ainda incipiente diálogo das ciências sociais com as áreas dedicadas ao estudo da Internet, como a comunicação, as ciências da computação, entre outras no Brasil. Apesar de haver estudos brasileiros tentando relacionar ciências sociais e Internet, poucos tratam especificamente das temáticas de privacidade/vigilância, ou seja, das consequências de “controle” ligadas ao desenvolvimento das tecnologias (a maioria dos estudos preocupa-se mais com as “potencialidades” das tecnologias).

Para além da questão relacionada diretamente a pouca relação citada acima, existe uma justificativa social no apresentar desta temática, já que no Brasil é frágil a legislação sobre privacidade, no ponto de que não há legislação específica sobre proteção a dados pessoais. Sendo este um tópico considerado pelo autor de extrema necessidade de apresentação ao público leitor.

## **2. POLÍTICA, PRIVACIDADE E INTERNET**

Para entendermos como o evento denominado de *CryptoRave* foi criado, se faz necessária uma análise na qual dois tópicos, a política e a privacidade, são relacionados a uma temática central: a Internet. Juntos, eles são pilares da discussão que hoje movimenta grande parte do ativismo mundial e da luta por direitos *on-line*.

A palavra “privacidade” tem seu significado neste trabalho empregado como atualmente é entendido: o direito à reserva de informações pessoais e da própria vida privada, em resumo "o direito de ser deixado em paz". Esta definição tem sua possível origem no estudo do jurista norte-americano Louis Brandeis um dos responsáveis pela criação do conceito de direito à privacidade. (WARREN; BRANDEIS, 1890)

Já a Internet terá como significado não apenas uma rede de máquinas interligadas por cabos de fibra óptica entre os continentes e oceanos e sim, um mecanismo que, para existir, mobiliza diversas questões sociais, políticas, econômicas e científicas anteriormente. Por trás do advento da rede mundial de computadores existe uma rede sociotécnica, que envolve desde os usuários da mesma, os computadores, os eventos nascidos dela e todas suas mais diversas finalidades e possibilidades. (LATOURE, 1994, p. 11)

Tal sistema global de redes de computadores, que hoje em dia é conhecido como Internet e se encontra conectado à vida de 3,2 bilhões de pessoas no mundo<sup>8</sup> (o que corresponde ao índice de 44% da população mundial) e a mais de 50% das casas brasileiras<sup>9</sup> passou por um longo caminho desde sua criação até seu ponto atual. Smartphones, redes sociais, eventos e movimentos organizados digitalmente, há menos de meio século não eram nada além de uma fantasia que não existia nem nos mais psicodélicos filmes.

O nascer da Internet se dá num esforço acadêmico financiado pelo IPTO (*Information Processing Techniques Office*) do governo dos Estados Unidos da América relacionada ao esforço de mudança de paradigma para a comunicação através de comutação de pacotes no momento do florescimento do "*time-sharing*" com o objetivo de poder usar os computadores sem precisar de processamento em lote.

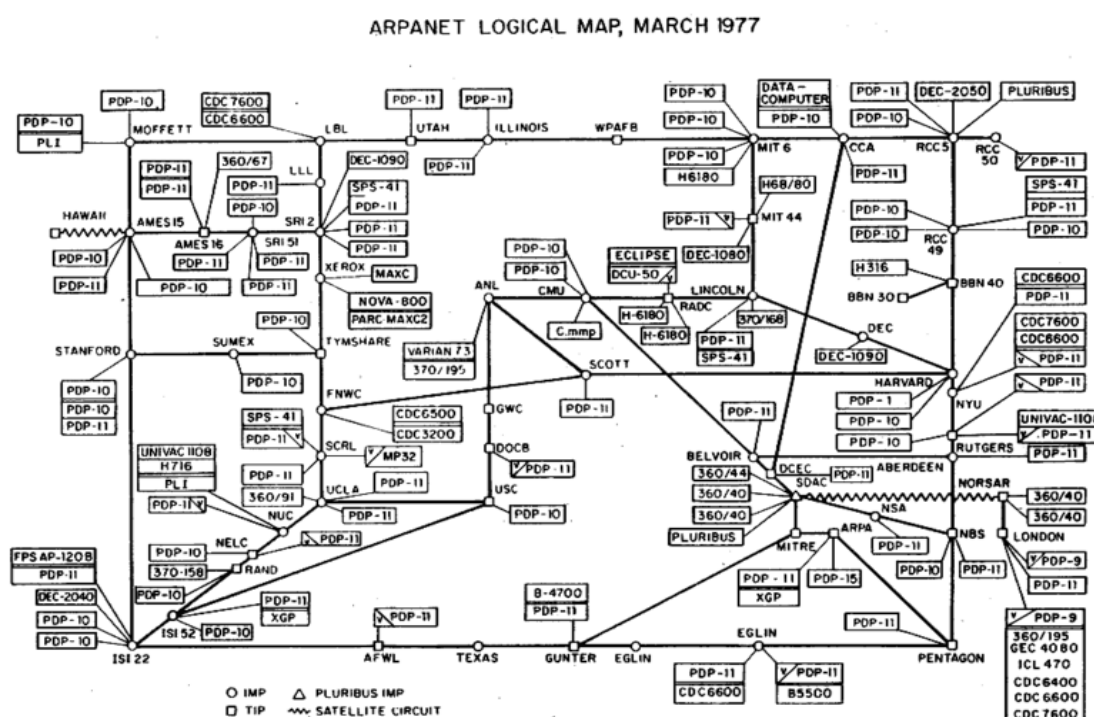
---

<sup>8</sup> Disponível em <<https://fbnewsroomus.files.wordpress.com/2016/02/state-of-connectivity-2015-2016-02-21-final.pdf>> Acesso em 30 de novembro de 2016.

<sup>9</sup> Disponível em <<http://data.cetic.br/cetic/explore>> Acesso em 30 de novembro de 2016.

Desenvolvida em 1969 pela agência Americana ARPA (Advanced Research and Projects Agency) e financiada pelo governo dos Estados Unidos da América, ficou conhecida como ARPAnet a mobilização da união de diversos computadores militares feita por várias pessoas que dominavam o conhecimento sobre computadores, redes e computação via cabos telefonicos, onde os arquivos e documentos digitalizados não teriam uma rota única de transporte ou um centro de armazenamento, tornando assim, a informação inextinguível. (HAUBEN, 1998, p. 08)

Figura 1 - Mapa lógico da ARPAnet em 1977, mostrando os diversos IPs conectados



Fonte: The Computer History Museum

O nome que usamos atualmente para nossas redes digitais, a saber, Internet, surgiu anos depois da tentativa bem-sucedida de conexão de computadores da ARPA, quando o número de conectados expandiu muito, interligando além dos cem primeiros pontos, diversas outras universidades, laboratórios, primeiramente apenas nos Estados Unidos da América e na Inglaterra e depois outros países do globo. (HAUBEN, 1998, p. 08)

Durante suas primeiras duas décadas de existência, rede da Internet fora restrita a ambientes acadêmicos e científicos. No ano 1987 o uso comercial da

Internet foi finalmente liberado nos EUA e em 1992 tornou-se muito famosa, fazendo com que surgissem empresas provedoras de acesso à rede de computadores.

A partir deste momento, a Internet começou a se popularizar em um ritmo frenético, entrando em contato com as mais diversas partes do mundo, criando uma rede complexa. Ao longo destes primeiros anos de história, um sentimento começou a surgir nos estudiosos de programação e pensadores políticos, uma esperança de um novo modo de se produzir conhecimento, fazer discussões e por fim, realizar uma ação política.

No início dos anos 1980, o movimento conhecido como “Movimento Software Livre” começa a emergir seguindo atentamente as quatro regras citadas acima pautadas por Richard Matthew Stallman, o criador do mesmo. Ao fim dos anos 1990, o movimento é apresentado ao mundo durante uma disputa política.

Formalmente estabelecem-se dois grupos: o *free*, que afirma ter como luta fundamental a “liberdade” dos usuários de *software* e ter como horizonte imediato o uso exclusivo de *softwares* livres; e o *open*, que embora afirme buscar as mesmas “liberdades” que o *free*, o faz a partir de outras instituições e com diferentes estratégias de luta – por exemplo, colocando o modelo livre de licenciamento de *software* como uma alternativa a coexistir com o modelo proprietário e argumentado que, acima de tudo, a abertura do código-fonte oferecida pelas licenças livres favorece o desenvolvimento de um *software* de melhor qualidade (EVANGELISTA, 2014, p. 175)

A discussão entre software livre, software privado, *free* e *open* fazem a Internet sofrer uma mutação e adquirir aos poucos uma faceta política em âmbito global. Isto, no Brasil, começa com o crescimento do pensamento aliado ao grupo *free* da discussão do *software* livre entre os meios dos movimentos sociais, militantes e sindicalistas. Essa apropriação fez com que o software livre tomasse principalmente uma posição de ferramenta de autonomia, independência, arma contra a globalização corporativa e o neoliberalismo e arma para a luta a favor da justiça social.

Daí que, por ora, há todo um conjunto novo de disputas e conflitos sobre a produção e a regulação da liberdade na Internet, na medida em que todo o valor capitalista está radicado em fazer os conectados livres permanecer dentro de limites programáveis e de conexões preestabelecidas, para recolher destes toda a sua produção social. É o paradigma de produção colaborativa do “tudo é meu” (Malini, 2008). Na contramão deste

movimento, há todo um outro que visa inflar de liberdade a rede, a partir da disseminação de dispositivos que aceleram a socialização e o compartilhamento de conhecimentos, informação e dados, seguindo novos modelos de direito público, abrindo um conflito com a governança capitalista da liberdade na rede. (MALINI; ANTOUN, 2013, p. 153)

Essa junção de Internet com questões políticas acaba com o passar do tempo se tornando algo quase de dissociação impossível. O termo tecnopolítica serve bem a esse respeito; significando que, para se realizar uma análise contundente de qualquer situação relacionada à Internet, não se pode deixar de fora o âmbito político da sociedade. Logo, a Internet não pode ser pensada sem ser politicamente.

A privacidade acaba se tornando “ponta de lança” da discussão relacionada com a política da Internet a partir do momento que a movimentação *on-line*, feita por coletivos, movimentos sociais, partidos e estudiosos em geral de matérias relacionadas à Internet e à cibercultura começam a explorar e debater o direito à anonimidade na rede mundial de computadores. Isto é, o poder de navegar sem se identificar.

Uma questão de natureza filosófica como essa mobiliza então muitas áreas do saber, como os estudos jurídicos, das ciências da computação e das ciências humanas. As leis, que pautavam questões como privacidade<sup>10</sup> e vigilância, devido ao crescimento intenso da Internet, foram rapidamente ficando ultrapassadas e demoraram tempo demais para serem mobilizadas novamente por atores humanos com poder de ação sobre a existência e a função delas, o que foi gerador de diversos incidentes, tanto no Brasil quando em diversos outros países do mundo.

O ponto central de mudança do pensamento que fez a Internet finalmente ter uma posição impossível de ser dissociada da política e de questões relacionadas à privacidade foi quando, em 2013, Edward Joseph Snowden, na época

---

<sup>10</sup> A privacidade como um direito do ser humano é considerada pelos estudiosos das ciências jurídicas um dos “direitos da personalidade”, que, por sua vez, deveriam pautar as relações do homem com a sociedade. Porém, sua existência como um vocábulo jurídico é algo extremamente novo, que inexiste na carta magna de 1988 (MATOS, 2005, p. 14). A menção ao direito à privacidade também não é feita na Declaração Universal dos Direitos Humanos, porém, dispositivo semelhante ao da Constituição Brasileira é encontrado em seu décimo segundo artigo (ONU, 1948). Já no Código Civil Brasileiro a tutela à privacidade é amparada pelo artigo 12 no capítulo dois, Direitos da Personalidade. (BRASIL, 2002). Lendo estes três trechos das leis que são aplicadas no dia a dia do brasileiro, nota-se que a realidade *on-line* é tratada com insuficiência pela legislação brasileira (Por brasileira, refiro-me à Constituição Brasileira e ao Código Civil Brasileiro, mas entra nessa miríade a Declaração Universal dos Direitos Humanos, que, como é explanada no seu nome, é algo tido como “universal”). Estas leis citadas acima não possuem a densidade necessária para gerir um dispositivo possuidor de diversas redes e características como a Internet.



administrador de sistemas da CIA, tornou públicos detalhes de vários programas que constituem o sistema de vigilância global da Agência Nacional de Segurança Americana, a NSA.

Os detalhes da vigilância global de informações executada através de vários programas (entre eles o programa de vigilância PRISM dos Estados Unidos) foram revelados por uma denúncia feita por Snowden aos jornais *The Guardian* e *The Washington Post*. Devido a isto, o Governo dos Estados Unidos incriminou-o por diversos crimes como comunicação não autorizada de informações de defesa nacional, roubo de propriedade do governo e comunicação intencional de informações classificadas como de inteligência para pessoa não autorizada. (BOWDEN, 2013. p. 13)

A partir deste momento, o que já era suspeita de muitos grupos sociais e organizações diversas que lutavam pela anonimidade se torna concreto: a Internet pode e é usada para vigilância; possibilitando uma vida conectada na qual a informação possui muito maior velocidade e potência, porém, informações contidas nela tidas como pessoais podem e são catalogadas para os mais diversos fins e aplicações.

### **3. CIBERATIVISMO, MANIFESTAÇÕES E EVENTOS BRASILEIROS – BASES DA CRYPTORAVE**

Com o aparecimento de notícias envolvendo os relatos de vigilância na Internet, diversas questões políticas e sociais distintas começam a vir à superfície ao mesmo tempo em que grupos sociais que serão abordados neste capítulo iniciam a luta por suas pautas *on-line*. Existem vários motivos para a possibilidade da mobilização dos atores e da decorrente criação de um evento como a *CryptoRave* ter acontecido no Brasil. Desde a chegada do ciberativismo no Brasil, do nascer de grandes ideias como o Fórum Internacional de Software Livre<sup>11</sup> até a criação de outros eventos inspirados em moldes dos mais diversos continentes, muito ocorreu.

A expansão da videovigilância, notável nos grandes centros urbanos após os atentados de 11 de setembro de 2001 nos Estados Unidos, reorganiza as relações entre segurança e vigilância. Elas não mais focalizam populações e espaços classificados como perigosos ou suspeitos, mas se dirigem a toda sorte de espaço público, semipúblico e privado. A emergência dos protestos políticos no Brasil em junho de 2013 é um dos exemplos mais recentes desta apropriação, na esteira de outros casos, como o da “primavera árabe”, no fim de 2010 e início de 2011, dos acampamentos e insurreições na Europa, em 2011 e 2012, das marchas e ocupações na América Latina e nos Estados Unidos<sup>4</sup>, entre outros. (...) Paralelamente, o ativismo político e a guerrilha informacional baseados no anonimato cibernético ganham visibilidade e repercussão, criando vias de expressão que diferem das práticas de exposição circunscritas à esfera do eu. O grupo *Anonymous* é exemplar neste processo (Cf. Coleman, 2012), assim como o *4Chan*, significativo no campo do compartilhamento de imagens de forma anônima (Cf. Auerbach, 2012) (BRUNO, 2013, p. 08)

Aqui, nesta parte do texto, veremos de maneira sintética o ciberativismo, que por fim trouxe a São Paulo o evento foco deste trabalho. Pontos centrais serão abordados para que o entendimento das bases da *CryptoRave* se torne algo palpável ao leitor. Começaremos aqui pelo ciberativismo em geral, que aliado à Internet, é um dos maiores atores mobilizadores do que aqui é explorado.

O ciberativismo conseguiu se consolidar em meados dos anos 90, com o crescimento da já comentada web com ênfase no comercial. Em resumo seria um

---

<sup>11</sup> O FISL é um evento que reúne grande parte do que se convencionou chamar de “comunidade de *software* livre brasileira”, pessoas que, em grande maioria, seguem os ideários espalhados por Richard Stallman, este mobilizou seus saberes nas disciplinas de ciência da computação, do direito e da economia para tecer uma proposta: a liberdade dos usuários de *software*. Esta liberdade funciona de uma maneira muito simples: todo *software* produzido por uma pessoa ou um grupo de pessoas, deve seguir princípios éticos, as quatro liberdades fundamentais do movimento: o *software* deve ser livre para ser modificado, executado, copiado e distribuído. Apoiando-se diretamente nessas quatro liberdades fundamentais, deu-se o surgimento no ano de 2000 no Brasil em Porto Alegre – RS do Fórum Internacional de Software Livre, conhecido popularmente como FISL. Este serviu e serve até hoje como uma espécie de molde para qualquer evento que trate de assuntos relacionados com Internet, Liberdade e etc. (EVANGELISTA, 2014, p. 182)

conjugado de práticas em defesa de causas políticas, socioambientais, sociotecnológicas e culturais, realizadas nas redes cibernéticas, especialmente na Internet, onde a mesma é utilizada como meio, pauta de reivindicação e ponto central (SILVEIRA, 2010, p. 31). O movimento inicial do que se entende como ciberativismo nasce logo após o surgimento da Internet em confluência com a cibercultura, definida por Pierre Levy como "(...) o surgimento de um novo universal, diferente das formas que vieram antes dele no sentido de que ele se constrói sobre a indeterminação de um sentido global qualquer" (LÉVY, 1999, p. 15). Para o autor, que foi um dos criadores deste conceito, a cibercultura é uma nova tendência nascida da tecnologia emergente e em especial da Internet e inclui o conjunto de práticas, técnicas (materiais e intelectuais), de modos de pensamento, de atitudes, e de valores que se desenvolvem juntamente com o crescimento do ciberespaço<sup>12</sup> (LÉVY, 1999, p. 17), desta maneira o mundo estaria passando, desde o surgimento da Internet, por um processo de universalização da cibercultura, na medida em que estamos dia-a-dia mais imersos nas novas relações de comunicação e produção de conhecimento que ela nos oferece.

Em 10 de abril de 1990, diversas pessoas autodenominadas ciberativistas se uniram para fazerem um pronunciamento contra a criação de uma unificação de diversos bancos de dados que continham informações variadas de mais de 120 milhões de norte-americanos. Este caso ficou conhecido como "Caso Lotus", em grande parte devido à campanha bem sucedida feita por tais ativistas, a qual envolvia distribuição em massa de e-mails e apresentações que tinham como função informar cidadãos sobre os possíveis riscos de permitir que uma empresa detivesse informações pessoais armazenadas. (GURAK, 1997)

Com o começo dos anos 2000, ações de ciberativismo começam seu alargamento. A reivindicação de diversas questões sociais e jurídicas começa a ser organizada por movimentos com um número sempre crescente de participantes; com um aumento exponencial no número de adeptos na primeira metade da década. (MALINI; ANTOUN, 2013, p. 152)

---

<sup>12</sup> "O termo [ciberespaço] especifica não apenas a infraestrutura material da comunicação digital, mas também o universo oceânico de informação que ela abriga, assim como os seres humanos que navegam e alimentam esse universo. Quanto ao neologismo 'cibercultura', especifica aqui o conjunto de técnicas (materiais e intelectuais), de práticas, de atitudes, de modos de pensamento e de valores que se desenvolvem juntamente com o crescimento do ciberespaço" (LÉVY, 1999, p. 17).

Iniciando em 2003, uma comunidade *on-line* descentralizada surge em fóruns da Internet. Eles ficam conhecidos como “Anônimos” (em inglês *Anonymous*) e atuam de forma coordenada e anônima com objetivos em comum combinados *on-line* entre si. Tais objetivos têm como pauta geralmente a luta por algum direito ou contra alguma injustiça.

No ano de 2007 para 2008 explodem nos sites de notícias como um dos maiores nomes do ativismo hacker do mundo devido à organização e força do coletivo. Seus métodos são ao mesmo tempo elogiados e temidos pelas diversas faces da opinião pública e acabam dando o tom do hacktivismo que estaria por vir.

Os Anônimos (...) agora usam suas super-habilidades de criação e manipulação de sistemas para atingir no coração os métodos de forjar a opinião pública e obter a atenção das massas usados pelos megameios de comunicação. (...) O fim da era Bush fez com que o ativismo hacker fosse redefinido tendo como alvo a desmoralização dos processos de formação de consenso massivo e de produção de atenção de massa. Eles definiram a princípio o canal /b/ do 4chan como local de reunião. Dali passaram a partir os principais petardos que podem balançar ou o YouTube ou o Twitter, apenas para mencionar dois sítios. Apelidados de /b/astardos (/b/tards), esses usuários fizeram da comunicação anônima sua principal arma para fazer tremer a rede mundial, inventando um novo capítulo, após o do ataque DDOS, para a novela da liberdade de expressão na comunicação distribuída em rede. Foram acusados desde dominar eleições de cantores na MTV até substituir fotos de usuários por imagens pornográficas no MySpace, passando até por abrir a conta de e-mail de Sarah Palin para visita pública. Tornaram-se notórios depois de deflagrar uma guerra contra a Scientology que grassava no meio artístico de Hollywood (MALINI; ANTOUN, 2013, p. 170).

Devido aos casos citados acima, instituições jurídicas começam a buscar regulamentações para as práticas na Internet, deflagrando várias ações contra ciberativistas. Um dos maiores exemplos relacionados a isso vem de Ángeles González Sinde, ministra da cultura Espanhola que em 2009 trouxe ao público uma lei em projeto encomendada pela indústria fonográfica que consentia que sites e páginas fossem deliberadamente desmantelados por oferecerem links para downloads de músicas sem o pagamento de licença autoral, essa empreitada ficou conhecida mundialmente como Lei Sinde<sup>13</sup>. (LETAI, 2012, p. 01)

Seguindo a guinada dos movimentos ciberativistas, onde a Internet é central, temos agitações que usaram das redes sociais *on-line* como auxílio para

---

<sup>13</sup> Nicolas Sarkozy, na época presidente da França, e o ministro da Cultura Italiano, Sandro Bondi criaram políticas paralelas às de Sinde atacando as Redes de compartilhamento P2P neste mesmo ano.

organização, como na Espanha em 2011, aconteceram diversos protestos conhecidos como “Los Indignados” ou “#15M”.

O #15M se originou após a aprovação da Lei Sinde, em 15 de fevereiro de 2011, que permite que sites de downloads considerados ilegais sejam tirados do ar pela Justiça espanhola. Contrários à lei, o movimento anti-Sinde catalisou a participação política no país, articulando distintos movimentos de críticas à democracia representativa no país (já que, embora adversários, os políticos de ambos os partidos aprovaram em processo de acordo a lei Sinde, ainda que sabendo-a antipopular). O acordo expunha as relações íntimas entre crise econômica, partidos políticos e a elite financeira espanhola (MALINI; ANTOUN, 2013, p. 202)

A grande movimentação que confirmaria ações relacionadas ao ciberativismo como possível ameaça a governos corruptos e ilegais devido à sua potência foi em também em 2011 com a Primavera Árabe. Estes levantes foram uma onda de protestos, revoluções populares e revoltas contra diversos governos do mundo árabe que desabrochou em no começo de 2011 e derrubou ditadores que estavam há mais de 30 anos no poder.

A Primavera começou em países do norte da África e se desenvolveu até o Oriente Médio. A população lutou pela melhora nas condições de vida, por direitos humanos e pela democracia em si nestes protestos devido ao fato de que por muitos anos países árabes sofreram com regimes repressores. A relação com o ciberativismo e movimentos sociais organizados por via *on-line* vem do fato que muitos dos manifestantes se organizaram e conseguiram escapar de repressões policiais via redes sociais como o Twitter, fazendo da plataforma uma maneira de articular a revolta de maneira eficaz. (MALINI; ANTOUN, 2013, p. 180)

Ocorreram entre 2011 e 2013 movimentações inspiradas pela Primavera Árabe que ficaram muito famosas na América do Sul, como o Occupy Wall Street, que nasceu nos Estados Unidos e teve como argumento central a luta contra a desigualdade econômica e social, a corrupção e a influência indevida das empresas, principalmente do setor financeiro, no governo dos Estados Unidos e as “Jornadas de Junho” ou “Manifestações dos 20 centavos”, que ocorreram no Brasil de maneira explosiva e se tornaram mobilizações enormes. Tais “Jornadas de Junho” foram manifestações variadas pelo país inteiro que tiveram como ponto de nascimento a insatisfação da população com o aumento nas tarifas de transporte público. As manifestações ocorreram principalmente nas capitais e se expandiram

em diversas outras pautas, envolvendo a luta contra a corrupção, revolta contra altos impostos e muitos outros clamores populares. Boa parte das manifestações usaram o Twitter e o Facebook como meio de organização para definir horários de encontro e objetivos a serem alcançados com o protesto. (SOUSA; SOUZA, 2013, p. 85)

As manifestações de junho de 2013 no Brasil e vários outros protestos que ocorreram ao redor do mundo nos últimos anos (Primavera Árabe, 15 M na Espanha e Occupy Wall Street, para mencionar apenas os mais visíveis), tornaram evidentes para boa parte da opinião pública o papel que a internet e as tecnologias digitais desempenham na geração de novas formas de sociabilidade, de identidade, e de comportamento político e social.” (SILVEIRA; BRAGA; PENTEADO, 2014, p. 05)

Em 2012 o congresso americano buscou criar, com a SOPA (*Stop On-line Piracy Act*) e PIPA (*Protect Intellectual Property*), leis que restringiam as informações de direito autoral e de direito de IP na internet. De tais medidas brotaram grandes manifestações na rede. O ciberativismo tomou a dianteira dos volumosos processos de conscientização e agiu para derrogar tais medidas no congresso lutando veementemente contra medidas que criminalizavam o comércio não comercial de arquivos pela Internet. (MA, 2015, p. 01)

Durante todos estes acontecimentos, movimentos organizados por via de redes sociais e manifestações de ciberativismo, grupos de pessoas interessadas nestas questões começaram a se reunir com o intuito de espalhar a ideia da luta a favor da privacidade *on-line*, do entendimento da Internet como algo a ser discutida e tratada de maneira política e do combate contra a vigilância na Internet. Um molde que ficou muito conhecido e adotado foi o de organização de eventos para divulgação de palestras, livros e conhecimento.

No Brasil dois grandes exemplos atuais disso são a *CryptoRave*, que será discutida profundamente a seguir, e o Fórum Internacional de Software Livre. Mesmo sendo um evento pago e com diversas facetas diferentes à *CryptoRave*, o Fórum Internacional de Software Livre ou FISL é um grande exemplo conhecido globalmente.

#### **4. CRYPTORAVE – SEGURANÇA, CRIPTOGRAFIA, HACKING, ANONIMATO, PRIVACIDADE E LIBERDADE NA REDE**

Já a *CryptoRave* inspira-se na ação global e descentralizada das chamadas *CryptoParties*, encontros ao vivo de pessoas associadas com a cibercultura e com interesses em comum com o objetivo de difundir os conceitos fundamentais e softwares básicos de criptografia. Os encontros que criam as *CryptoParties*

funcionam em um formato completamente aberto em que pessoas, independentes de idade, gênero ou conhecimento se reúnem trazendo seus computadores, *smartphones*, etc. para aprender sobre programação, privacidade digital e derivados.

Figura 2 - Logo oficial da CryptoParty



Fonte: <https://www.cryptoparty.in>

Conforme o texto introdutório disponível no site oficial das *CryptoParties*<sup>14</sup> a privacidade seria o lugar onde as ideias nascem, onde você pode refletir em qualquer ideia da maneira que quiser. Este lugar não é apenas físico, mas digital, também. Nenhum governo ou corporação respeita isso. Mas nas *CryptoParties*, isso é respeitado (CRYPTOPARTY.IN, 2017a)<sup>15</sup>.

As *CryptoParties* possuem alguns princípios centrais, criados coletivamente pelos seus participantes, que guiam o fluxo dos encontros e são aproveitados pela *CryptoRave*. São eles, em ordem disponível no site<sup>16</sup>:

1. Ser excelente com os outros. Pois estes encontros são ambientes onde as pessoas devem se sentir seguras e bem-vindas não importa qual seja sua origem ou seu grau de saber; todas questões serão relevantes e as explicações serão direcionadas às pessoas com menor saber sobre o tópico em questão. Isso também significa que qualquer tipo de comportamento com o intuito de envergonhar ou humilhar alguém não possui lugar em uma *CryptoParty*.
2. Faça coisas. Estes encontros acontecem porque pessoas fazem eles acontecerem. Se você não souber se o tópico que quer debater é interessante, tente mesmo assim e se você tiver muita vergonha, comece perguntando para a pessoa ao lado.
- 3.

<sup>14</sup> Disponível em <<https://www.cryptoparty.in/>> Acesso em 30 de novembro de 2016.

<sup>15</sup> Tradução e adaptação livre

<sup>16</sup> Tradução livre



Respeitar a política contra abusos. Toda *CryptoParty* deve ser dedicada a ser um local onde nenhuma espécie de abuso pode ser tolerado (CRYPTOPARTY.IN, 2017b).

Estes princípios de organização fazem com que a rede de qualquer tipo de *CryptoParty* se mantenha coesa e com uma função acolhedora. Além disso, como ferramentas para ajudar na organização, está disponível no site oficial um livro de mais de 335 páginas chamado de “The *CryptoParty* handbook”, algo como “O livro de bolso da *CryptoParty*”; em que todos os saberes necessários para a realização de um encontro desse tipo são cuidadosamente explanados, desde pequenas aulas sobre e-mail, browsing, publicações, SMS, senhas, etc.

Em 2013, na época de efervescência das “Jornadas de Junho” e das revelações de Snowden foi realizada a primeira *CryptoParty* em São Paulo. Após muitos interessados comparecerem, uma reunião entre os organizadores foi feita, o evento foi ampliado e a ideia de fazer uma *CryptoParty* de 24 horas nasceu e se transformou em *CryptoRave*.

Como a ideia original das *CryptoParties* é de criar um espaço para difundir criptografia e técnicas de privacidade para todos, esta foi abraçada pela *CryptoRave*. Todas as edições contam com uma série de palestras e oficinas dedicadas a ensinar como usar criptografia.

Figura 3 - O logo da *CryptoRave* e diversos outros cartazes relacionados com as causas defendida pelo evento



Fonte: <https://CryptoRave.org/>

A *CryptoRave* desde então consta no site oficial das *CryptoParties* como a maior *CryptoParty* brasileira. Um marco para os eventos coletivos que prezam a cibercultura.

Sabe-se que a *CryptoRave* é atualmente o maior evento e rede de disseminação de conhecimento sobre segurança e privacidade no Brasil; organizada voluntariamente com o objetivo de ensinar a criptografia para todos, de forma gratuita e aberta. A última edição da *CryptoRave* ocorreu entre o dia 5 e 6 de maio de 2017, na Casa do Povo em São Paulo e segue um modelo que envolve: financiamento coletivo do evento, trilhas de discussão, palestrantes do Brasil e do mundo, workshops, festa na madrugada e muitas outras atividades.

No ano de 2016 o evento contou com cinquenta e uma palestras/workshops<sup>17</sup>. Dezessete dessas com o foco em questões de segurança, nove em política, nove *hacking*, oito em criptografia, cinco em questões de gênero, duas *Keynotes* – que são palestras de longa duração com convidados especiais – e uma exibição de filme.

Já no ano de 2017 o número de palestras aumentou consideravelmente. Foram oitenta e seis atrações divididas em vinte e oito voltadas a questões de segurança, vinte e quatro à política, doze à criptografia, doze a gênero, dez a *hacking*, duas *Keynotes* e uma exibição de filme.

<sup>17</sup> As palestras de 2016 não foram classificadas por temática pelo coletivo, então, tomei a liberdade de eu mesmo fazê-las. Já para as palestras de 2017 a divisão divulgada pelo coletivo foi utilizada.

Ambas as edições contaram com a presença de advogados, artistas, ativistas, cientistas da computação, engenheiros, escritor, estudante, jornalistas, pesquisadores, professores, sociólogos, técnicos em informática, psicólogos, etc. Criando um evento interpenetrado pelas mais diversas áreas do saber.

Ao contrário do que pode ser pensado sem uma reflexão prévia, a *CryptoRave* em si não é um coletivo. É um evento organizado por coletivos e indivíduos. Na última edição, de 2017, foram cinco coletivos organizadores, os já citados: Actantes, Escola de Ativismo, Intervezes, Encrypta e Saravá. Além dos coletivos, há também indivíduos que participam ativamente da organização e há outras organizações que apoiam o evento com doações e empréstimos de equipamentos. Nesse sentido a *CryptoRave* é mais um esforço coletivo do que "um coletivo".

Em entrevista com os organizadores, foi exposto que a programação do evento foi se aperfeiçoando ao longo do tempo e um "Chamado para Atividades" foi estabelecido para organizar parte da programação. Isso envolve escolher palestras, falar com o palestrante e organizar sua logística. Relatado como um trabalho penoso que ajuda a estruturar a comunidade.

Tanto na edição de 2016 quanto na de 2017 o "Chamado para Atividades" foi feito no ano anterior e teve como objetivo receber atividades nos seguintes formatos: (*CRYPTORAVE*, 2016)

- Apresentação musical, literatura, exibição de filme ou instalação artística
- Palestra e debate;
- Oficina, jogo, mão na massa, colaboração em projeto free/libre/open software/source;
- Exposição de trabalhos.

E para as tais atividades enviadas serem avaliadas e aceitas (ou não), um modelo feito pela organização deveria ser seguido:

- As atividades de palestras que forem merchandising de produtos serão automaticamente desclassificadas;
- Não haverá nenhuma compensação financeira ou contrapartida da *CryptoRave* ao colaborador de uma atividade;
- Não serão aceitas as propostas enviadas por outros meios como Twitter e Facebook.

Em relação ao Chamado para Atividades de 2016, no primeiro semestre do ano encontros presenciais para definir local, infraestrutura necessária, *keynotes*, voluntariado, entre outras coisas foram feitos. A campanha financeira de 2016 e 2017 foi realizada no Catarse, uma plataforma de financiamento coletivo *on-line*. Em 2016 uma campanha para arrecadar quarenta e cinco mil reais para as despesas foi realizada; a mesma foi finalizada após dois meses, com cinquenta e um mil reais de arrecadação num processo longo e desgastante, segundo os organizadores. Em 2017 também fora realizada a campanha com o intuito de recolher sessenta mil reais e finalizou arrecadando nove mil a mais do que o esperado.

De acordo os organizadores, os maiores desafios durante a organização de tamanho evento foram a criação de uma oferta de programação em si que fosse interessante e a seguinte organização das diversas atividades e propostas divergentes em grandes tópicos. Além disso, devido à necessidade de reuniões semanais, muitos tiveram que perder trabalho ou faculdade para conseguirem fazer todas as tarefas do evento.

A *CryptoRave* focou sua publicidade nas mídias sociais e em lista de e-mails reunidas ao longo do tempo pelos participantes e organizadores sem focar em um público-alvo, focalizando assim a ideia de um evento hacker aberto e inclusivo para as mais diversas faixas etárias; seguindo assim os dogmas das *CryptoParties*.

Tanto em 2016 quanto em 2017 a *CryptoRave* contou com seis espaços onde, durante vinte e quatro horas seguidas, mais de cinquenta palestras aconteceriam em um circuito enorme de conhecimento. Estes seis espaços com diferentes temáticas e funções foram categorizados assim:

- Espaço Aaron Swartz: com debates e discussões sobre Neutralidade da Rede, Marco Civil e outros temas relacionados à regulamentação da Internet;
- Espaço Chelsea Manning: voltado para apresentações e palestras sobre os últimos avanços e vulnerabilidades da criptografia;
- Espaço Edward Snowden: focado na desmistificação e o compartilhamento de técnicas de *hacking* e exploração dos limites da Internet;
- Espaço Alan Turing: montando oficinas práticas de instalação e uso de ferramentas de comunicação segura, privacidade e proteção de dados.

- Espaço Ada Lovelace: criando um espaço que democratiza o acesso para pessoas que sofrem com a desigualdade de gênero.
- Espaço Ian Murdock: com o foco central em segurança pessoal digital.

Junto com as palestras divididas nestes seis grandes espaços, dois *Keynotes* por ano foram feitos. As já citadas palestras de maior duração, com temáticas amplas e convidados especiais.

Além destes seis espaços e das duas *Keynotes* por ano, a *CryptoRave* traz em seu âmago a ideia de aliar os ideais das *CryptoParties* com uma balada de sete horas de duração com seis atrações diferentes; uma instalação artística interativa e rodadas de *Capture the Flag*, um tipo de competição que reúne diversos desafios de segurança da informação, exigindo dos participantes conhecimento em diversas áreas das ciências da computação.

Dividiremos cada um dos espaços para uma verificação das maneiras quais as questões relacionadas à luta pela privacidade e o enfrentamento à vigilância se transformam e são apresentadas como questões politizadas na *CryptoRave*. Seguiremos a ordem divulgada no site oficial da *CryptoRave*. Devido ao grande número de palestras e a impossibilidade de explorar cada uma delas no trabalho sem o mesmo se transformar em algo muito extenso, para as 2016 foram selecionadas as palestras que divulgaram mais informação *on-line* no site da *CryptoRave*; e para as palestras de 2017, serão exploradas as quais assisti no evento.

#### **4.1 Espaço Aaron Swartz: Regulamentação da Internet, anonimidade e direitos humanos**

O espaço que recebe a abertura oficial da *CryptoRave* e, também, o que mais possui palestras ao todo recebe o nome de Aaron Swartz, um programador estadunidense e ativista na Internet; co-autor da criação do RSS<sup>18</sup> e um dos fundadores do Reddit<sup>19</sup>. Aaron foi encontrado morto em seu apartamento no

<sup>18</sup> Esta tecnologia permite aos usuários da Internet se inscreverem em sites que fornecem "feeds". Estes recebem atualizações dos sites automaticamente e ao vivo, desta maneira o utilizador pode permanecer informado de diversas notícias/novidades de muitos sites sem precisar visitá-los um a um.

<sup>19</sup> Um site de mídia social onde usuários podem divulgar ligações para conteúdo na Web. Outros usuários podem então votar positivamente ou negativamente nas ligações divulgadas, fazendo com

começo do ano de 2013, dois anos depois de ter sido preso pelas autoridades federais dos Estados Unidos, por usar a rede do Instituto de Tecnologia de Massachusetts para descarregar sem pagamento, grandes volumes de artigos da revista científica *JSTOR*. Swartz lutava contra a prática desta revista por remunerar editoras e não os autores e cobrar o acesso aos artigos, limitando o acesso para comunidades acadêmicas. Hoje, Aaron é símbolo da luta pelo software e pela informação livre.

A legislação da rede mundial de computadores, reações a leis como as de Ángeles Sinde, o Marco Civil da Internet, a Neutralidade da Rede<sup>20</sup>, e outros temas relacionados à regulamentação da Internet são o foco deste espaço. As palestras *Keynotes* de ambos anos aconteceram nesta área da *CryptoRave*; as de 2016 foram “Terrorismo e Vigilância” e a segunda, “Marco Civil e CPI dos Cibercrimes”; já em 2017 foram “Resistindo à Distopia” e “Não começou com Snowden e não vai terminar com o Vault7”.

A *Keynote* inicial de 2016 traz ao público a experiência de três convidados que conviveram por algum tempo como inimigos do Estado, após terem sido enquadrados em leis anti-terroristas por sua profissão e seu ativismo, e a segunda *Keynote* explora o Marco Civil e como ele tramita como uma espécie de “constituição do mundo virtual”, estabelecendo direitos, garantias, princípios e deveres para o uso da Internet no Brasil. Este é localizado sob o nome de lei nº 12.965.

Art. 3º A disciplina do uso da Internet no Brasil tem os seguintes princípios:

- I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
- II - proteção da privacidade;
- III - proteção dos dados pessoais, na forma da lei;

Um dos pontos principais deste Marco se dá na sua relação com a privacidade, que a partir de agora se transforma em uma garantia legislativa<sup>21</sup>. Uma

---

que apareçam de uma forma mais ou menos destacada na sua página inicial.

<sup>20</sup> A neutralidade de rede significa que uma empresa que provê conexão com a Internet é obrigada a tratar todos os dados que nela circulam igualmente. Assim, um provedor específico não pode fazer um site ter mais capacidade e velocidade de acesso e uso do que outro. (SOLAGNA, 2015)

<sup>21</sup> Debates públicos sobre os conteúdos do Marco aconteceram entre abril e maio de 2010 e em agosto de 2011 o já então projeto de lei foi enviado pela presidenta Dilma Rousseff à câmara. Em 2013, após o escândalo das notícias vazadas confirmando a espionagem eletrônica dos Estados Unidos da América no Brasil, a Presidenta e a Ministra das Relações Internacionais, na época Ideli

das maiores diferenças práticas que sua existência traz é que os dados das pessoas que estão navegando na Internet só perderão sua proteção e sigilo total mediante ordem judicial e os e-mails e outros tipos de comunicações *on-line* privadas possuem agora a mesma proteção que cartas, conversas via telefone, etc. possuía. Além disso, nenhuma empresa que trabalha com publicidade *on-line*, analisa dados de usuários e produz propagandas poderá utilizar estes sem o consentimento expresso do internauta.

A liberdade de expressão na Internet é pautada pelo Marco da mesma maneira que é na Constituição de 88, garantindo a democracia no ambiente digital. Esta garantia se desdobra em segurança e privacidade a todos os usuários dentro da rede brasileira de Internet.

Em 2017 a *Keynote* “Resistindo à Distopia” teve como foco maneiras de dialogar com coletivos e pessoas não especialistas via órgãos não governamentais e *softwares* para alertar e mobilizar questões relacionadas à segurança digital e a luta contra vigilância. Também, no mesmo ano, “Não começou com Snowden e não vai terminar com o Vault7” dá aos espectadores um resumo da história da luta recente contra a vigilância.

Palestras como “Privacidade, liberdade de expressão e governança global<sup>22</sup>” do advogado Jefferson Nascimento e “Grampolândia: a República da Escuta<sup>23</sup>”, de Silvio Rhatto e Gustavo Gus trazem à *CryptoRave* atividades com o objetivo de apresentar o estado do debate sobre o direito à privacidade e liberdade de expressão no âmbito de organizações internacionais, dando ênfase ao protagonismo internacional do Brasil no tema – reação à espionagem sofrida por agências dos Estados Unidos – e as contradições com as políticas adotadas e os principais casos e escândalos de interceptações no país, mostrando o funcionamento dos grampos telefônicos e digitais e como se proteger.

Essas duas palestras começam a relacionar a temática do Marco Civil com acontecimentos que ocorreram nos últimos anos da história do Brasil<sup>24</sup>, usando

---

Salvatti, notaram a necessidade da aprovação do Marco Civil da Internet devido às suas garantias legais de direitos digitais. Após quase trinta votações adiadas na Câmara dos Deputados, no dia 25 de março de 2014 o projeto de lei fora aprovado e enviado ao senado federal e finalmente aceito e sancionado pela presidenta, entrando em vigor no dia 23 de junho de 2014.

<sup>22</sup> Palestra da *CryptoRave* 2016.

<sup>23</sup> Palestra da *CryptoRave* 2016.

<sup>24</sup> Notícia sobre os acontecimentos disponível em <<http://g1.globo.com/politica/noticia/2015/07/lista-revela-29-integrantes-do-governo-dilma-espionados-pelos-eua.html>> Acesso em 30 de novembro de 2016

desse fator histórico para entrar em contato com o público do evento e trazer ao mesmo uma reflexão que combina ciências da computação com política e questões sociais.

A revelação dos grampos que ocorreram no mandato de Dilma Rousseff (2011-2016) pelo *WikiLeaks* foi peça-chave de uma reflexão sobre privacidade e vigilância feita tanto pelos órgãos governamentais quanto pelos civis brasileiros. Com estas duas palestras citadas acima, este espaço da *CryptoRave* começa já trazendo a discussão sobre vigilância para um nível muito próximo do real; explorando a maior figura do poder político brasileiro da época (a então presidenta Dilma Rousseff) em uma situação quase inacreditável: tendo mais de vinte e nove telefones do governo – incluindo o de ministros, assessores e diplomatas – espionados pela Agência Nacional de Segurança dos Estados Unidos.

Em seguida, “*Anonymous: O Hacktivismo como consciência política*<sup>25</sup>”, da Jornalista Marina Neto expõe como a abertura de uma consciência coletiva de novos agentes da resistência digital proporcionou a luta pela liberdade de informação e transparência na rede por grupos como o já citado *Anonymous*<sup>26</sup>. A temática desta palestra sintetiza muito o pensamento que circunda os organizadores da *CryptoRave*, estes que possuem uma identificação muito profunda com movimentos e ideários de resistência dentro da realidade da Internet.

Ao abordar a luta do grupo *Anonymous*, o espaço Aaron Swartz explana aos seus participantes como é possível criar e participar de um movimento organizado dentro do universo *on-line*. Com a pauta trazida pela Jornalista Mariana Neto em mente, três palestrantes anônimos trazem à *CryptoRave* a história e o funcionamento do *BrasilLeaks* na palestra intitulada “Nós somos o BrasilLeaks!<sup>27</sup>”, um site de denúncias anônimas inspirado na *WikiLeaks* que surgiu em discussões entre membros do Partido Pirata no Brasil sobre a falta de segurança em

---

<sup>25</sup> Palestra da *CryptoRave* 2016.

<sup>26</sup> “Somos uma idéia que surgiu em 2004 e sempre seguiu uma linguagem de memética e muitas sátiras. Hoje, Anonymous é uma idéia de mudança, um desejo de renovação. Somos uma idéia de um mundo onde a corrupção não exista, onde a liberdade de expressão não seja apenas uma promessa, e onde as pessoas não tenham que morrer lutando por seus direitos. Não somos um grupo. Somos uma idéia de revolução. Acreditamos que cada geração encontra sua forma de lutar contra as injustiças que encontra. Temos em mãos pela primeira vez o poder de produzir, distribuir e trocar informações. Uma oportunidade nunca vista antes na história para colaboração e construção de um mundo onde a esperança, a dignidade e a justiça sejam princípios a serem respeitados.” Trecho da aba “Quem somos” do site da Anonymous Brasil. Disponível em <<http://www.anonymousbrasil.com/sobre-anonymous/>> Acesso em 30 de novembro de 2016.

<sup>27</sup> Palestra da *CryptoRave* 2016.



ferramentas que tentam garantir anonimato. Segundo os palestrantes, buscando a transparência e a participação cidadã, o *BrasilLeaks* almeja construir uma sociedade justa e democrática com denunciadores encorajados a disponibilizar informações sobre corrupção, desvio de verbas, abusos físicos e/ou sexuais, etc. em um ambiente seguro e anônimo.

Posteriormente às palestras referentes à anonimidade e suas implicações, o repórter Daniel Bramatti, a jornalista Sabrina Duran, o economista Bruno Paes Manso e o sociólogo Henrique Parra põem em contato na palestra “Jornalismo Investigativo e Pesquisa Científica: privacidade, informações sensíveis, liberdade de informação e conhecimento<sup>28</sup>” jornalistas investigativos, cientistas-ativistas e a comunidade ativista *on-line* com o intuito de gerar um debate sobre os novos dilemas emergentes relacionados aos processos de trabalho nesses segmentos face à expansão das tecnologias digitais de comunicação. Com a reunião de profissionais da área de jornalismo investigativo e pesquisadores acadêmicos que lidam com informações sensíveis, suas rotinas e formas trabalho são relatadas, de maneira a evidenciar para comunidade de ativistas *on-line* quais os novos problemas e necessidades relativos à privacidade, proteção de dados sensíveis, liberdade de informação e conhecimento. O objetivo da mesa é, centralmente, sensibilizar os profissionais e o público em geral sobre problemas relativos ao uso das tecnologias (que novos problemas surgem sobre privacidade, anonimato, etc.) para contribuir para a elaboração de guias/tutoriais de orientação; e disseminar tecnologias de fácil uso para profissionais (jornalistas investigativos, cientistas-ativistas, entre outros).

Na última palestra do primeiro espaço da *CryptoRave* de 2016, Jamila Venturini trabalha a internet em “Termos de Uso e Direitos Humanos: discutindo o papel do setor privado na regulação de direitos humanos *on-line*<sup>29</sup>”, como um ambiente que atualmente está hiperregulado por conta tanto da influência de governos, quanto da emergência de um amplo espectro de entidades privadas capazes de regular o acesso e a difusão de informações por meio de contratos e de coletar grandes quantidades de informações pessoais sobre os usuários e suas atividades. Essas entidades desempenham na prática uma função de guardiões da Internet, exercendo uma espécie de soberania sobre as redes ou as plataformas

<sup>28</sup> Palestra da *CryptoRave* 2016.

<sup>29</sup> Palestra da *CryptoRave* 2016.

cuja arquitetura lógica (através dos códigos ou algoritmos) e regras são definidas e controladas exclusivamente por eles.

As condições contratuais que regulam a relação entre os serviços *on-line* e seus usuários são definidas por meio dos chamados “Termos de Uso”, que podem ser considerados na prática como verdadeiras “leis das plataformas”, definidas e implementadas unilateralmente pelos provedores de serviços. Ao clicar em aceitar os Termos de Uso ou simplesmente visitar uma página web, os usuários ficam obrigados a cumprir o que está ali acordado e se vinculam às políticas da empresa. Essas regras contratuais podem limitar a difusão de determinados tipos de conteúdo e condicionar a participação dos usuários ao fornecimento de uma série de informações sobre suas atividades, tendo implicações concretas na aplicação dos direitos humanos *on-line*. Visando ampliar as discussões sobre o tema, a atividade proposta traz ao público os objetivos: (i) apresentar os resultados do projeto “Termos de Uso e Direitos Humanos”, desenvolvido pelo Centro de Tecnologia e Sociedade da FGV Direito Rio, que analisou como as políticas de 50 plataformas lidam com os direitos à liberdade de expressão, privacidade e processo justo e (ii) promover um debate sobre o impacto dos contratos dos intermediários privados que viabilizam as comunicações *on-line* em determinar as atividades permitidas ou não na rede e sua responsabilidade em respeitar os direitos dos usuário de Internet.” -Jamila Venturini (2016), em sua introdução da palestra dada na *CryptoRave*.

Assim como em outras palestras deste espaço, Jamila transparece um fato cotidiano e o transforma em possível objeto de estudo para os participantes do evento. Termos de Uso, textos que temos acesso e aceitamos quase que semanalmente, aqui, se tornam motivo de debate.

Em contato com a anonimidade e a luta por mais pessoas engajadas e encorajadas tratada neste espaço, Corvolino traz em 2017 para o espaço Aaron Swartz o “Mini guia para se manter mais seguro na Internet<sup>30</sup>”, que tem como intuito nortear mudança comportamental dos espectadores para navegar de forma mais segura na Internet; e o Coletivo Mariscotron palestra sobre “Política e Tecnologia na Sociedade de Controle<sup>31</sup>”, apresentando técnicas de criptografia assimétrica e boas práticas com respeito à tecnologia para o desenvolvimento de uma cultura volvida para a segurança dos de baixo.

Perto do fim da *CryptoRave* 2017, Sérgio Amadeu trouxe ao evento “Espionagem no Brasil: A estrutura e os alvos<sup>32</sup>”. Nesta palestra, o assunto

---

<sup>30</sup> Palestra da *CryptoRave* 2017.

<sup>31</sup> Palestra da *CryptoRave* 2017.

<sup>32</sup> Palestra da *CryptoRave* 2017.

fundamental é a rede de conexões das agências de espionagem no Brasil, sua estrutura e dinâmica.

Entre as palestras e apresentações, o espaço também contou com a presença, tanto em 2016 quanto em 2017, de um Capture The Flag<sup>33</sup>. Um tipo de competição de mais de seis horas de duração que reúne diversos desafios de segurança da informação, exigindo dos participantes um conhecimento multifacetado, envolvendo áreas da criptografia, engenharia, programação e administração.

O funcionamento do desafio se dá no modelo pergunta e resposta (jeopardy), onde é necessário encontrar uma resposta para um problema específico. Por exemplo: um competidor é questionado quanto a possibilidade de extração de informações ocultas em uma imagem formato PNG e deverá utilizar técnicas de esteganografia para recuperar a senha, ou a flag, que é a resposta para aquele desafio. –Organizadores do Capture The Flag da *CryptoRave* (2016)<sup>34</sup>

E, além do jogo interativo, a *CryptoRave* de 2016 e a de 2017 também contou com uma balada na madrugada com a presença de diversos DJs. A mesma teve como intuito a congregação dos participantes e o proveito de outros modos de interação social, aqui, manifestos em uma festa.

## 4.2 Espaço Chelsea Manning: limites e novidades da criptografia

O espaço na *CryptoRave* detentor do nome de Chelsea Manning tem como cerne o ensino das novidades e explorar os limites da criptografia. Divergindo um pouco do primeiro espaço apresentado no sentido de explorar uma temática mais objetiva e científica, este adentra no desejo por trás das *CryptoParties* e da *CryptoRave*, que anseiam por um local onde a criptografia seja livre e discutida com todos participantes.

Chelsea Manning, mulher transexual nascida sob o sexo masculino e de nome Bradley Manning, é uma militar do Exército dos Estados Unidos que foi presa e processada por acesso e divulgação de informações sigilosas que resultaram no escândalo conhecido como "*Cablegate*"<sup>35</sup>. Sua detenção foi realizada em maio de

---

<sup>33</sup> Capture a Bandeira, em tradução livre.

<sup>34</sup> Informação disponível em <<https://CryptoRave.org/>> Acesso em 30 de novembro de 2016

2010, enquanto servia às tropas norte-americanas no Iraque e foi liberada finalmente de sua prisão em 2017.

Figura 4 - Foto de Manning de peruca e maquiada. Ela enviou para seu supervisor em 2010



Fonte: <https://www.independent.co.uk/>

A palestra que inaugura este espaço em 2016 é de Sergio Amadeu e Matheus Cassina, chamada de “*Hacking Team na América Latina: conceitos técnicos e exemplos*”<sup>36</sup> que versa sobre o vazamento de aproximadamente 400 Gb de informação da empresa italiana *Hacking Team*<sup>37</sup>, incluindo códigos, e-mails, contratos e documentação interna. Relacionado diretamente com esta primeira palestra temos “Vigiando os dissidentes nas ruas”<sup>38</sup>, onde Dia Kayyali se aprofunda na história da vigilância estatal, desde os anos 1960 até hoje em dia, com o intuito de responder como algumas manifestações políticas seriam reprimidas se a vigilância que está inscrita na nossa sociedade hoje em dia fosse realidade algumas décadas atrás.

“*Hacking Team na América Latina*” e “Vigiando os dissidentes nas ruas” adentram a indagação ciberativista de como a nossa realidade contemporânea é penetrada por mecanismos de vigilância nas mais diferentes esferas de existência. Empresas com escândalos de vazamentos de informações; câmeras, softwares e hardwares vigilantes espalhados por todos locais onde a ação humana é possível e

---

<sup>35</sup> O vazamento de telegramas diplomáticos dos Estados Unidos teve início no final de novembro de 2010 quando o site WikiLeaks e cinco grandes jornais publicaram uma quantidade de documentos oficiais sigilosos que detalhavam correspondências entre o Departamento de Estado dos Estados Unidos e embaixadas estadunidenses ao redor do mundo. (UOL, 2010)

<sup>36</sup> Palestra da *CryptoRave* 2016.

<sup>37</sup> Uma empresa cujo produto principal são softwares para vigilância, utilizados por vários governos ao redor do mundo, incluindo regimes violadores de direitos humanos.

<sup>38</sup> Palestra da *CryptoRave* 2016.

mudanças nas legislações de proteção à individualidade e à privacidade são mobilizados dentro da lógica também utilizada por Julian Assange, o jornalista, escritor e ciberativista australiano fundador do maior site de divulgação de vazamentos de informações sigilosas do mundo, o *WikiLeak*, onde:

Ações cotidianas e trocas sociais no ciberespaço tornam-se permeáveis ao rastreamento, constituindo uma fonte valiosa de informação ou conhecimento sobre indivíduos e grupos. Curiosamente, as mesmas tecnologias que ampliam as possibilidades de emissão, acesso e distribuição da informação tornam-se instrumentos potenciais de vigilância e controle; as mesmas tecnologias que possibilitam o anonimato nas relações sociais e comunicacionais mostram-se eficientes instrumentos de identificação.

Paralelamente, o ciberespaço é marcado pela expansão das margens de visibilidade do que costumávamos entender por intimidade, como vimos no capítulo anterior. Parte da sociabilidade na Internet envolve a exposição voluntária de dados pessoais, narrativas e registros diversos da vida cotidiana (ASSANGE, 2013, p. 125)

Julian Assange traz aos seus leitores a dupla face da vigilância, onde tecnologias que ampliam a distribuição da informação podem tornar-se instrumentos potenciais de vigilância e controle. Neste mesmo sentido, mas sob o viés de uma área pouco explorada na *CryptoRave* temos a palestra “1984, hoje – Você está sendo vigiado<sup>39</sup>” de Bruno Wagner e Renata Nobre, que relaciona literatura com estudos de vigilância. A dupla, ao trazer o livro 1984, de George Orwell, uma distopia futurística de um Estado totalitário em que a vigilância em massa permeia a sociedade, expõem situações reais que demonstram que as ideias absurdas daquela época são cada vez mais atuais.

(...) aplicativos de smart TV, celulares e computadores podem ter acesso a camera, fotos e documentos do seu aparelho? Você sabia que o uso das informações geradas por Health trackers já são usadas para monitorar o horário em que as pessoas de uma cidade inteira dormem e acordam? Você já reparou que após uma simples pesquisa de um item que você quer comprar, gera muitas propagandas relacionadas ao produto nas suas redes sociais?” –Bruno Wagner e Renata Nobre (2016), em sua introdução da palestra dada na *CryptoRave*.

A *CryptoRave* nestes espaços, novamente, dilucida aos participantes uma face não tão conhecida do nosso cotidiano de maneiras diferentes. Essa didática que traz, em um mesmo local físico a literatura, a ciência da computação e os

---

<sup>39</sup> Palestra da *CryptoRave* 2016.

estudos de vigilância, possui a intenção de fazer o conteúdo ser absorvido pelos mais diversos participantes.

Como última palestra deste espaço em 2016, “Educando um mini-hacker: introduzindo a cultura hacker para crianças<sup>40</sup>” do professor de matemática Fabio Hirano, traz aos pais de jovens crianças uma discussão que versa como introduzir os conceitos de programação e sistemas computacionais para os hackers mais novos, as contribuições tecnológicas já feitas por crianças e o que esperar de uma geração que já nasceu conectada a uma quantidade de conhecimento inimaginável anos atrás.

A cultura hacker é uma subcultura baseada em entender a fundo uma determinada área do conhecimento, a fim de promover melhorias ou soluções inovadoras. Tradicionalmente, as atividades hacker estão intimamente ligadas à tecnologia. Com as ferramentas que possuímos hoje, conseguimos trazer para as crianças diversas técnicas que, aliadas à capacidade criativa natural delas, podem gerar soluções completamente inesperadas para problemas reais e atuais -Fabio Hirano (2016), em sua introdução da palestra dada na *CryptoRave*.

Claramente, pode-se notar a preocupação dos organizadores do evento em criar métodos nos quais o saber pode ser transmitido para as próximas gerações de maneira interessante e válida, pois este é tido como artifício basilar para a proteção e a segurança dos usuários da Internet. Esta palestra encerra de maneira completa o circuito denominado Espaço Chelsea Manning ao tentar passar para as próximas gerações o conhecimento explorado na *CryptoRave*.

### **4.3 Espaço Edward Snowden: mergulhando nas fronteiras da Internet**

Um dos nomes mais conhecidos quando se trata de Internet e sua exploração para uma agenda de bem maior é o do já citado Edward Snowden. O ex-administrador de sistemas da CIA e ex-contratado da NSA se tornou famoso ao tornar público detalhes de vários programas que constituem o sistema de vigilância global da NSA americana.

O governo espiona todos os cidadãos. E ele também tem um grande medo de que as pessoas saibam que ele espiona. Por isso usa tudo que pode para que essa informação não vaze. Até mesmo intimidações diplomáticas são usadas para impedir que esses dados acabem vazando para o mundo  
—Edward Snowden via Twitter em <<https://twitter.com/snowden>>

---

<sup>40</sup> Palestra da *CryptoRave* 2016.

Snowden defende a divulgação de informações classificadas como "altamente secreta" dentro de seu modo de ver o mundo. Ele protege a decisão que fez sob a ideia de que sua ação vai ajudar o povo dos EUA, que agora tem "o poder de decidir por eles mesmos se estão dispostos a ceder a sua privacidade a um estado de vigilância constante".

Quando você é a organização mais poderosa do mundo, isso é muito perigoso. Mas uma decisão ruim da autoridade mais poderosa do mundo pode afetar milhões de vidas. Até bilhões. Por isso é preciso haver controles rigorosos e um alto padrão de responsabilidade entre as autoridades do governo." –Edward Snowden via Twitter em <<https://twitter.com/snowden>>

Segundo as ideias de Snowden, este espaço da *CryptoRave* tem como foco a desmistificação e o compartilhamento de técnicas de *hacking* e exploração dos limites da Internet. A palestra de Thais Siqueira e Caio Wagner inaugura este espaço; colaboradores do Pixelated<sup>41</sup>, eles trabalham há alguns anos com desenvolvimento de software e ultimamente vêm se envolvendo cada vez mais com assuntos como criptografia, Internet livre e democrática para todos, privacidade e direitos fundamentais dos indivíduos na Internet.

"Por que a privacidade importa?<sup>42</sup>", palestra também de Thais e Caio, explora a carreira de Edward Snowden no sentido de exibir e explorar como e por que os dados publicados ou mesmo comunicações através da web são sistematicamente interceptados e analisados pela Agência Nacional de Segurança dos Estados Unidos. A ameaça ao direito constitucional do indivíduo é, também, tema central desta palestra.

Já, "Capitalismo de vigilância e a ameaça a direitos humanos na era pós-Snowden<sup>43</sup>" do Núcleo de estudos em Tecnologia e Sociedade da USP (NETS/USP) retomada o caso Snowden sob novo enfoque, com destaque às possíveis intersecções entre os temas de vigilantismo e proteção de dados a partir do conceito de capitalismo de vigilância e da consideração da privacidade como um direito humano.

---

<sup>41</sup> Cliente de e-mail que une a usabilidade do e-mail moderno com a privacidade da criptografia.

<sup>42</sup> Palestra da *CryptoRave* 2016.

<sup>43</sup> Palestra da *CryptoRave* 2017.

Por outro lado, a palestra “Construindo hardware para criptografia, o que é preciso considerar?”<sup>44</sup> de Luckas Judocka aborda mecanismos de construção de hardware dedicado para criptografia. Esta atividade pretendeu responder perguntas muito pontuais sobre ciência da computação e explorar uma aula coletiva complexa.

Adentrando mais uma óptica dentro do mesmo estilo de temática, Florence traz a discussão “Cabos submarinos, acesso à Internet, vigilância e geopolítica – quais desafios para o Brasil<sup>45</sup>” à *CryptoRave* explanando quais benefícios para o Brasil em termos de melhoria da qualidade e do acesso à banda larga o termo de parceria entre o Brasil, o Camarões e a China assinado em 2015 para a construção de um cabo submarino Sul-Sul entre Fortaleza e o Camarões poderá trazer e quem são os atores do consórcio que realizará a gestão do cabo após sua construção.

Destarte, o espaço de Edward Snowden na *CryptoRave* consegue instigar nos seus participantes o desejo de relacionar saberes das relações internacionais políticas com as ciências da computação. Isto posto, situações complexas que são abordadas quando a privacidade e a segurança entram em jogo podem ser mais bem entendidas

#### **4.4 Espaço Alan Turing: ferramentas e oficinas necessárias para a segurança na rede**

O espaço de Alan Turing foi feito para divulgação de oficinas práticas de instalação e uso de ferramentas de comunicação segura, privacidade e proteção de dados. Este recebe esse nome devido ao influente matemático que participou do desenvolvimento da ciência da computação e da formalização do conceito de algoritmo e computação com a máquina de Turing<sup>46</sup>, desempenhando um papel importante na criação do computador moderno. Alan era homossexual e isso resultou para ele em um processo criminal em 1952, pois atos homossexuais eram ilegais no Reino Unido na época. Suicidou-se em 1954, depois de ter feito tratamento com hormônios femininos e castração química, como alternativa à

<sup>44</sup> Palestra da *CryptoRave* 2016.

<sup>45</sup> Palestra da *CryptoRave* 2016.

<sup>46</sup> A Máquina de Turing é um dispositivo teórico conhecido como máquina universal, pensada muitos anos antes de existirem os modernos computadores digitais. Em resumo, é um modelo abstrato de um computador, que se restringe apenas aos aspectos lógicos do seu funcionamento.



prisão. Sua história é uma inspiração para matemáticos e defensores dos direitos humanos até hoje.

Thais Siqueira e Denis Costa, os já citados anteriormente colaboradores da Pixelated, voltam a este espaço da *CryptoRave* em 2016 homenageando Alan Turing ao trazerem a oficina “Senhas e gerenciadores de senha<sup>47</sup>”. Nesta aula aberta, o objetivo central é aprender que uma senha forte não é necessariamente uma senha difícil de lembrar e como memorizar senhas pode se tornar algo do passado.

Todos os dias, criamos usuários e senhas nos mais diversos serviços. Com o passar do tempo, os requerimentos foram ficando mais complexos com números, letras minúsculas, letras maiúsculas, pontuação e mais caracteres. Por outro lado, cada vez mais, ouvimos falar de serviços sendo invadidos e informações sendo roubadas. O que demonstra o quão importante é não usarmos a mesma senha em serviços diferentes. -Thais e Denis (2016), em sua introdução da oficina dada na *CryptoRave*.

A oficina de Thais e Denis homenageia Alan, que trabalhou anos num centro especializado em quebra de códigos e por um tempo foi chefe do Hut 8, a seção responsável pela criptoanálise da frota naval alemã e o planejamento de uma série de técnicas para quebrar seus códigos. Senhas e materiais de criptografia que são usados hoje diariamente atualmente são frutos de pesquisas como as de Turing.

Outra oficina, a de Luciano Ramalho, Technical Principal na ThoughtWorks<sup>48</sup> e co-fundador do Garoa Hacker Clube<sup>49</sup> tem foco no público denominado pelo palestrante como “curiosos”, pessoas sem conhecimento prévio em áreas da ciência da computação que querem entender um pouco mais sobre criptografia. Tal oficina apresenta, com exemplos simples, os principais fundamentos da criptografia. Tópicos como letras versus byte; códigos e cifras; algoritmos de chave pública; algoritmos de chave privada; fontes de dados; e como bolar uma boa senha são pontos focais explorados por Luciano em “Códigos e cifras – criptografia para curiosos<sup>50</sup>”.

---

<sup>47</sup> Palestra da *CryptoRave* 2016.

<sup>48</sup> *ThoughtWorks* é uma consultoria global em tecnologia de informação (TI) que tem como foco o desenvolvimento de software. Disponível em <<https://www.thoughtworks.com/pt>> Acesso em 30 de novembro de 2016

<sup>49</sup> Disponível em <[https://garoa.net.br/wiki/Garoa\\_Hacker\\_Clube:Sobre](https://garoa.net.br/wiki/Garoa_Hacker_Clube:Sobre)> Acesso em 30 de novembro de 2016

<sup>50</sup> Palestra da *CryptoRave* 2016.

Parceiros de Luciano na *ThoughtWorks* Brasil e Consultores da mesma, os apresentadores da palestra “Confia no comunicador que está usando?”<sup>51</sup> são Giovane, desenvolvedor e entusiasta em internet livre e direitos digitais que atualmente participa em uma iniciativa que busca melhorar ou criar ferramenta relacionadas a segurança e privacidade na internet.

Várias aplicações para computadores que são utilizados para a troca de mensagens cifradas já existem, provendo mais privacidade e em alguns casos, mais segurança. Thais e Giovane expõem o fato e lutam contra estes softwares não olharem a segurança por padrão, evitando que os usuários tenham que tomar decisões sobre coisas que muitas vezes eles não têm conhecimento.

#### 4.5 Espaço Ada Lovelace: Gênero, sexualidade e feminismo na *CryptoRave*

Figura 5 - Uma ilustração de Ada feita para a en:Ada Initiative



Fonte: [vhttps://adainitiative.org/](https://adainitiative.org/)

Dando uma guinada um pouco diferente ao esperado de um evento focado em questões relacionadas com ciência da computação e suas implicações dentro do âmbito de privacidade e vigilância, o Espaço Ada Lovelace tem como objetivo explorar a temática da sexualidade e suas implicações no que tange ao acesso para pessoas que sofrem com a desigualdade de gênero à tecnologia.

Ada Augusta King, Condessa de Lovelace foi uma matemática e escritora inglesa. Reconhecida atualmente principalmente por ter escrito o primeiro algoritmo para ser processado por uma máquina analítica.

---

<sup>51</sup> Palestra da *CryptoRave* 2016.

Mariana Pita, jornalista e membra do conselho do Coletivo Intervezes e Fernanda Bruno, Professora e Membro fundador da Rede Latino-americana de Estudos sobre Vigilância, Tecnologia e Sociedade/LAVITS<sup>52</sup> examinam em “Algoritmos & discriminação<sup>53</sup>” os pré-conceitos que estão sendo mediados no uso de algoritmos para definição de cada vez mais atividades na vida das pessoas. A palestra trabalha a desmistificação da ideia de que uma sociedade “quantificada” e baseada em algoritmos é uma sociedade mais justa e igualitária.

Sob o fluxo visível das trocas e conversações sociais, constitui-se um imenso, distribuído e polivalente sistema de rastreamento e categorização de dados pessoais que, por sua vez, alimenta estratégias de publicidade, segurança, desenvolvimento de serviços e aplicativos, dentro e fora destas plataformas. Cruzando este processo, empresas e governos especializam-se em monitorar e coletar rastros, gerados pela navegação de usuários na Internet, construindo bancos de dados e técnicas de composição de perfis que orientam ações comerciais, políticas, securitárias, administrativas. (BRUNO, 2013, p. 09)

Bruno e Pita denunciam estes sistemas de categorização e rastreamento, pontuando como podem ser usados para um monitoramento dos mais diversos aspectos do cotidiano das pessoas. Sendo fins lucrativos, com propagandas e anúncios ou fins de pura vigilância o propósito deles.

Adentrando diretamente questões de gênero, a roda de conversa “Visibilidade e vigilância sobre corpos virtuais femininos<sup>54</sup>” apresentada e moderada por Fernanda Shira com a participação de Gabi Juns, Patricia Cornils, Bárbara Paes, Karen Ka e Fernanda convida mulheres que trabalham com segurança, comunicação e direitos digitais para conversar sobre a vigilância e visibilidade sobre corpos virtuais femininos e estratégias para apropriação das tecnologias livres com o intuito de aumentar o arsenal da luta feminista.

A internet e as novas formas de comunicação digital proporcionaram o acesso do público feminino a uma nova esfera de debate, articulação e mobilização *on-line*. O discurso que antes era confinado a ambientes privados foi compartilhado com um público amplo e impulsionou grupos feministas a deslanchar campanhas nas redes sociais. No território virtual o corpo feminino se sente empoderado com as novas ferramentas disponíveis, mas também sofre com o sexismo que é reproduzido e ampliado no ambiente *on-line*. Além disso, esses debates e violências acontecem em redes comerciais que oferecem serviços em troca das

<sup>52</sup> Disponíveis em <<http://lavits.org/?lang=pt>> Acesso em 30 de novembro de 2016

<sup>53</sup> Palestra da *CryptoRave* 2016.

<sup>54</sup> Palestra da *CryptoRave* 2016.

nossas informações e pouco fazem para proteger as agressões racistas e machistas –Fernanda Shira (2016), em sua introdução da roda de conversa feita na *CryptoRave*.

Em diálogo com a roda de conversa, Inês Nin, artista, educadora e pesquisadora de questões relacionadas à subjetividade, autonomia, lugares e rotas de fuga, percorre em “Desaparecer e diluir identidades: condvíduos, máscaras e personas fugidias<sup>55</sup>” Personagens forjadas, pseudônimos, heterônimos, figuras ficcionais, imagens construídas são alguns dos conceitos explorados sob a luz da questão “seriam maneira que pessoas encontraram de camuflar suas “verdadeiras” identidades, ou simplesmente outros modos de agir?”.

Inês vai contra a política de nomes e números, que rastreia, mapeia e monitora indivíduos e propõe a criação de personas, anedotas, versões variantes de um paradeiro, imagens, estratégias, ações, respostas absurdas com o objetivo final de causar confusão. A sua atividade é dividida entre oficina e exposição de trabalhos relacionados às temáticas centrais da palestra.

A última palestra do espaço Ada Lovelace em 2016 é ministrada por Yaso, na qual a distribuição dos meios de produção, baseada em software e hardware livre é o foco. Movimentos de faça você mesmo foram influenciados por este modo de distribuição e essa junção tem beneficiado muitas pessoas ao redor do mundo que sofrem por estarem fora dos processos legais de produção e venda.

O palestrante defende que a descentralização desses meios e da Web pode ser a próxima fronteira para a autogestão de recursos e a eliminação de intermediários exploradores. Este modo de pensamento é algo comumente inscrito na lógica pertencente a participantes de *CryptoParties* e simpatizantes do software livre, onde modos de mudança do mundo são pensados via Internet.

A Coding Rights, uma organização de direitos digitais liderada por mulheres, desenvolve na *CryptoRave* o *workshop* “Violência *on-line*, privacidade e anonimato<sup>56</sup>” que explora quem é e quem mais sofre violência *on-line*, táticas de defesa, a posição do poder público, privado e perspectivas legais. Segundo a organização a ideia foi pensar como fazer frente aos ataques racistas, sexistas e a repressão política *on-line* sem ampliar os poderes de censura e vigilância de Estado e empresas.

---

<sup>55</sup> Palestra da *CryptoRave* 2016.

<sup>56</sup> *Workshop* da *CryptoRave* 2017.

Entre as palestras deste espaço, Camille Laurent em “Art e tecnologia<sup>57</sup>” divulga aos participantes uma oficina prática de introdução à tecnologia na área das artes. Esta oficina é a continuidade de uma instalação de luz que foi realizada para a balada da *CryptoRave* e se organiza em três partes, a primeira conta com a introdução e a influência do uso da tecnologia na arte; a segunda, foca nas noções sobre a arte de hackear e como o artista se apropria o conceito do *hack*; e a terceira, uma oficina prática, ensina a hackear algumas luminárias do centro cultural e montar uma programação com o intuito de controlar as luminárias.

O espaço Ada Lovelace fica assim como uma oportunidade de mostrar que tramas labirínticas de uma realidade vigiada como a questão da identidade e do nosso poder de ação podem ser estudadas e entendidas por outros meios, não só apenas a ciência dura da computação e da criptografia. A arte é introduzida como meio de sorver o mundo computadorizado e moderno dos dias de hoje.

#### **4.6 Espaço Ian Murdock: segurança digital pessoal**

O último espaço apresentado pela *CryptoRave* ganha o nome de Ian Murdock. Ian foi um engenheiro de software americano, melhor conhecido por ter sido o fundador do projeto Debian e do Progeny Linux System, uma companhia comercial Linux. Murdock foi encontrado morto em 2015, sob circunstâncias até hoje nunca explicadas.

Seu espaço tem como foco central a segurança pessoal digital. Palestras voltadas aos cuidados do usuário, tanto experiente quanto amador, são apresentadas com o intuito da distribuição de saber.

Este espaço é inaugurado em 2016 por Alex Nunes com sua palestra “Ameaças móveis, arquitetura, vulnerabilidades e reações corporativas<sup>58</sup>”. Pesquisador independente e entusiasta tecnológico, o palestrante tem desenvolvido experimentos de quebra de segurança a mais de 10 anos. Atualmente tem pesquisado e desenvolvido técnicas de subversão voltadas para dispositivos móveis e sistemas embarcados e faz disso o foco de sua apresentação.

---

<sup>57</sup> Palestra da *CryptoRave* 2016.

<sup>58</sup> Palestra da *CryptoRave* 2016.

A última grande onda digital tem sido pautada por tecnologias em dispositivos móveis, fiel companheiro dos seus usuários estes dispositivos em larga escala expõem um ambiente rico para formas criativas de subversão. A palestra irá demonstrar algumas ameaças, tentativas corporativas de mitigação e resultados práticos da sua exploração. –Alex Nunes (2016), em sua introdução da palestra da *CryptoRave*.

Euler Neto, bacharelando do último período de Ciências da Computação da Universidade Federal de Sergipe é entusiasta da área de segurança da informação e de redes de computadores e computação forense. A palestra “Explicando segurança e privacidade com *Wireshark*<sup>5960</sup>”, de Euler, tem como objetivo utilizar o software para mostrar como os dados trafegam na rede, mostrando exemplos de capturas em determinados cenários e discutindo a importância da segurança em cada um deles para não deixar informações expostas como senhas, números de cartão de crédito, entre outros. São discutidas também algumas técnicas que podem contornar métodos de vigilância sem discutir detalhes técnicos de como são feitos os ataques à privacidade, e sim que medidas podem ser tomadas para que uma pessoa saiba que está sob ataque. A partir disso, o Tor será demonstrado aos expectadores como um software que vem incomodando tanto grandes empresas quanto governos.

Estas duas primeiras apresentações deste espaço têm como público pessoas mais especializadas em questões de segurança em computadores pessoais. O espaço Ian Murdock pode ser considerado o mais “fechado” da *CryptoRave* ao possuir palestras com temáticas mais focadas em assuntos herméticos da ciência da computação. Um bom exemplo desse conteúdo profundo e não estudado cotidianamente, além das conferências inaugurais do espaço, pode ser visto em “[IN]Secure Healthcare Systems<sup>61</sup>”, aula de Arthur Paixão sobre a forte tendência de crescimento do uso de tecnologia na indústria da saúde e como isso traz grandes prejuízos causados pela falta de maturidade no ciclo de desenvolvimento de software relacionado à segurança da informação.

O palestrante pós graduando em Computação Forense e Perícia Digital faz os participantes imaginarem o que poderia acontecer se o resultado de um exame médico fosse alterado ou se mudássemos a dosagem de algum medicamento

---

<sup>59</sup> Palestra da *CryptoRave* 2016.

<sup>60</sup> O *Wireshark* é um programa que analisa o tráfego de rede, e o organiza por protocolos. Disponível em <<https://www.wireshark.org/>> Acesso em 30 de novembro de 2016.

<sup>61</sup> Palestra da *CryptoRave* 2016.

crítico; e se suas informações clínicas fossem vendidas no mercado negro para empresas de plano de saúde. Sendo assim, a apresentação mostra o quão perigoso pode ser uma simples consulta ao médico e que tipo de riscos estamos expostos.

Ao fim da *CryptoRave* 2016, a exposição “O que os metadados<sup>6263</sup> podem revelar sobre nossas vidas? (A análise dos metadados do caso *Hacking Team*<sup>64</sup>)” busca mostrar a dinâmica dos metadados em uma sociedade conectada e repleta de aparelhos e dispositivos cibernéticos. Matheus Cassina procura entender os diferentes tipos de metadados, de um simples software de edição de texto até os metadados de um roteador ou de um sensor da chamada IoT (internet das coisas).

Para evidenciar o potencial de tratamento de metadados, o palestrante evidencia o caso do vazamento dos cabeçalhos de e-mail do *Hacking Team*. Eles permitem identificar a movimentação do grupo, seus líderes, suas viagens e a missão de seus funcionários, mostrando assim, por fim, que o conhecimento sobre metadados é um elemento fundamental da luta pela privacidade.

A palestra de Cassina ilustra o espaço de Ian Murdock de uma maneira muito sólida. Envolvendo conhecimentos de segurança pessoal digital e uma análise de uma situação onde a falta de cuidados do usuário, neste caso, a *HackingTeam*, levou a empresa a uma situação vulnerável.

Com isto finalizamos a abordagem de cada um dos espaços. Em seguida será feita uma análise do evento.

---

<sup>62</sup> Palestra da *CryptoRave* 2016.

<sup>63</sup> Metadados são dados sobre outros dados. Os metadados facilitam o entendimento dos relacionamentos e a utilidade das informações dos dados.

<sup>64</sup> *Hacking Team* é uma empresa de TI com sede em Milão, que vende ferramentas para ataques de acesso e vigilância.

## 5. ANÁLISE DA *CRYPTORAVE*

Após termos contato com a grande maioria das palestras das últimas edições da *CryptoRave*, divididas em seus grandes seis espaços, podemos desenvolver uma análise sobre o evento. Antes de adentrar em observações sobre o saber divulgado pelo sucedido, é interessante lembrar alguns dados dele.

Envolvendo palestras sobre privacidade e vigilância, criptografia, ciência da computação, ativismo, direitos humanos, legislação e artes diversas, a autodenominada “maior festa da criptografia brasileira” mergulha em muitos tópicos diferentes, mas sempre com um mesmo ideário: ensinar aos participantes criptografia, liberdade na Internet e privacidade. Isso tudo mobilizando profissionais das áreas de tecnologia da informação, advogados, artistas, ativistas, cientistas da computação, engenheiros, escritores, estudantes, jornalistas, pesquisadores, professores, sociólogos, psicólogos etc.

Ao topo disso, a *CryptoRave* conseguiu ultrapassar em 15% a sua meta de arrecadar R\$ 45 mil (dinheiro usado para organização, aluguel e despesas do espaço) em 2016 e em 16% em 2017 sua meta de R\$ 60 mil, divulgada pelo Catarse, um site de financiamento coletivo *on-line*. Este número mostra a confiança dos participantes na qualidade do evento e em seu potencial e reforça o mesmo no patamar de maior *CryptoParty* do Brasil.



Abordando a questão de gênero, o evento em 2016 contou com quarenta e oito palestrantes autodeclarados<sup>65</sup> homens e vinte e três pessoas palestrantes autodeclaradas mulheres, fazendo assim uma contagem de 67,6% de homens e 32,4% de mulheres. Este número pode ser visto como positivo, quando é levado em conta que, por exemplo, nos cursos relacionados à informática do Brasil, apenas 15%<sup>66</sup> do alunato é feminino.

Em 2017, a participação de palestrantes mulheres aumentou em 21,74% em relação ao ano anterior, ao termos vinte e oito pessoas autodeclaradas mulheres e quarenta e seis autodeclaradas homens. Esse aumento no número total de participantes mulheres pode ser explicado pela *CryptoRave* ser um evento com uma forte vertente feminista, no qual ocorre a participação de coletivos como o já citado *Coding Rights*, que possui como pauta a luta pela presença maior da mulher em áreas dominadas por homens como a ciência da computação, programação e tecnologia da informação.

Para além da presença de coletivos feministas na organização do evento, o próprio evento possui o também já citado Espaço Ada Lovelace onde questões de gênero tomam a dianteira nas palestras e *workshops*. A discussão sobre gênero faz com que a privacidade e a luta contra a vigilância fiquem em uma posição até secundária, mas isso, segundo os organizadores, permite que a conscientização da luta feminista possa atingir pessoas que talvez não tenham tanto contato com essa temática de estudo de uma maneira diferenciada e aberta.

Ambas as edições contaram com a presença de advogados, artistas, ativistas, cientistas da computação, engenheiros, escritores, estudantes, jornalistas, pesquisadores, professores, sociólogos, técnicos em informática, psicólogos etc. criando um evento interpenetrado pelas mais diversas áreas do saber.

Abordando a temática dos saberes mobilizados pela *CryptoRave* durante as palestras, oficinas e aulas, é de suma importância para uma análise do evento reforçar como a privacidade e a vigilância são tratadas e politizadas neste meio. O livro de Fernanda Bruno (apresentadora de duas palestras do evento em 2016)

---

<sup>65</sup> Alguns participantes da *CryptoRave* usam codinomes neutros e /ou não se identificam com gêneros binários, então, estes números apenas contam com quem divulgou seu nome verdadeiro no site oficial do evento.

<sup>66</sup> Informação disponível em <<https://oglobo.globo.com/sociedade/tecnologia/mulheres-ainda-sao-poucas-no-mercado-de-computacao-12242530>>. Acesso em 28 de janeiro de 2017.

chamado “Máquinas de ver, modos de ser” exemplifica muito bem a parte mais filosófica desta questão:

Toda vigilância, como se sabe, implica não apenas a observação de indivíduos e populações, mas a produção de um saber que permita governar as suas condutas (Foucault, 1994; Rose, 1999). Se tomarmos como referência as análises de Foucault sobre os dispositivos de vigilância na modernidade (...), identificamos dois elementos centrais: o olhar (as táticas do ver e do ser visto) e as técnicas de coleta, registro e classificação da informação sobre os indivíduos. Ou seja, além do olhar (...), a informação é um outro elemento-chave dos processos de vigilância. O alcance e os efeitos da observação disciplinar requeriam também todo um “sistema de registro intenso e de acumulação documentária (...) com seus métodos de identificação, de assimilação ou de descrição” (Foucault, 1983, p. 168). Na escola, no exército, na fábrica, nos hospitais, nas prisões, os sujeitos são ao mesmo tempo olhados e objetivados através de exames que irão constituir registros dos seus dados individuais (suas competências, evoluções, falhas, sintomas, características físicas e psíquicas, biografia etc.) e organizar campos comparativos que permitam classificar, estabelecer médias e fixar normas (Idem, p.169). (BRUNO, 2013, p. 145)

Esta relação entre o olhar e as técnicas de coleta é talvez o ponto onde toda a *CryptoRave* converge. Ao expor como no nosso cotidiano somos interpenetrados por mecanismos de controle de que não temos conhecimento, as palestras de todos os espaços nos oferecem métodos diversos para lutarmos contra a vigilância, e ao fazer isso, mostram ao espectador a necessidade do discurso sobre tais tópicos ser politizado e levado a sério.

Em relação às questões de privacidade e vigilância, das mais de cinquenta palestras do evento em 2016, pelo menos oito tratam diretamente de criptografia e, em 2017, das quase cem palestras, doze têm este foco, incluindo muitos workshops apresentados neste espaço de como podemos aprender a usá-la no dia a dia e em situações que exigem uma complexidade maior. A criptografia, como pode ser visto nos conteúdos das palestras e *workshops*, é tratada no ambiente da *CryptoRave* como algo extremamente importante, capaz de mudar o mundo. Podemos observar este mesmo sentimento nesta citação de Julian Assange:

(...) o universo, o nosso universo físico, apresenta essa propriedade que possibilita que um indivíduo ou um grupo de indivíduos codifique algo de maneira confiável, automática e até inconsciente, de forma que nem todos os recursos e nem toda a vontade política da mais forte superpotência da Terra será capaz de decifrá-lo. E as trajetórias de criptografia entre as pessoas podem se fundir para criar regiões livres das forças repressoras do Estado externo. Livres da interceptação em massa. Livres do controle

do Estado. Desse modo, as pessoas poderão se opor a uma superpotência plenamente mobilizada e vencer. A criptografia é uma incorporação das leis da física e não se deixa abalar pela petulância dos Estados nem pelas distopias da vigilância transnacional.

Não está claro se o mundo terá de ser realmente assim. Mas, de uma forma ou de outra, o universo recebe a criptografia de braços abertos.

A criptografia é a derradeira forma de ação direta não violenta. (ASSANGE, 2013, p. 28)

Ao lermos este trecho, confirmarmos, como dito acima, que a criptografia é algo muito além do que é mobilizado diariamente pelos internautas. Para Assange, esta mesma tecnologia que faz o usuário comum proteger sua conta numa rede social ou seu login no computador pode criar uma realidade em que a informação pode fluir livremente, sem um controle estatal nocivo ao fluxo interacional das pessoas na rede digital.

Para resumir, a tão citada palavra “criptografia” tem origem no termo grego para “escrita secreta” e designa a prática de se comunicar em código [fonte?]. Em nossa realidade atual, a criptografia é algo muito mais incorporado às nossas redes sociais, tanto analógicas quanto digitais.

Basicamente nada do que fazemos está distante de ser relacionado com a criptografia ou alguma coisa criptografada. Nossos smartphones, contas no banco, senhas para toda e qualquer coisa, códigos de sites que visitamos; tudo isso é, em algum nível, criptografado com o intuito de proteger o que quer que deva ser protegido.

Acho que a única defesa eficaz contra a iminente distopia da vigilância é aquela em que cada um toma medidas para proteger a própria privacidade, porque os grupos capazes de interceptar tudo não têm incentivo algum para reduzir o próprio controle. Uma analogia histórica seria o modo como as pessoas descobriram que precisavam lavar as mãos. Essa mudança exigiu a consolidação e depois a popularização da teoria do germes da doença e demandou o enraizamento da paranoia em relação ao alastramento da doença por meio de alguma coisa na nossa mão que não podia ser vista, da mesma forma como não dá pra ver a interceptação em massa. Quando esse conhecimento se propagou o suficiente os fabricantes de sabonete se puseram a fabricar produtos que as pessoas consumiam para aliviar o medo. É necessário instilar medo nas pessoas para que elas compreendam o problema antes de uma demanda suficiente ser criada para solucioná-lo. (ASSANGE, 2013, p. 82).

A questão da criptografia para um evento como a *CryptoRave* tem raízes em discussões sobre até que ponto a criptografia pode ser usada para “melhorar” o

mundo em que vivemos. Como ela pode ser ensinada e manipulada pela sociedade; como ela pode ser descoberta e incorporada ao senso comum para transformar a troca de informações em algo seguro e fora do controle estatal, em resumo, livre.

A força de praticamente todas as autoridades modernas provém da violência ou da ameaça de violência. É preciso reconhecer que, com a criptografia, nem toda a violência do mundo poderá resolver uma equação matemática. (ASSANGE, 2013, p. 80)

A criptografia é um método para escapar esta supracitada violência e ameaça de violência<sup>67</sup>. Ao criptografar robustamente algo, transformamos a informação em algo protegido por fórmulas matemáticas complexas que apenas pessoas que possuem a senha necessária podem acessar.

Dito isso, e tendo visto como ocorreu o evento e sua formação, podemos entender como é realizada a politização dos tópicos centrais tratados pela *CryptoRave*. A análise será dividida em dois pontos: a) de que forma a *CryptoRave* constrói a questão da privacidade como um problema social; b) qual a solução proposta no evento para esse problema.

#### a) A privacidade como problema social

Usando a teoria de John Hannigan sobre a construção de problemas sociais seguimos traçar uma ligação direta entre o que é sugerido pelo autor e o que ocorre no evento.

Segundo Hannigan, central para a construção de problemas sociais é a ideia de que estes não surgem e somem de acordo com um conjunto de critérios fixo, associal e autoevidente. Em vez disso, o seu progresso varia em resposta direta ao sucesso de "fazer reivindicações" por um elenco de atores sociais que inclui cientistas, industriais, políticos, funcionários públicos, jornalistas e ativistas (HANNINGAN, 2006).

Neste caso a *CryptoRave* surge como um conjunto de atores sociais das mais diversas áreas que tem como objetivo informar os participantes, via palestras

---

<sup>67</sup> Violência aqui não precisa ser entendida necessariamente como violência física. A opressão da fala, a monitoração ilegal da vida cotidiana e muitas outras violências simbólicas entram neste âmbito.

e *workshops*, sobre questões como a falta de privacidade, a necessidade de criptografia e a luta contra a vigilância para que estas questões possam se transformar em problemas sociais bem construídos, para então o “peso” destas questões aumentar e poder assim desenvolver mais o potencial e possíveis maneiras de mudança do *status quo*.

E é seguindo este movimento de ensino e busca de informação que a politização de um assunto antes desconhecido e com uma técnica hermética começa a acontecer. Ao trazer ao público, por intermédio de um evento aberto, o conhecimento da criptografia e seus usos para a proteção de dados, navegação privativa e muitos outros, pessoas que não tinham acesso a esta questão podem se inteirar e fazer desta ferramenta um instrumento de proteção e até mesmo, luta.

Com a privacidade em conta, a *CryptoRave* expõe cada vez mais um fator cotidiano que apenas há pouquíssimo tempo – devido a divulgações de notícias envolvendo vazamentos de dados e espionagem, principalmente – começou a ser levado a sério e entendido como pauta de discussão importante, a questão de que: devemos ter direito à privacidade em todos âmbitos, inclusive na Internet. Ao usar de exemplos simples em palestras, como notícias divulgadas por grandes meios jornalísticos, a importância da legislação da rede mundial de computadores, o Marco Civil da Internet, a Neutralidade da Rede, e outros temas relacionados à regulamentação da Internet são expostos, relacionados e abrangidos.

A mobilização técnica-política também se faz vista fortemente no mote da luta contra a vigilância; esta que, como mostrado anteriormente, nasce de uma mobilização que data do começo do ciberativismo e teve grande intensificação com a criação do site *WikiLeaks*. Ao utilizar o conhecimento técnico, na *CryptoRave* diversos estudiosos se reúnem para mostrar como e por que em diversos aspectos a vigilância deve ser combatida e cada vez mais tomada como questão política e problemática.

O vetor central para que isso aconteça é o entendimento histórico de que a vigilância implica não apenas a observação de indivíduos e populações, mas a fabricação de um saber que permita governar as suas condutas e ações. Isto, por intermédio de uma aproximação histórica, é exposto para uma conscientização do poder que a Internet, quando administrada com determinada intenção, pode ter.

Temos como exemplos empíricos do que foi dito acima as já citadas palestras “Privacidade, liberdade de expressão e governança global”, são centradas em mostrar como o direito à privacidade e liberdade de expressão na Internet é tratado atualmente por órgãos governamentais e instituições internacionais e “Por que a privacidade importa?”, que exhibe como e por que dados, arquivos, materiais publicados ou até mesmo comunicações através da Internet são sistematicamente interceptados e analisados pela Agência Nacional de Segurança dos Estados Unidos.

Além dessas palestras (e de muitas outras ao longo do evento), a *keynote* “Marco Civil e CPI dos Cibercrimes” apresenta a importância da discussão legal sobre privacidade como um direito ao explorar o Marco Civil e como ele tem como objetivo funcionar como uma espécie de “constituição do mundo virtual”, estabelecendo deveres, condutas, direitos e garantias para o uso da Internet no Brasil

Dessa forma, conseguimos entender como a *CryptoRave* constrói a questão da privacidade como um problema social. Podemos em seguida averiguar a proposta do evento para tal problemática.

#### b) A tecnopolítica como solução proposta pela *CryptoRave*

Após observarmos como a privacidade se constrói no evento como problema social, temos então a questão da solução proposta pelo evento a isto. A tecnopolítica é explorada pela *CryptoRave* para garantir um empoderamento dos participantes em relação à realidade atual, onde a vigilância se torna cada vez mais espalhada e intensa (BRUNO, 2013, p. 08).

Consultando os dados recolhidos ao longo das pesquisas feitas para escrever este texto e os dados disponibilizados pelos organizadores do evento, temos um panorama interessante: as informações parecem mostrar uma forma de politização que funciona muito mais no sentido de um processo de empoderamento individual. Esse empoderamento tem como mote o domínio da tecnologia e sua utilização no cotidiano e não um processo de organização coletiva para demandar leis ou políticas de defesa da privacidade.

Essa forma de ação se relaciona diretamente com os argumentos da *Lifestyle Politics* de W. Lance Bennett (BENNETT, 2004, p. 03) Para o autor as “políticas do estilo de vida” são caracterizadas por inclinações a questões baseadas em suas associações significativas de identidade social, redes profissionais e pessoais, tendências sociais e diversas preferências particulares. Sendo assim, a “política do estilo de vida” ocorre após uma mudança de paradigma, onde a primazia é o interesse particular de cada um e não uma identificação direta com um movimento, uma classe ou um movimento uniforme.

A lógica de ação personalizada e/ou individualizada do universo dos ciberativistas age nesse sentido e, durante o evento, nota-se a preocupação dos organizadores e palestrantes em mostrar a cada pessoa em particular o porquê da necessidade da proteção na Internet. Desta maneira, a batalha contra a vigilância se faz individualizada, com cada pessoa aprendendo métodos para sua proteção, envolvendo criptografia e tecnologias livres, principalmente.

Neste sentido, os silêncios e ausências falam tanto quanto o que é dito e apresentado. A ausência de discussões mais voltadas a processos de organização e ação coletiva é um claro indicador da opção por outra forma de pensar o ativismo. Temos aqui uma ênfase em uma ação individualizada, baseada no empoderamento a partir do uso dos instrumentos técnicos, ao invés da construção de coletivos ou movimentos sociais.

Podemos notar essa posição nas mais diversas palestras e *workshops* do evento. Como exemplos, temos o “Mini guia para se manter mais seguro na Internet”, que incentiva a mudança comportamental dos participantes do evento para navegar e se comunicar de forma mais segura na Internet e a oficina “Códigos e cifras – criptografia para curiosos”, que tem como público alvo pessoas sem muito domínio de técnicas de criptografia para apresentar com exemplos simples os principais fundamentos desse conhecimento. Além disso, temos “Educando um mini-hacker: introduzindo a cultura hacker para crianças”, que apresenta aos pais de jovens e crianças métodos para introduzir os conceitos de programação e sistemas computacionais para seus filhos. Neste workshop, aparece a preocupação com que, desde cedo, as pessoas possam se empoderar para se proteger da vigilância, e o foco no ensino seguindo a lógica de ação personalizada

e/ou individualizada dos ciberativistas e organizadores, para construir uma próxima geração com maiores conhecimentos de conceitos de computação.

Vale ressaltar também que todo o espaço Alan Turing tem como finalidade apresentar ferramentas e oficinas necessárias para a segurança na rede que tanto pessoas leigas quanto estudiosos possam usar em seu dia a dia. Este espaço une ambas as questões objetivas do evento, politizando e mostrando a utilidade de mecanismos de proteção e ensinando os participantes a utilizá-los em consonância com a tecnopolítica para se empoderarem.

## 6. CONSIDERAÇÕES FINAIS

Ao longo das páginas anteriores, temos a análise de como a *CryptoRave* politiza a questão da privacidade ao apresentar para seu público diversas temáticas que abordam o estudo da criptografia, a luta contra a vigilância do Estado e o direito à privacidade. No capítulo Política, Privacidade e Internet é realizada uma análise na qual dois tópicos, a política e a privacidade, são relacionados a uma temática central: a Internet, para assim poder ser introduzido no capítulo Ciberativismo, Manifestações e Eventos Brasileiros diversas questões que formam as bases da *CryptoRave*. Então é feita uma abordagem descritiva dos Espaços do evento e suas palestras para finalmente chegarmos à análise do evento em si. Sendo assim, chega-se a algumas conclusões sobre o evento e questões relacionadas a ele.

Citado pelos organizadores como o único evento hacker gratuito no Brasil, a *CryptoRave* realiza atividades sobre segurança, criptografia, *hacking*, anonimato, privacidade e liberdade na rede através das já citadas palestras e *workshops*. Cada um dos espaços possui um foco central para as mais diversas áreas de estudo serem atingidas, são eles: Espaço Aaron Swartz, com foco em regulamentação da Internet, anonímia e direitos humanos; Chelsea Manning, centrado nos limites e novidades da criptografia; Edward Snowden, com cerne nas fronteiras da Internet;



Alan Turing, focalizado nas ferramentas e oficinas necessárias para a segurança na rede; Ada Lovelace, com palestras sobre gênero, sexualidade e feminismo; e Ian Murdock, com a temática de segurança digital pessoal.

Essa divisão de espaços cumpre seu papel de atingir conhecimentos diversos e atrair diferentes tipos de interessados, desde estudiosos de tecnologia até interessados e interessadas em movimentos como o feminismo. Antes de focar nas conclusões sobre o objetivo do evento e a politização buscada pelo mesmo, devemos observar questões estatísticas e em relação aos participantes e palestrantes.

No ano de 2016, a *CryptoRave* teve quarenta e oito palestrantes autodeclarados homens e vinte e três pessoas autodeclaradas mulheres. No ano seguinte, a participação de palestrantes mulheres aumentou em 21,74% com vinte e oito pessoas autodeclaradas mulheres e quarenta e seis autodeclarados homens. Isto provavelmente ocorreu devido à grande presença de saberes feministas e da luta pela igualdade de gênero trazida pelos palestrantes. É interessante considerar como hipótese que, em edições futuras, possivelmente irá ocorrer uma igualdade do número de homens e de mulheres; este fato não só para um evento focado em tecnologia, mas praticamente para qualquer tipo de evento é deveras interessante e positivo. Possuir um número de palestrantes de gênero igualitário poderá ajudar a legitimar cada vez mais questões importantes como os direitos das mulheres.

Além disso, como já citado, o evento em 2016 conseguiu ultrapassar em 15% a sua meta de arrecadação R\$ 45 mil e, em 2017, superou em 16% sua meta de R\$ 60 mil. Estes números mostram a confiança dos participantes na qualidade do evento e pode-se supor que o mesmo está em pleno crescimento, com aumento de qualidade e interessados.

Sobre a politização buscada pela *CryptoRave* e seus organizadores, como observado ao longo do texto, ela tem dois objetivos: o primeiro é transformar questões como a luta pela privacidade, a criptografia e a antivigilância em problema social, público e/ou político; o segundo foca na criação de métodos para agir frente a tais problemas.

A propósito do primeiro objetivo podemos constatar que o evento funciona de maneira produtiva, relacionando notícias, diários oficiais, textos e imagens em palestras e *workshops* distintos para a construção da luta pela privacidade e da

batalha antivigilância em problemas sociais por intermédio das reivindicações feitas pelos participantes, palestrantes e organizadores. Sobre o segundo objetivo, nota-se que os métodos para agir frente tais problemas sociais possuem ênfase em uma ação individualizada, baseada no empoderamento a partir do uso dos instrumentos técnicos.

Essa escolha do evento de focar na problematização e politização das temáticas abordadas é aparentemente bem recebida, já que o seu formato se mantém de ano a ano e os números de interessados sempre vêm aumentando. Este fato se mostra em consonância com o segundo objetivo do evento, que é apresentar aos participantes métodos de luta aliados com a tecnopolítica e os dogmas ciberativistas.

Podemos então chegar à conclusão de que a *CryptoRave* cumpre seus objetivos educativos e politizadores ao transformar a privacidade em problema social via informação passada por palestras e *workshops* para assim focar no ensino de forma individual. Ao sugerir a tecnopolítica como solução e mostrar como a criptografia pode ajudar pessoas na sua proteção seguindo orientações ciberativistas, o participante do evento é empoderado.

A criptografia desta maneira é artefato central na luta pela privacidade e seu desenvolvimento e propagação parece ser o instrumento a partir do qual a *CryptoRave* busca concretizar sua ação em defesa da privacidade. Ação não apenas demandando o direito à privacidade, mas ao mesmo tempo construindo e publicitando instrumentos para garantir este direito no cotidiano das pessoas através do engajamento direto destas no uso e difusão da criptografia.

Em relação à importância deste trabalho para a sociologia e as ciências sociais vale ressaltar novamente o ainda incipiente diálogo dessas matérias com as áreas dedicadas ao estudo da Internet, como a comunicação, as ciências da computação, entre outras. Este trabalho serve como mais uma forma de união dessas áreas em um estudo sobre um caso brasileiro, trazendo um panorama atualizado das discussões feitas no âmbito da privacidade, vigilância e tecnopolítica, desta maneira, podendo abrir portas para mais abordagens desse tipo em eventos futuros.

Para análises futuras e sugestões de outras pesquisas, indico explorar, por exemplo, como o feminismo funciona dentro da realidade da *CryptoRave* como

outro método de politização. Além disso, é possível abordar a possibilidade de construção de outros eventos parecidos com a *CryptoRave* por outras cidades do Brasil e como a formação e organização dos interessados pode ocorrer; tópico pouco explorado neste texto.

## REFERÊNCIAS

ASSANGE, J. **Cypherpunks - liberdade e o futuro da internet**. 1. ed. São Paulo: Boitempo, 2013.

BRASIL, **Constituição Federal**, 1988. Disponível em: <<http://www2.planalto.gov.br/acervo/constituicao-federal>>

BENNETT, W. **Branded Political Communication: Lifestyle Politics, Logo Campaigns, and the rise of Global Citizenship**. 1. ed. 2004.

BOWDEN, C. **The US surveillance programmes and their impact on EU citizens' fundamental rights**. 2014.

BRUNO, F. **Maquinas de ver, modos de ser**. 1. ed. Porto Alegre: Editora Sulina, 2013.

CRYPTOPARTY.IN. **Why cryptoparty?**. 2017a. Disponível em: <<https://www.cryptoparty.in/>>.

\_\_\_\_\_. **How to organize a cryptoparty**. 2017b. Disponível em: <<https://www.cryptoparty.in/organize/howto>>.

CRYPTORAVE, Organizadores da. Entrevista concedida a Emílio Fregapani Toscani, 1 out. 2016 [A entrevista encontra-se transcrita no Apêndice “A” desta monografia].

EVANGELISTA, R. **O movimento software livre do brasil: política, trabalho e hacking**. Horizontes antropológicos, 2014. v. 20, n. 41, p. 173–200. Disponível em:

<[http://www.scielo.br/scielo.php?script=sci\\_arttext&pid=S0104-71832014000100007&lng=en&nrm=iso&tlng=pt](http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0104-71832014000100007&lng=en&nrm=iso&tlng=pt)>.

GURAK, L. J. **Persuasion and Privacy in Cyberspace: The Online Protests over Lotus MarketPlace and the Clipper Chip**. New Haven: Yale University Press, 1997.

HANNIGAN, J. **Environmental sociology**. 2º ed. Londres: Routledge, 2006.

HAUBEN, M.; HAUBEN, R. **Behind the net: the untold story of the arpanet and computer science**. First monday, 1998. v. 3, n. 8. Disponível em: <<http://firstmonday.org/ojs/index.php/fm/article/view/612/533>>.

LATOURETTE, B. **Jamais fomos modernos**. 1º ed. São Paulo: Editora 34, 2009.

LETAI, P. **A futile attempt. Spain implements web-blocking regulation**. 2012. Disponível em: <<http://kluwercopyrightblog.com/2012/01/09/a-futile-attempt-spain-implements-web-blocking-regulation/>>

MA, Y. **Stop Online Piracy Act: The Next Step in Copyright Protection or Censorship of Online Expression**. 2015. Disponível em <[http://scholarship.shu.edu/cgi/viewcontent.cgi?article=1667&context=student\\_scholarship](http://scholarship.shu.edu/cgi/viewcontent.cgi?article=1667&context=student_scholarship)>

MALINI, F.; ANTOUN, H. **A internet e a rua: ciberativismo e mobilização nas redes sociais**. 1º ed. Porto Alegre: Editora Sulina, 2013.

ONU. **Declaração Universal dos Direitos Humanos**, 1948. Disponível em: <<https://nacoesunidas.org/direitoshumanos/>>

SILVEIRA, S. A. Da. **Ciberativismo, cultura hacker e individualismo**. Revista USP, 2010. n. 86.

\_\_\_\_\_. **Ferramentas conceituais para a análise política nas sociedades informacionais e de controle**. São Paulo: 35º encontro anual da ANPOCS, 2011.

\_\_\_\_\_; BRAGA, S.; PENTEADO, C. **Cultura, política e ativismo nas redes digitais**. 1º ed. São Paulo: Fundação Perseu Abramo, 2014.

SOLAGNA, F. **A formulação da agenda e o ativismo em torno do marco civil da internet**: Universidade Federal do Rio Grande do Sul, 2015. ISBN 9788578110796.

SOUSA, C. M. De; SOUZA, A. De A. **Jornadas de junho - repercussões e leituras**. 1ª ed. Campina Grande: Editora da Universidade Estadual da Paraíba, 2013.

UOL. **Veja o que já foi divulgado nos documentos vazados no wikileaks**. 2010.

Disponível em: <<http://noticias.uol.com.br/internacional/ultimas-noticias/2010/11/30/veja-o-que-ja-foi-divulgado-nos-documentos-vazados-no-wikileaks.htm>>.

WARREN, S.; BRANDEIS, L. **The right to privacy**. Harvard law review, 1890. v. 4, n. 5.

## **APÊNDICE “A”: Entrevista sobre a *CryptoRave* para o coletivo organizador realizada em 2016.**

### **1. Histórico da *CryptoRave***

Pergunta: Como se originou a *CryptoRave* no Brasil?

Resposta: Em 2013 realizamos a primeira *CryptoParty* em São Paulo. Após muitos interessados comparecerem, nós fizemos uma reunião e pensamos como ampliar o evento. No início de 2014 tivemos a ideia de fazer uma *CryptoParty* de 24 horas.

P: Como as *CryptoParties* influenciaram a criação da *CryptoRave*?

R: A ideia original da *CryptoParty* é de difundir criptografia e privacidade para todos. Essa ideia foi abraçada pela *CryptoRave*. Então em todas as edições tivemos uma série de palestras e oficinas dedicadas a ensinar como usar criptografia.

P: Com que finalidade o evento fora criado?

R: Difundir e semear o debate sobre a segurança e privacidade no Brasil.

### **2. Organizadores**

P: Quem são os participantes do coletivo?

R: A *CryptoRave* não é um coletivo. É um evento organizado por coletivos e indivíduos. Na última edição, de 2016, foram quatro coletivos organizadores: Actantes, Escola de Ativismo, Intervezes, Saravá. Além dos coletivos, há também indivíduos que participam ativamente da organização e há outras organizações que

apoiam o evento com doações e empréstimos de equipamentos. Nesse sentido a *CryptoRave* é mais um esforço coletivo do que "um coletivo".

P: Como vocês se conheceram?

R: Algumas pessoas já se conheciam dos eventos de software livre. Outras nós conhecemos a partir da primeira *CryptoParty* e algumas outras a partir da própria *CryptoRave*.

P: Como o coletivo se define? Uma descrição

R: A *CryptoRave* é um evento hacker de 24 horas de privacidade, segurança e liberdade na rede.

P: O coletivo trabalha com outros projetos além da *CryptoRave*?

R: Não. A organização trabalha apenas para realizar a *CryptoRave*. No dia a dia cada organização tem sua agenda de atividades. Em algumas os temas do evento convergem com o trabalho delas.

P: Desde quando o coletivo existe?

R: A *CryptoRave* existe desde 2014.

P: O coletivo tem relação com movimentos sociais? Se sim, quais e como?

R: Em algum em particular, não. A *CryptoRave* é aberta a participação de todas/os.

P: O coletivo é aberto para receber mais membros? Se sim, como funciona a seleção?

R: Não. A entrada para a organização da *CryptoRave* é feita por convite pelos coletivos. Se todos os organizadores considerarem que sim, então uma pessoa ou coletivo é convidado.

### **3. Organização da *CryptoRave* de 2016**

P: O que mudou da primeira *CryptoRave* para a terceira edição?

R: A programação foi se aperfeiçoando ao longo do tempo e estabelecemos um Chamado para Atividades para organizar parte da programação. Isso envolve escolher palestras, falar com o palestrante e organizar sua logística. É um trabalho penoso que ajuda a estruturar a comunidade. Assim como a infraestrutura do próprio evento. Também conseguimos entender melhor a nossa própria dinâmica interna: o que cada um fica responsável em fazer. Além disso, na primeira edição não imaginávamos quantas pessoas teríamos organizando. Já nessa última edição tivemos um grande número de voluntários, o que ajudou muito.

P: Como foi realizada a organização da *CryptoRave* 2016?

R: Nós fizemos um Chamado para Atividades no final do ano passado. Ao longo do primeiro semestre nós fizemos encontros presenciais para definir local, infraestrutura necessária, *Keynotes*, voluntariado, entre outras coisas. Fechamos a nossa campanha financeira após dois meses, o que foi bastante longo e desgastante.

P: Quais as dificuldades e os desafios enfrentados?

R: Organizar um evento com financiamento coletivo tem diversos desafios. Primeiro é ofertar uma programação em si que seja interessante. Depois temos que organizar e encaixar as diversas atividades e propostas que aparecem.

P: Quanto tempo o coletivo teve que dedicar à organização do evento deste ano?

R: Além das reuniões semanais, muitos tiveram que perder trabalho ou faculdade para conseguirem fazer todas as tarefas do evento. Assim é difícil estimar a quantidade de horas que cada um dedicou.

P: Como foi feita a publicidade do evento?

R: Além das mídias sociais, nós fomos entrevistados por revistas, jornais e sites. Também divulgamos a partir do nosso mailing list e de organizações parceiras.

P: Qual foi público-alvo do evento?

R: Não trabalhamos exatamente com esse conceito. Fazemos um evento hacker aberto e inclusivo. Há atividades para quem está chegando e para pessoas mais velhas. Também procuramos não dialogar só com uma faixa etária (jovens) e procuramos fazer atividades diversas. Esse ano tentamos fazer o espaço para crianças, mas poucos pais e mães foram ao evento. O que identifica todas essas pessoas com o evento é o interesse pela cultura hacker, pela privacidade e pela segurança.

P: Qual foi o público presente?

R: Muitas caras novas. De todos os outros eventos técnicos no Brasil, o que realmente chama a atenção é como a *CryptoRave* atrai pessoas novas.

P: Qual a avaliação do coletivo sobre a *CryptoRave* de 2016?

R: Houve alguns problemas de infraestrutura, principalmente referente as obras no Centro Cultural São Paulo. Isso impactou negativamente no som das palestras. Mas estivemos muito mais organizados esse ano e com muitos mais braços. Pelo menos dessa vez todos os palestrantes saíram com uma camiseta do evento.

#### **4. Palestrantes e Palestras**

P: Como os temas abordados no evento são escolhidos?

R: Os temas das *Keynotes* são decididos em reunião pela organização tendo sempre em vista os assuntos de privacidade e segurança.

P: Como os palestrantes da *CryptoRave* são escolhidos?

R: Após pensar nos temas das *Keynotes*, nós fazemos uma seleção de possíveis convidados e verificamos a disponibilidade deles.

P: O que faz uma palestra ser aprovada?

R: Talvez seja mais fácil ver o contrário. O que faria uma atividade ser rejeitada. Do nosso Call for Activities:

•As atividades de palestras que forem merchandising de produtos serão automaticamente desclassificadas (<https://CryptoRave.org/cfa.html>). Além disso nós rejeitamos atividades que sejam a divulgação de software proprietário. Assim evitamos vendedores.

P: Existe uma preferência do coletivo para com palestrantes de determinadas universidades?

R: Não. Inclusive no chamado para atividades a graduação acadêmica não é exigida.

P: Nota-se uma presença de maior público masculino (67,6%) nas palestras, qual a opinião do coletivo sobre isso?

R: Embora isso seja algo recorrente nos eventos de tecnologia, a *CryptoRave* tem uma trilha organizada por mulheres. Talvez uma medida melhor seja ver o público geral do evento e não só nas palestras. Além disso, nós buscamos compor as *Keynotes* de forma paritária.

P: O nível de escolaridade entra em questão na hora da escolha do palestrante?

R: Não.

P: Há palestrantes com diferentes trajetórias profissionais (professores, ativistas, técnicos de TI): por que a organização *CryptoRave* busca essa diversidade?

R: Para atrair visões diferentes sobre segurança e privacidade, por acreditar que o problema da vigilância é político, técnico e jurídico. Se advogados acham que vão enterrar a vigilância em massa com um projeto de lei, nós precisamos lembrar o que é o grampo no Brasil ou o que são os programas vigilância da NSA. Se ativistas acreditam que basta protestar contra esses programas e denunciar as violações às autoridades competentes, então precisamos mostrar o quão vivo



estão esses programas mesmo após Edward Snowden. O problema da vigilância é multifacetado e precisamos enfrentar com o poder da diversidade.

## 5. Proposta

P: Qual a finalidade da *CryptoRave*, na opinião do coletivo?

R: Ser um evento de segurança e privacidade.

P: Qual a importância da *CryptoRave* para o Brasil, na opinião do coletivo?

R: A *CryptoRave* é o único evento hacker gratuito no Brasil aonde qualquer um pode participar das atividades. Mesmo em outros países, os maiores eventos têm ingresso que, no geral, não são baratos. Temos nossos limites de infraestrutura, mas ainda assim conseguimos oferecer um espaço e encontro para a comunidade hacker.

P: O que o evento oferece ao seu público?

R: Debates, palestras, oficinas e contato com temas que dificilmente se encontrará em outros eventos e, principalmente, de graça.

## 6. Discussões

P: Quais discussões no âmbito da anti-vigilância e da criptografia a *CryptoRave* traz ao Brasil?

R: Realizamos palestras sobre novas cifras criptográficas com os maiores especialistas da área no país e também tivemos atividades explicando como as curvas elípticas funcionam.

P: Quais discussões no âmbito dos movimentos sociais o evento traz ao Brasil?

R: Na primeira *CryptoRave* o Cypherpunk Jeremie Zimmermann falou sobre o futuro distópico das tecnologias que estão na ponta dos nossos dedos. Em 2015 o Peter Sunde, ex-fundador do Pirate Bay falou sobre a luta contra o direito autoral. Em 2015, trouxemos um jornalista do Netzpoliitk que vazou documentos sigilosos do governo alemão. Em 2016, falamos como as lei anti-terroristas atingiram jornalistas, ativistas e administradores de sistemas.

## 7. Aprendizado

P: Quais Workshops e palestras vocês consideram os mais importantes?

R: Temos dado bastante ênfase nas oficinas básicas de criptografia. Em todas as edições nós repetimos: OTR, GPG, Tor.

## 8. Financiamento

P: Por que o Catarse foi a plataforma escolhida para o financiamento coletivo e como o mesmo funciona?

R: É uma plataforma de campanhas onde pode se doar anonimamente ou não, ele tem taxas bancarias e de funcionamento mais por ser bem conhecido costuma trazer facilidades para divulgação.

## **9. Realizadores**

P: Qual a relação de vocês com outros coletivos?

R: Contamos com o apoio de empresas e organizações sociais. Às vezes só na ajuda financeira e em outras com o empréstimo de equipamentos. Essa é uma política de vizinhança que temos tentado manter.

P: Qual a relação de vocês com a Actantes? Escola de Ativismo? Interozes? A Saravá?

R: Todos os coletivos realizam a *CryptoRave* e outras atividades, eventualmente, juntos.

## **10. Apoiadores**

P: Quais são os apoiadores mais importantes para a *CryptoRave*?

R: Todas as pessoas que apoiam, tanto na campanha como de voluntários no dia são importantes para que o evento ocorra.

P: O que os apoiadores fizeram para o evento?

R: O suporte para que ele possa acontecer, nesse caso vemos inclusive a organização enquanto apoiador.

## **11. Impacto**

P: Qual a avaliação do coletivo sobre os efeitos da *CryptoRave*?

R: Achamos que ela é muito importante para ampliar o debate sobre o direito da privacidade e o uso das tecnologias no Brasil. Assim também como compartilhar as experiências dos movimentos mundiais com a nossa realidade. E provar que é possível através de uma organização autônoma e coletiva tocar um evento desse porte.

P: O evento tem atingido as finalidades às quais se propõe?

R: Imaginamos que sim.

P: O coletivo identifica efeitos não planejados do evento?

R: Como nunca criamos uma agenda específica tudo que se desenvolveu do evento para nós é importante e interessante, assim, não conseguimos pensar em algo não planejado exatamente.