

Universidade Federal de Juiz de Fora
Pós-Graduação em Ciências Sociais
Mestrado em Ciências Sociais

Ana Carolina Estorani Polessa da Silva

SOCIETAS ANONYMOUS
A Construção Política e Social do Hacker

Juiz de Fora
2016

Ana Carolina Estorani Polessa da Silva

SOCIETAS ANONYMOUS
A Construção Política e Social do Hacker

Dissertação apresentada ao Programa de Pós Graduação em Ciências Sociais, área de concentração: Cultura, Democracia e Instituições, da Universidade Federal de Juiz de Fora, como requisito parcial para obtenção do grau de Mestre.

Orientador: Prof. Dr. Rubem Barboza Filho

Juiz de Fora

2016

Ana Carolina Estorani Polessa da Silva

SOCIETAS ANONYMOUS

A Construção Política e Social do Hacker

Dissertação apresentada ao Programa de PósGraduação em Ciências Sociais, área de concentração: : Cultura, Democracia e Instituições, da Universidade Federal de Juiz de Fora, como requisito parcial para obtenção do grau de Mestre.

Aprovada em

BANCA EXAMINADORA

Professor Doutor Rubem Barboza Filho (Orientador)

Universidade Federal de Juiz de Fora

Professor Doutor Antonio Claudio Engelke Menezes Teixeira

Universidade do Estado do Rio de Janeiro

Professor Doutor Paulo Roberto Figueira Leal

Universidade Federal de Juiz de Fora

Aos meus pais, minha irmã, familiares mais próximos e meus amigos que nunca me deixaram desistir.

AGRADECIMENTOS

Agradeço a todos que contribuíram direta ou indiretamente em todas as fases para o desenvolvimento deste trabalho.

Aos meus familiares mais queridos, que não posso deixar de citar:

Aos meus pais, e seu apoio e amor incondicional, que nunca mediram esforços para que eu sempre seguisse em frente. Para minha irmã Marina, que mesmo sendo mais nova, sempre esteve ao meu lado me dando coragem para nunca desistir.

A minha tia Maria, que apesar de tudo, sempre esteve disponível para ajudar no que pode.

Para minha avó, que nos deixou antes que ela pudesse ver o resultado de todos meus esforços.

Aos colegas e amigos que conheci durante o mestrado, em especial para Nathália, Paula Emília, Paula Boarin e Vanessa que tanto me ensinaram e me apoiaram, tornando as preocupações acadêmicas e pessoais bem mais leves.

A amigos que não importa a distância, sempre estiveram tão perto como: Nayara e Welington, Erika, Alessandra e Carolina Macedo, demonstrando que amizades verdadeiras o tempo não apaga.

E aos amigos que sempre entenderam minhas ausências em função do trabalho em si ou de algum prazo... e que tornam cada (re)encontro sempre tão alegre, demonstrando que a amizade está nas coisas mais simples: Aninha, Anderson, Barbara Mendonça, Barbara Rezende, Daniel, Nicole, Thaís, Thiago, Maiara, Rafael e Virginia.

Aos professores do departamento, em especial ao meu orientador Rubinho, que sempre acreditou em mim e neste trabalho.

Não poderia deixar de agradecer aos professores Antonio Claudio Engelke e Paulo Roberto Figueira Leal, pela disposição em participar da banca e as observações feitas durante a defesa que tanto contribuíram para este trabalho.

Por fim, para todos os Hackers e Anonymous que me ajudaram para o desenvolvimento desta pesquisa, que me ensinaram na prática o valor e a importância do conhecimento livre e de compartilhar novos saberes.

RESUMO

Este trabalho apresenta a construção, as influências políticas e sociais sofridas pela Cultura Hacker em suas duas principais raízes (divididas em dois capítulos): por meio da exploração de linhas telefônicas desde 1878 até sua evolução para o phreaking por volta da década de 1960. Posteriormente, o *phreaking* foi absorvido por movimentos de contracultura nos Estados Unidos, se tornando uma forma de protesto contra a guerra do Vietnã a partir da década de 1970, período ao qual a prática foi popularizada gerando grandes prejuízos a empresas de telefonia, se tornando assim, um problema social. A segunda raiz da Cultura Hacker está relacionada ao surgimento dos primeiros computadores por volta do final da Guerra Mundial, inicialmente restrita ao meio acadêmico e ao setor militar, com forte influência da Guerra Fria e do chamado mito pós-nuclear, até começar a emergir para a população em geral na metade da década de 1970, em função do início das vendas dos computadores pessoais, que fez com que o phreaking e o hacking de computador convergissem durante este período. Buscando apresentar uma perspectiva diferenciada, pesquisamos os desafios para a construção da Cultura hacker no Brasil, colocando o país dentro de um contexto que se desenvolvia em diversos países do mundo no final da década de 1980. Com o desenvolvimento da rede mundial de computadores no início da década de 1990, o número de usuários da internet passou a crescer de maneira vertiginosa e entre 1994 e 1996, surge o hacktivismo - ativismo feito por hackers - que buscavam garantir o anonimato e a liberdade de expressão e do próprio ciberespaço. Na terceira parte do trabalho, analisamos a forma ao qual o Anonymous ampliou os limites do hacktivismo, apresentando quais são os principais motivos que desencadeiam suas ações, baseando suas atividades na ideia de Cidade por Projetos idealizada por Luc Boltanski e Eve Chiapello.

Palavras chave: Hacker , Hacktivismo, Anonimato, Cidade por Projetos

ABSTRACT

This work presents the construction, the political and social influences underwent by the Hacker Culture in its two main branches (divided in two chapters): through the exploration of telephone lines since 1878 until its evolution to phreaking around the decade of 1960.

Afterwards, the *Phreaking* was absorbed by counter-cultural movements in the United States, becoming a protest tool against the Vietnam War after 1970, period on which this practice rose on popularity, causing a great loss to phone companies, becoming, thus, a social problem. The second branch of the Hacker Culture is related to the development of the first computers by the end of the First World War, initially restricted to scientific and military organizations with great influence of the Cold War and the so-called “post-nuclear myth”, until it starts to spread out to the rest of the population during the second half of 1970, due to the sales of personal computers, which made such practices like Phreaking and Hacking to converge during this period. In order to present a differentiated approach, we researched the challenges related to the construction of the Hacker Culture in Brazil, introducing the country in a context that developed itself in many other countries in the end of 1980. With the growth of the World Wide Web in the beginning of the 1990, the number of internet users started to skyrocket and, between 1994 and 1996, comes up the hacker-activism – that was an activism made by hackers in order to ensure anonymity and the their own freedom of expression, along with the freedom of the cyberspace. In the third part of the work, we analyze how the group *Anonymous* expanded the limits of this “hacktivism”, showing what the reasons that initiated its actions are, basing its activities on the idea of the “Projective City”, designed by Luc Boltanski and Eve Chiapello.

Key-Words: Hacker, Hacktivism, Anonymous, Projective City

SUMÁRIO

1	INTRODUÇÃO	10
2	PROTOHACKERS E PHREAKING	13
2.1	Proto-hackers	13
2.2	Hackers de telefone e o desenvolvimento das Blue-boxes	16
2.3	Phreakers (1970)	21
2.3.1	<i>Popularização das Blue-Boxes</i>	22
2.3.2	<i>Phreaking como forma de protesto. Hackers Underground</i>	26
2.4	Conclusões	31
3	HACKERS DE COMPUTADOR	33
3.1	Modelo aberto como estratégia da Guerra Fria	33
3.1.1	<i>O mito pós-nuclear</i>	35
3.2	Simbiose entre homens e máquinas	37
3.3	Relação do hacker com a informática	41
3.4	“Eles são uma legião”: os hackers de hardware	45
3.5	O hacker brasileiro da década de 1980	52
3.5.1	<i>Desafios para inserir a cena hacker no Brasil</i>	53
3.5.2	<i>Cyberpunk como indivíduo no Brasil</i>	57
3.6	Conclusões	65
4	HACKTIVISMO	67
4.1	A Lógica do ciberespaço	67
4.2	O surgimento do hacktivismo	71
4.3	Anonymous	76
4.3.1	<i>Dos BBS ao 4Chan</i>	76
4.3.2	<i>Dando forma ao personagem</i>	80
4.3.3	<i>Pool’s closed. The Internet Hate Machine</i>	83
4.3.4	<i>Chanology</i>	84
4.3.5	<i>O Homem e seu passado: Por que a máscara de Guy Fawkes?</i>	90
4.3.6	<i>Critérios utilizados para seleção das amostras</i>	98
4.3.7	<i>Desencadeando operações</i>	103
4.4	Conceito de cidades de Luc Boltanski	107
4.4.1	<i>Escolha da operação</i>	111
4.4.2	<i>Análise da #OpDarkNet</i>	112
4.5	Considerações finais	108
5	REFERÊNCIAS	122
	ANEXOS	133

"Temos que reconhecer que cada ferramenta poderosa pode ser usada para o bem ou para o mal (...) apoie um planeta justo e correto, mas lembre-se: não é papel da tecnologia fazer as regras ou aplicá-las. Não podemos culpar a tecnologia quando cometemos erros" (Sir. Tim Berners-Lee)

1 INTRODUÇÃO

A partir da década de 1980, as discussões acadêmicas voltadas para o tema da “Cultura Hacker” começaram a ser aprofundadas em diversas áreas de conhecimento. Parte deste interesse ocorreu em função tanto de um processo de integração¹ de hackers e computadores, que passaram a estar mais presentes na vida cotidiana da sociedade, quanto da transformação do *hacking* em um problema.

Segundo Himanem (2001, p.7), “os hackers não são celebridades da TV cujo os nomes são amplamente reconhecidos, mas todos já ouviram falar de suas façanhas, que constituem grande parte da base tecnológica da sociedade”.

Quando nos referimos à “Cultura Hacker”, nos referimos também a “subculturas de um universo hacker muito mais vasto” (CASTELLS;2003), que engloba diversas culturas hackers relacionadas a tradições geográficas e históricas muito próprias, com perspectivas, construções e trajetórias específicas a cada uma destas comunidades.

Um dos grandes desafios de um trabalho sociológico que busca analisar o *hacker* e, mais adiante, os *hacktivistas* do Anonymous é trabalhar com uma temática que possui grande envolvimento do senso comum, em construções estereotipadas criadas pelos próprios pesquisadores, pela mídia, pelo cinema, pelo governo e, por fim, por “mitos” criados pelos próprios *hackers*.

Castells (2003) faz um breve debate em relação a estes mitos, buscando inicialmente dissipar o mito da marginalidade dos hackers, expondo o fato de que, apesar de possuírem um domínio tecnológico superior à média da população, a maioria vive suas vidas “normalmente”, muitas vezes em conformidade à ideologia dominante da sociedade.

Um segundo mito apresentado por Castells (2003) é em relação à ideia de cooperação, liberdade e a cultura do dom, que se desenvolveriam quando possuem suas necessidades básicas atendidas, permitindo que estes indivíduos possam dedicar suas vidas para a criatividade intelectual, uma contradição para hackers que vivem em países mais pobres, aos quais as adversidades os levam a procurar alternativas para a prática de seu *hacking*.

Pesquisadores europeus como Alberts e Oldenziel (2014) criticam o fato da “cultura hacker ser lida como uma história americana, que por extensão clama por universalidade”,

¹ Para que ocorra um processo de integração na sociedade é necessário que o objeto/ tema faça sentido na vida cotidiana das pessoas (STREETER;2011)

reforçando a necessidade de se compreender o *hacking* a partir da motivação dos próprios indivíduos.

Procuramos identificar a luz das ciências sociais, a maneira com a qual o hacker se tornou um problema social, com base na posição que tais atores ocupam ou passaram a ocupar dentro da própria sociedade.

Esta dissertação é dividida em três partes: A primeira, analisando como a prática do *hacking* esteve originalmente ligada à área de engenharia, principalmente a elétrica, com foco na exploração de linhas telefônicas desde 1878. Porém, foi apenas por volta de 1950 que as pesquisas no setor de telefonia foram intensificadas, buscando atender uma maior demanda de usuários que realizavam ligações à distância. (MADDOX,1976; STERLING,1994)

Segundo pesquisadores, um dos grandes erros das empresas de telefonia entre 1950-1960 foi implantar o sistema mais barato dentre os três possíveis (FLORY, 1990), permitindo a produção de meios para realizar ligações gratuitas. Teria sido esta a base para o surgimento dos *hackers* de telefonia, que posteriormente originaram a comunidade dos *phreakers* ao redor do mundo, uma das principais raízes do *hacker* de computador.

O *phreaking* foi absorvido por movimentos de contestação das décadas de 1960 e 1970, que tornaram a prática uma forma de protestar contra a Guerra do Vietnã (1955-1975). E durante a década de 70 o *hacking* de computador e o de telefone começaram a se convergir.

A segunda parte do trabalho se dedica a analisar a construção da cultura hacker pelos computadores, sua raiz mais conhecida. Debatendo a construção da própria cultura da Internet, que segundo Samuel (2004, p.40) existia de forma difusa em múltiplas culturas: a dos cientistas da computação, a dos amadores e a dos assistentes de pesquisa - agrupados em torno de tudo que os *mainframes*² fossem capazes de acessar.

Logo no início, torna-se claro que certas definições (em relação a termos e posturas) poderiam ser extremamente variadas entre seus membros, variando de acordo com a área e até mesmo das intenções do indivíduo ou grupo de indivíduos nela envolvida.

Para Castells (2003 p.34):

A cultura da Internet é a cultura dos criadores da Internet. Por cultura entendo um conjunto de valores e crenças que formam o comportamento; padrões representativos de comportamento geram costumes que são repetidos por instituições, bem como organizações sociais informais. Cultura é diferente de ideologia, psicologia ou representações individuais. Embora explícita, a cultura é uma construção coletiva que transcende preferências individuais, ao mesmo tempo em que influencia as práticas das pessoas no seu âmbito, neste caso os produtores/usuários da Internet.

² Também chamados de supercomputadores ou computadores de grande porte. São equipamentos capazes de realizar processamento de dados complexos.

Buscando uma perspectiva diferenciada, pesquisamos os desafios para construção da cultura hacker no Brasil, colocando o país dentro de um contexto que se desenvolvia em diversos países no mundo.

Iniciamos o capítulo 03 apresentando o desenvolvimento da rede mundial de computadores (a *World Wide Web*), que possibilitou um maior acesso de usuários à rede e às principais características da comunidade que se desenvolveram no ciberespaço, momento no qual as teorias de rede voltaram a ser aprofundadas nas Ciências Sociais. Na parte inicial deste capítulo, também apresentamos o surgimento do hacktivismo entre 1994 e 1996 e seus principais desdobramentos.

Posteriormente, analisamos a origem do Anonymous nos chans a partir de 2003, buscando compreender a forma com a qual eles teriam ampliado os limites do hacktivismo, utilizando a ideia de cidade idealizada por Luc Boltanski e Eve Chiapello (2009) para explicar as variadas ações nas quais o Anonymous está inserido, seguido das conclusões deste trabalho.

2 PROTOHACKERS E PHREAKING

O período entre 1875-1910 é descrito por Chapuis e Joel (2003) como o da infância do telefone, ao qual boa parte dos componentes essenciais da vida moderna foram introduzidos. As empresas que produziam equipamentos eletrônicos eram as mesmas que produziam cabos para firmas de energia elétrica e companhias telefônicas.

Em um período entre duas guerras mundiais, o telefone se popularizava ao redor do mundo tal como o interesse, o estudo e a exploração de linhas telefônicas, que formaram uma das mais antigas e consistentes raízes da Cultura Hacker. Boa parte de seu desenvolvimento técnico, teórico e histórico que se sucederam, eventualmente, serviriam de base para o surgimento de uma verdadeira comunidade: os *phreakers*.

Segundo Mungo (1993, p.9) antes do objetivo do *phreaking* (principalmente a partir da década de 1970) ser o de “libertar a tecnologia do controle do Estado e da Indústria”, a prática começara como um passatempo, com indivíduos com um grande talento na área de eletrônica formando uma comunidade *underground* bem antes de se ouvir falar deles.

2.1 Proto-hackers

Uma das bases que construiu a complexa Cultura Hacker, certamente, pode ser associada à relação destes indivíduos com a tecnologia e a própria engenharia elétrica, em especial com os sistemas de telefonia, com raízes mais antigas do que eventualmente se descreve.

Sterling (1994) aponta que parte desta construção remete ao ano de 1878, cerca de dois anos após Alexander Graham Bell inventar o telefone. O chefe do sistema de telégrafo de *Western Union* não via o telefone como um “negócio sério” e já havia recusado os protótipos apresentados por Bell. Entre os argumentos, afirmava que ao contrário do telefonema, os destinatários poderiam responder os telegramas quando tivessem tempo e quando lhes fosse conveniente. O telégrafo elétrico foi criado em 1830 e em 1876 tinha mais de 214,000 milhas de fios e 8.500 escritórios (STERLING,1994).

O telefone, antes visto como uma tecnologia íntima (voltada a esfera privada), passou a ser visto de outra forma, a partir de janeiro de 1878, quando houve um grande desastre de trem em Tarriffville (Connecticut) e o telefone se mostrou essencial para contatar médicos na região, para ajudar no resgate das vítimas, mostrando sua potencialidade para o mundo real. Tal fato,

fez aumentar a demanda e a necessidade de contratar um maior número de operadores de telefone.



Ilustração 01: The great Tariffville Train Wreck, January 14, 1878

Fonte: Thomas J. Dodd Research Center, University of Connecticut Libraries

Ainda segundo Sterling (1994), inicialmente, empresas de telefonia, como a “*Bell Telephone Company*”, evitavam contratar mulheres como operadoras, temendo a liberação feminina³ e optaram contratar (garotos) adolescentes, por aceitarem salários mais baixos e por terem experiência com o telégrafo. Eles teriam sido uma espécie de “*proto-hackers*”, mesmo que não houvesse tal definição nesta época.

Em menos de um ano, as empresas, tanto nos Estados Unidos quanto na Inglaterra, aprenderam a “lição que combinar adolescentes e linhas telefônicas os colocando no comando do sistema era um desastre rápido e consistente” e o engenheiro chefe os descrevia como “índios selvagens” (STERLING, 1994, p.13).

³ No ano de 1878, ocorreu em Paris o primeiro congresso internacional de direitos das mulheres

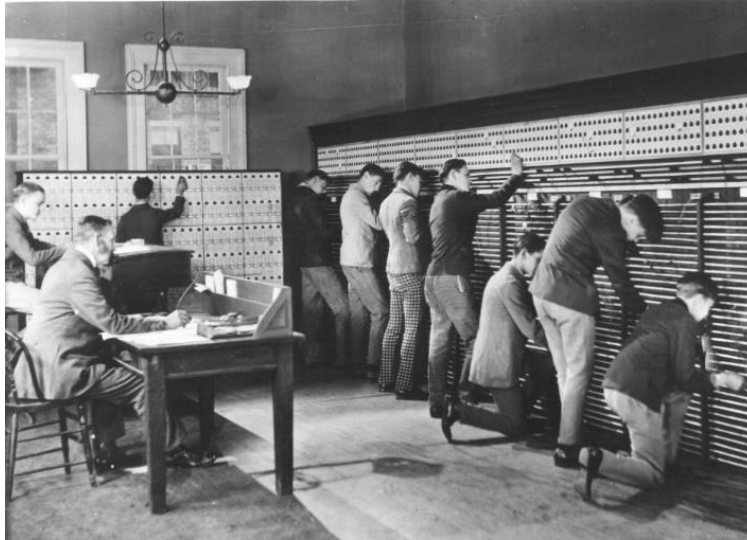


Ilustração 02 : Primeiros Operadores de Telefone
 Fonte: *The Telecommunications History Group* (1877~78)

Além de serem grosseiros no atendimento ao público, faziam brincadeiras, desligavam ligações, cruzavam as linhas dos clientes e conversavam com estranhos (STERLING;1994, MADDOX;1978). Para Sterling (1994, p.13) “Esta combinação de poder, domínio técnico e anonimato pareciam agir como erva de gato⁴ em adolescentes”.

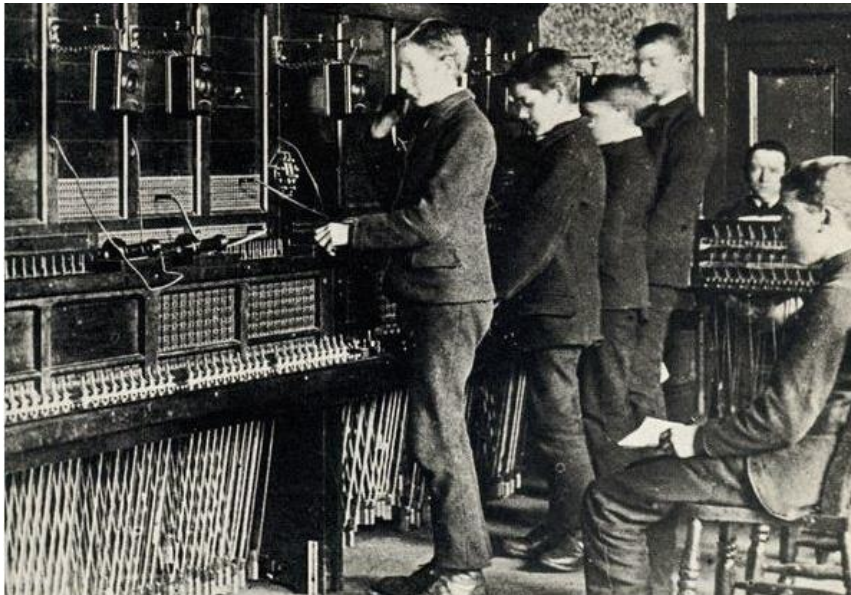


Ilustração 03 : Primeiros Operadores de Telefone (Inglaterra)
 Fonte: *Boy Operators on Sunderland Exchange* 1883

⁴ *Nepeta Cataria, catnip* ou “erva de gato” faz parte da família das hortelãs, conhecidas por atrair a atenção de gatos domésticos pelo odor.

Posteriormente em 1881, as empresas passaram a dar preferência a contratação de mulheres como operadoras de telefone⁵, por considerá-las mais calmas, pacientes e educadas para o serviço, o que para Brenda Maddox (1978) era uma vantagem: os empregos oferecidos para as mulheres nas companhias de telefone foram uma nova oportunidade para que elas pudessem trabalhar em outras áreas, além de fábricas e fora do serviço doméstico.

2.2 Hackers de telefone e o desenvolvimento das *Blue-boxes*

Como visto, inicialmente havia uma necessidade de operadores que completassem manualmente as ligações telefônicas. Enquanto ocorria um aumento das ligações à distância e da própria demanda de usuários, se tornou vital que as empresas investissem em um novo tipo de sistema, uma vez que manter os operadores gerariam um custo ainda maior para as companhias.

Segundo David Flory (1990), as melhorias tecnológicas das redes de telefonia que se sucederam (entre as décadas de 1950-1960) possibilitaram as fraudes no próprio sistema por dois motivos, sendo o primeiro pela escolha das empresas que optaram em implantar um sistema mais barato.

Na época, havia possibilidade da implantação de 3 tipos de sistemas: *out-of-band*, que precisava de equipamentos mais sofisticados para lidar com a largura da banda (que significa a capacidade de transmissão que determina a velocidade que os dados passam pela rede); *External Channel Routine*, que também exigia equipamentos mais caros e ainda precisavam de investimentos para solucionar os problemas para coordenar o sinal e a voz durante as ligações; e, por último, o *in-band*, que foi a opção escolhida em função de seu baixo custo de implementação e pela facilidade para realizar uma ligação. (FLORY;1990)

O segundo motivo, foi um erro da própria empresa de Graham Bell, a *American Telephone and Telegraph Company* (atualmente conhecida como AT&T). Entre as décadas de 1950 e 1960, artigos como “*Single-Frequency Signaling System for Supervision and Dialing over Long-Distance Telephone Trunks*” de Weaver e Newell (1951) começaram a ser publicados (LAPSLEY,2013)

⁵ Emma Mutt foi a primeira operadora contratada em 1881, pela *Telephone Despatch Company*, em Boston, Massachusetts.

Em 1954, o periódico *Bell System Technical Journal*⁶ publicou o artigo “*In-band single Frequency Signaling*”⁷, que explicava detalhadamente o método de instalação e como funcionava o sistema de telefonia, “com clareza, plenitude e detalhes” (LAPSLEY,2013) oferecendo detalhes técnicos e apontando as possíveis falhas do sistema.

Flory (1990) explica que do momento que uma pessoa fazia uma discagem internacional, o sistema da empresa identificava a melhor forma de fornecer o acesso, verificando a disponibilidade de uma linha, por meio da emissão de uma frequência de 2600Hz⁸, que mostrava que uma linha estava inativa, no caso livre para realizar a ligação.

Segundo Lapsley (2013, p.32) o artigo ainda explicava como as chamadas no exterior eram possíveis e “incluía diagramas esquemáticos simplificados e os circuitos elétricos necessários para gerar os tons utilizados para controlar a rede”. E as maiores universidades de engenharia eram assinantes desta publicação.

O quebra-cabeças do trabalho de Weaver e Newell foi completado em 1960, quando Breen e Dahhbom publicaram “*Signaling Systems for Control of Telephone Switching*” no mesmo periódico, explicando detalhadamente as frequências que eram usadas para cada dígito. (ROSENBAUM,1973; LAPSLEY,2013; FLORY,1990)

Em 1961, o setor de segurança da *Bell* encontrou a primeira *Blue-Box* no *Washington State College* em Pullman, em um suposto estúdio de fotografia e descreveram como “um estranho dispositivo com chassis de metal azul, conectado a linha de telefone do estúdio com o nome *Blue -Box*” (FLORY,1990, p.118).

O equipamento recebeu esse nome, pelo simples fato de ser dessa cor, sendo capaz de atingir a frequência de 2600Hz e realizar ligações nacionais e internacionais de maneira gratuita, antes mesmo dos usuários de telefone comuns, que só conseguiram fazer este tipo ligação a partir da década de 1970. (FLORY,1990, LAPSLEY;2013, COE,1995; STERLING,1994)

⁶ Fundado em 1922

⁷ Também de Weaver e Newell

⁸ Frequência disponível em países como Canadá e Estados Unidos. Em países como o Brasil e a Argentina a frequência necessária era de 3825Hz.

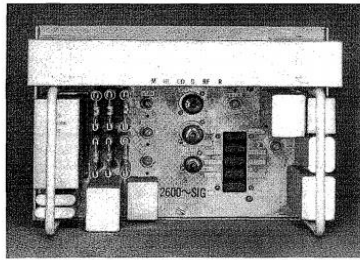


Fig. 10 — Front view of the 2,600-cycle signaling panel.

The *n* delay, because of guard action and the fact that its secondary winding is closed through a varistor and resistance, is relatively slow to operate and fast to release. For this reason some form of pulse correction is necessary to get good dial operation. This is obtained with the *nc* (regenerate) relay and its associated *cr* timing network, and there results an output pulse within the needed limits, even though the signal on the *n* relay is shortened considerably.

DESCRIPTION OF 2,600-CYCLE DESIGN

The 2,600-cycle unit, shown in Fig. 10, is just half the size of the 1,600-cycle unit, costs less than half as much, and is of the "plug in" type so it can be readily replaced for maintenance action.

A simplified diagram of the new signaling circuit is shown in Fig. 11, with the transmitting portion in the upper part of the figure and the receiver in the lower part. The transmitting portion employs three relays designated *m*, *hl*, and *co* which are interconnected to perform the following functions: relay *m* is used to key the signaling tone; relay *hl* (high level) adds 12 decibels to the tone power at the beginning of each signal tone application to improve signal reliability in the presence of line noise and variations in attenuation; and relay *co* (cut off) cuts the line momentarily to prevent noises originating in the switching equipment from interfering with signaling.

The operation of the receiver will be explained by describing its action (except for pulsing which will be described later) when signal frequency is received. This ac tone is amplified (or limited if it is too large) and then passed on to the signal and guard networks where a relatively high voltage results in the signaling channel and a lower voltage in the

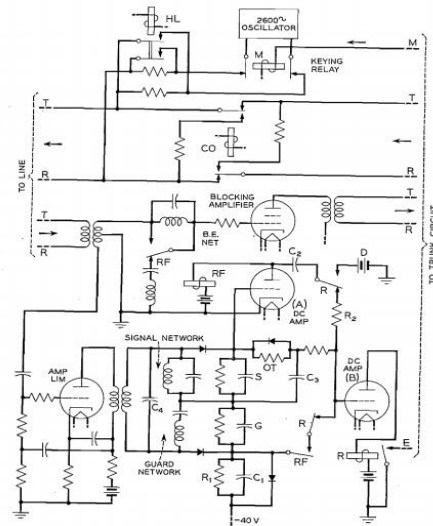


Fig. 11 — Simplified diagram of 2,600-cycle signaling circuit.

Ilustração 04: Fragmento do artigo *In-Band Single-Frequency Signaling*

Fonte: *In-Band Single-Frequency Signaling* By A. WEAVER and N. A. NEWELL (1954)

Explicando de uma forma mais simples: atingindo a frequência de 2600Hz, o usuário realizava uma “rediscagem” e se tornava o operador da ligação, conseguindo fazer ligações nacionais e internacionais gratuitamente.

Os primeiros modelos de *blue-boxes* eram relativamente grandes e pesados, construídos com tubos a vácuo. Posteriormente, foi utilizado um transistor⁹ para fazer versões menores do equipamento¹⁰, podendo ser usadas até em telefones públicos. (COE;1995).

No meio acadêmico, as primeiras informações do hackeamento de linhas telefônicas vieram do MIT (*Massachusetts Institute of Technology*), mais relacionadas a um grupo fundado entre 1946-1947 chamado *Tech Model Railroad Club*¹¹ (TMRC), que envolvia estudantes e projetistas que partilhavam o interesse comum de reconstruir réplicas de determinados modelos de trens, por diversão, por valores históricos ou sentimentais (LEVY;2012).

Tal grupo seria a principal referência, apontada por diversos pesquisadores, como sendo uma das origens da Cultura *Hacker*, compreendida como um elemento que compõe a Cultura a Internet (CASTELLS;2003).

⁹ Peça responsável pela amplificação do sinal, que também funciona como um controlador que libera ou interrompe uma corrente elétrica. Foi desenvolvido em 1947 pelo próprio laboratório da *Bell Telephone*. (HAUTSCH,2010)

¹⁰ Existem várias versões, com sistemas diferentes, mas com objetivos semelhantes. Como as *silver-boxes*, *red-boxes*, *yellow-boxes*, *black-boxes*, *Beige-box*, etc.

¹¹ Clube de Ferreomodelismo

O TMRC é uma das principais fontes para o início da prática do hacking do telefone, em tentativas e testes de controlar trens por meio de linhas de telefonia. É o que Lapsley (2013, p.17) destaca:

(...) As empresas de telefonia doaram equipamentos para o clube apenas para este fim, e o orientador do clube estava no comando do sistema de telefonia do MIT, por isso não foi surpreendente que os operadores dos modelos de trens do TMRC, utilizassem um mostrador de telefone para selecionar o trem que queriam controlar. Era um terreno verdadeiramente fértil para os entusiastas de telefone.

Um dos registros mais antigos encontrados da utilização do termo *hacker* que encontramos, e mais próximo do sentido que conhecemos atualmente, é de uma publicação datada de 20 de novembro de 1963 na revista “*The Tech*”, do próprio MIT, e é relacionada aos *hackers* de telefonia.

No artigo “*Telephone Hackers Active*”, de Henry Lichstels, é descrito que os telefones do MIT teriam sido cortados em função das atividades “dos chamados *hackers*”. Relata-se que havia uma média de 2-3 expulsões anuais pela prática.

Os estudantes teriam descoberto as chamadas “*tic-lines*”¹²(linhas internas) e, segundo o professor Carlton Tucker, chefe do departamento de telefonia do MIT, estes alunos “utilizavam de métodos ‘exotéricos’ e descobriram as linhas ‘à força’ ” (LICHSTELS;1963), possibilitando a realização de telefonemas (inclusive internacionais), que aumentavam consideravelmente o gasto do Instituto com ligações telefônicas.

No artigo, o professor Tucker afirma que admirava a curiosidade dos estudantes, ressaltando inclusive a fala de um desses *hackers* de que “este é um campo aberto para experimentação”. Porém, disse que esta prática poderia causar expulsão e prisão, reforçando que eles deveriam parar de *hackear* linhas telefônicas, pois estavam causando problemas e prejudicando a todos os estudantes.

Em 31 de maio de 1966, a matéria de Charles W. Bevard para o jornal *The Crimson*, da Universidade de Harvard noticiou que quatro alunos da universidade e um do MIT, realizaram por 8 meses ligações nacionais e Internacionais pela *Bell System* até serem pegos. Foi identificado um caderno de anotações chamado “*Fine Arts 13*”¹³ com 121 páginas das pesquisas do grupo sobre o tema.

¹² A tic-line são geralmente utilizadas para fazer ligações interna de empresas.

¹³ Segundo o *The Crimson*, Fine Arts 13 foi um curso ministrado a partir de 1952 por estudantes de arquitetura, que sugeriam em seus grupos de estudo o que poderia ser lido de forma útil, mas não essencial. O foco do grupo era “estimular o pensamento criativo e desenvolver um olhar crítico, retardando o curso da pesquisa para um objeto específico”. O curso ajudava a desenvolver o pensamento criativo e a verbalizar experiência. E era considerado “o melhor curso em Harvard”. O curso ficou voltado para a área de artes até ser extinto de 1991, por considerarem sua carga de leitura e métodos não eram mais interessantes. Fonte: <https://goo.gl/VitgRx>

Segundo Bevard (1966), a história teria começado em 1962 quando os estudantes descobriram por acidente um código que os permitia ignorar o operador, até conseguir identificar os números do "*inward operators*" (operadores internos) da empresa em Boston, que completavam as ligações para qualquer localidade, deduzindo que eram funcionários da própria empresa.

Posteriormente, estes alunos descobriram que era possível contornar a ligação para qualquer operador por meio da emissão da frequência de 2600Hz, os ligando diretamente as *trunking lines*¹⁴, construindo assim um dispositivo capaz de reproduzir os tons das 12 frequências utilizadas para controlar equipamento de telefone automaticamente, além de identificar que era possível realizar a operação por meio de assovios ou instrumentos musicais. (LAPSLEY;2013, BEVARD,1966)

Segundo Himanem (2001, p.8), “os próprios *hackers* sempre admitiram essa aplicação maior de sua atuação ”, tendo a possibilidade de envolver “um perito ou entusiasta de qualquer área. É possível ser um *hacker* em Astronomia, por exemplo”, dando assim a possibilidade de ser um *hacker* sem ter nada a ver com computadores.

As motivações para a prática de hackeamento de linhas telefônicas eram muito variáveis. O fato é que a prática foi gradualmente se ampliando para fora do meio universitário, até se desenvolver o *phreaking*.

Um *phreaker* não é necessariamente um *hacker*. Um *phreaker* poderia apenas utilizar o equipamento ou o produzir a partir de instruções prontas. O *hacker* era capaz de fazer adaptações, modificações e desenvolver tais manuais, por meio de sua curiosidade e pesquisa.

Douglas Martin do *The New York Times* (2007), afirma que os *hackers* de telefone teriam sido os precursores dos *hackers* de computação, começando como um grupo disperso de adolescentes “interessados em aprender ou usar redes de telefonia” (LAPSLEY;2013)

Não era exclusivamente necessário que tal procedimento fosse realizado com uma *blue-box* (ou alguma de suas versões¹⁵). Também por volta da década de 60, segundo Martin (2007), um deficiente visual chamado Joe Engressia, que estudava na *University of South Florida* e era conhecido como “*Whistler*”, conseguia atingir a frequência de 2600hz assoviando¹⁶.

¹⁴ Segundo Machado e Sondré (2009), o entroncamento ou ‘trunkin’ é o conceito pelo qual um sistema de comunicações pode fornecer acesso à rede para vários clientes, por meio da partilha de um conjunto de linhas ou frequências, ao invés de proporcioná-las individualmente.

¹⁵ Além das blue-boxes, existiam red-boxes, black-boxes, entre outras que eram modelos com diferentes arranjos técnicos e com funcionalidades semelhantes. Também era possível realizar o procedimento sem o equipamento, utilizando-se por exemplo de apitos que atingiam a frequência.

¹⁶ Entre 1991 e 2007 (quando veio a falecer) era chamado de Joybubbles. É possível ver Engressia atingindo a frequência de 2600HZ com um assovio em: <https://goo.gl/O6F0O2> . Maiores informações sobre phreaking podem ser encontradas no documentário “History of Hacking” disponível em: <https://goo.gl/2Czict>

Ele foi expulso da faculdade pouco depois, acusado de violações na linha telefônica e por cobrar dos alunos US\$ 1 por ligação, como uma consequência de uma série de medidas tomadas pelas empresas de telefonia nos Estados Unidos para evitar que esse tipo de prática se popularizasse (FLORY;1990). Orth (1971), afirma que Engressia memorizou entre os 12 e 16 anos, entre 4.000 e 5.000 números de telefone.

Martin (2007) descreve que Joe havia se tornado uma lenda ao redor do mundo falando ao telefone e ouvindo a si mesmo do outro lado e, segundo escritor e jornalista Ron Rosenbaum, ele teria sido o catalizador que reuniu os *phreakers* ao redor do mundo e se tornou “o centro nervoso do movimento”.

Posteriormente Engressia conheceu John Draper. Juntos descobriram que um apito de brinquedo que vinha como brinde do cereal *Cap'n Crunch* também atingia tal frequência. Draper ficou conhecido como *Captain Crunch* (ou Capitão Crunch) pela façanha e começou a desenvolver e vender *blue-boxes*, se tornando um dos *phreakers* mais conhecidos da época (LAPSLEY;2013, MARTIN;2007). Teria sido por *phreakers* como eles que a prática havia sido ampliada.

Por esse motivo, separamos *hackers* de linhas telefônicas dos *phreakers*, para evitar comparações, uma vez que teriam sido os *phreakers* que popularizaram a prática na década de 1970 para a população e geral. Foi o período em que também foram abertas uma série de investigações, acusações e prisões por fraude no sistema telefônico, mas, ao mesmo tempo, muitos *hackers* de computação que vieram posteriormente, absorveram muitas destas posturas em sua própria comunidade, principalmente em relação ao anonimato, a curiosidade e a exploração de limites de um sistema, de um software ou de um hardware.

2.3 Phreakers (1970)

Segundo a definição do *The Jargon File*, *phreaking* é a ciência de “craquear” (ou quebrar) a rede de telefonia, uma atividade que era "semi-respeitada" pelos *hackers*. Originalmente, havia um acordo de que o *phreaking* deveria ser uma atividade semelhante a um jogo intelectual e de exploração.

Porém, teria ocorrido uma conversão do próprio sentido desta comunidade, influenciada pela divulgação da prática para o público em geral. Foi um período que começaram a existir graves fraudes no sistema de telefonia e a circulação de *fanzines* especializados na área, em especial a *Youth International Party Line*, que depois mudou o

nome para TAP Magazine (*Technological American Party* ou *Technological Assistance Program*) produzida pelos *Yippies*.

2.3.1 Popularização das Blue-Boxes

Os primeiros detalhes sobre a comunidade foram tema de dois artigos publicados entre outubro e novembro de 1971. O primeiro, e mais conhecido, na revista *Esquire* chamado “*Secrets of the Little Blue Box*” de Ron Rosenbaum, que entrevistou um *phreaker* chamado Al Gilbertson¹⁷, que deu ao jornalista acesso à informações importantes que revelaram, pela primeira vez, a dimensão da prática do *phreaking*.

Além oferecer detalhes técnicos de como era feita uma ligação gratuita, ele destacou as vantagens de se fazer uma ligação gratuita. Explicava que pessoas como Al Gilbertson tinham um sentimento de poder em desenvolver e utilizar uma *blue-box*, sabendo que se fosse bem utilizada, eles não poderiam ser pegos, permitindo “ficar no escuro em muitos níveis que você gostaria, permitindo que você ligue sem ser rastreado se fizer do jeito certo.” (Rosenbaum, 1971, p.121). O jornalista revelou um verdadeiro comércio que estava se desenvolvendo para a venda dos equipamentos, a exemplo de um lote para Las Vegas de 1.000 *blue-boxes* a US\$300,00 cada.

Gilbertson falou abertamente do descuido que as empresas de telefonia tiveram ao publicar os artigos no periódico *Bell System Technical Journal*, com detalhes fundamentais para o desenvolvimento do equipamento. Assim que ele encontrou o artigo, correu para o laboratório e em menos de 12 horas desenvolveu seu primeiro modelo de *Blue-box*. Ele afirmou que, mesmo que a empresa tentasse retirar os artigos de circulação, as frequências necessárias para realizar um *phreaking*, já haviam se tornado públicas. (ROSEBAUM;1971)

Segundo o artigo de Rosenbaum, o circuito de comutação da companhia era incapaz de distinguir a diferença entre um apito ou um equipamento que emitisse o som, o que seria diferente caso ainda tivesse um operador. Quanto maior era a empresa e mais distante estivesse de um possível operador, mais vulnerável a empresa ficava, revelando um profundo conhecimento dos *phreakers* do próprio sistema de telefonia.

Rosenbaum afirma que uma rede *underground*¹⁸ de telefone havia se desenvolvido nos Estados Unidos¹⁹ e ele teve acesso a ela, encontrando diversas conferências, nomes, grupos,

¹⁷ Pseudônimo

¹⁸ *Underground* se caracteriza como um ambiente que foge dos padrões convencionais

¹⁹ Lembrando que a prática não era uma exclusividade dos Estados Unidos.

além, claro, de contatar *Captain Crunch*, um dos mais conhecidos e antigos praticantes do *phreaking*.

Durante a entrevista, alguns entrevistados afirmavam que na realidade estavam explorando sistemas, computadores, e entendiam que as companhias de telefonia nada mais eram que um computador. Um dos mais antigos *phreakers* da Costa Oeste dos Estados Unidos, chamado Mark Bernay²⁰, afirmou que aprendeu boa parte do que sabia, por curiosidade própria, lendo jornais antigos da área de eletrônica.

Taylor (1999) descreve que os interesses de Bernay começaram a mudar quando ele entrou em uma empresa de computação e ficou fascinado com as senhas que restringiam o acesso a certas informações. Posteriormente passou a pensar em formas e desenvolver programas para descobrir estas senhas. Durante estes momentos ele afirma que passava a usar o codinome de “*The Midnight Skulker*²¹”, e era motivado com o sentimento de ser pego e gradualmente, administradores destas empresas passaram a se preocupar com roubo de informações. (ROSENBAUM;1971, TAYLOR;1999)

Mungo (1993, p.20) afirma que:

O artigo de Rosenbaum em 1971 introduziu os americanos pela primeira vez para uma nova contracultura, a da alta tecnologia que tinha crescido no meio deles, envolvendo um grupo de viciados em tecnologia, que sintetizou o *ethos* da nova década. À medida que os anos sessenta terminaram, e os anos setenta começaram, a cultura da juventude – e sua estranha mistura de música, moda e postura adolescente – tinham se tornado mais fortes e radicais.

O artigo de Maureen Orth para Los Angeles Times, chamado “*For Whom Ma Bell Tolls Not*”, começa descrevendo uma ligação de Cap. Crunch para a embaixada americana na Rússia e descreve que havia entre 200 e 300 integrantes envolvidos em “*phone freaks*”. Principalmente a partir da década de 60 quando as companhias de telefone dos Estados Unidos investiram bilhões de dólares em um sistema baseado em 12 tons²², atraindo uma série de estudantes e adolescentes que se consideravam “*Phone freaks*”, por controlar os sinais como operadores, sendo possível segundo o artigo desligar uma cidade inteira em menos de 45 minutos, tornando o sistema “ocupado”.

²⁰ Pseudônimo. Geralmente hackers usam a expressão “aka” (“Also Known As”), seguidos de seu “nome real” para ressaltar seus pseudônimos. Exemplo, John Draper aka. Capitão Crunch.

²¹ HQ de 1958 que descreve o personagem BC que durante o dia era o pacato e humilde BC e a noite se tona o “Vigilante Noturno” (*The Midnight Skulker*)

²² Para maiores detalhes sobre DTMF. In: Wikipédia: a enciclopédia livre. Disponível em: < <https://goo.gl/YP0kH1> > Acesso em: 10 jan 2016.

Muitas pessoas foram declaradamente influenciadas e introduzidas ao *phreaking* por meio destes dois artigos, entre eles Steve Jobs²³ e Steve Wozniak²⁴ que aprenderam a produzir *Blue boxes* com o Capitão Crunch e a aperfeiçoaram criando um dispositivo digital (mais fácil de utilizar) e financiaram um ano na faculdade (POOLE;2005).

Segundo Wozniak (*in* Lapsley, 2013): “ Ele (Steve Jobs) uma vez me disse que a Apple nunca existiria sem a *blue box*. E eu concordo”. Wozniak define que um *hacker* quer chegar aos seus limites, descobrir algum detalhe que não estão nos livros.

Não por um acaso, anos adiante, em janeiro de 2007, a Apple, fundada por Jobs e Wozniak lançaria o iPhone, se tornando uma referência e mudando o conceito do ramo de *smartphones*, integrando em um mesmo aparelho: celular, câmera, mp3, acesso à Internet de maneira simples e dinâmica. Colocando em prática e ampliando conceitos de autores como McLuhan, de um computador como uma extensão da vida do homem.

Crunch fez parte do *People's Computer Club* (PCC) que viria a se chamar *Homebrew Computer Club* a partir de 1975, na região do Vale do Silício, reunindo *hackers* e entusiastas da computação visando debates sobre a construção de computadores pessoais, onde segundo Poole (2005), foi pensado o APPLE-1.

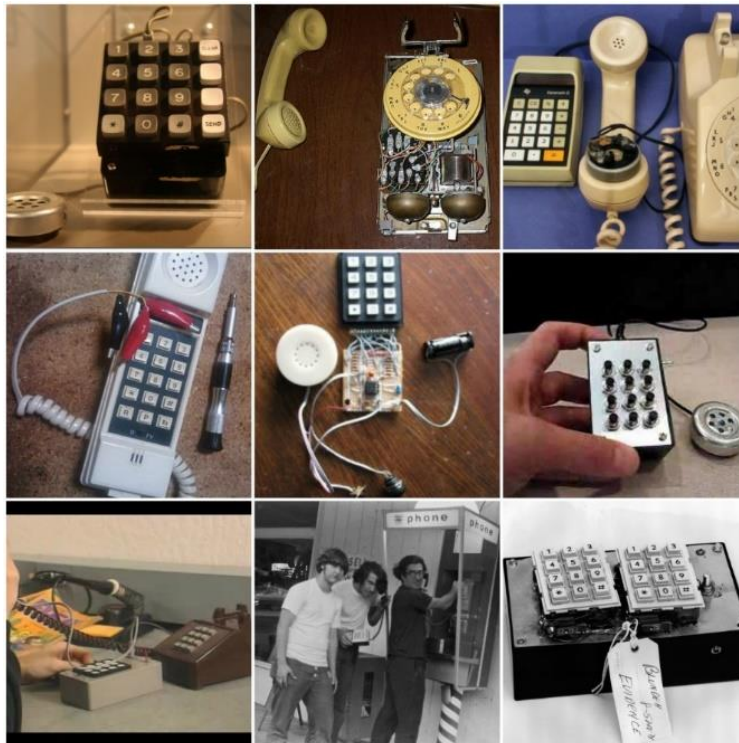


Ilustração 05: Modelos de *Blue-Boxes*
Fonte: Reprodução/ Pesquisa

²³ O telefone e o computador foram as duas paixões de Jobs, que em 1994 chegou a declarar que se não fosse a Blue-box, talvez a Apple nunca existisse. Entrevista disponível em: <https://goo.gl/5ogUKp>

²⁴ Segundo Poole (2005) a primeira ligação de Wozniak foi para o Papa, “para se confessar”.

Em 1972, o *phreaker* Ray Oklahoma publicou na revista Rampart o artigo “*Regulating The Phone Company In Your Home*”, que não apenas explicava as vantagens das blue-boxes, mas efetivamente instruía o leitor que não estivesse efetivamente familiarizado com a técnica, a anotar as peças necessárias para fazer uma versão de uma blue-box e não mostrar o artigo da revista na loja. Mostrando detalhadamente, o passo a passo para produzir um equipamento, semelhante, mas que não realizava ligações internacionais. Na época, a *Bell Company* conseguiu na justiça a autorização para que fossem retiradas de circulação desta edição da revista.

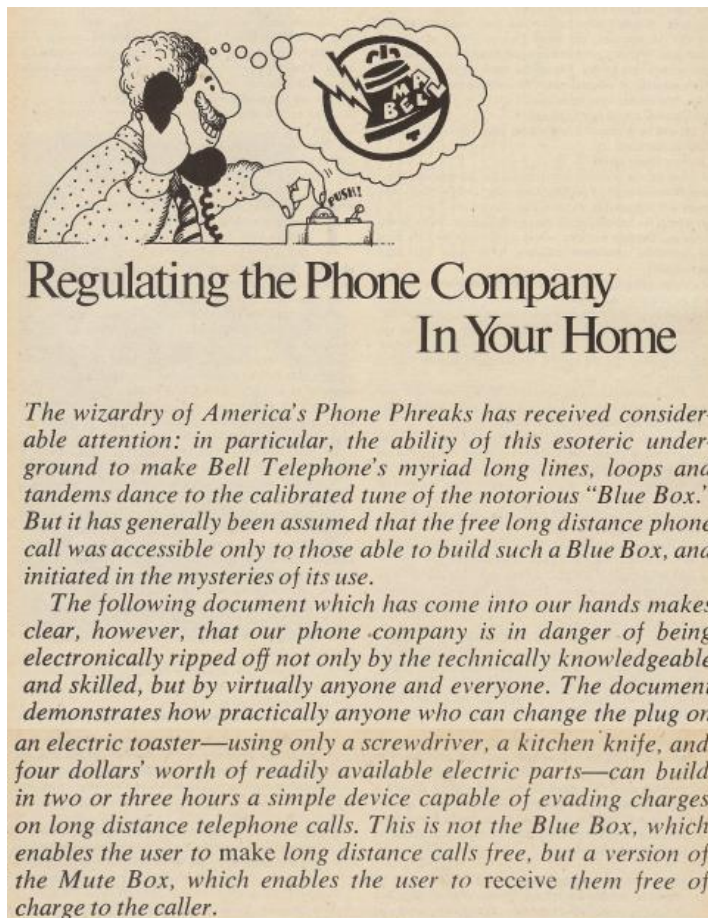


Ilustração 06: Fragmento da edição de 1972 da Revista Rampart
Fonte: Revista Rampart

Com tantas informações nos artigos, as empresas de telefonia ficaram em alerta. A *Bell Company* juntamente com o governo, tomaram medidas técnicas, como detectores que identificavam a emissão da frequência de 2600Hz e legais, como a abertura de amplas investigações na tentativa de desencorajar novos casos e tentar reduzir o prejuízo que as empresas sofriam anualmente. (FLORY;1990)

2.3.2 Phreaking como forma de protesto. Hackers Underground

No final da década de 1960, a juventude se tornava o centro das atenções em função de uma série de protestos que eclodiam ao redor do mundo, com uma forte crítica política e social ao capitalismo e a sociedade de consumo. Segundo Silva (2011,p.53):

Aos anseios de maior liberdade política soma-se a revolta contra toda a forma de autoridade, desde aquela exercida pelos pais até a do Estado, passando pela do professor, do policial, ou de qualquer adulto com mais de 30 anos. Essa luta, que inicialmente questiona as instituições escolares, também capta outros conteúdos potencialmente revolucionários. Rapidamente as revoltas estudantis contribuíram para um questionamento da maneira de viver na sociedade como um todo, principalmente com relação aos papéis futuros reservados aos jovens naquele modelo de sociedade.

Enquanto para Cardoso (2005, p. 94):

Os movimentos dos anos de 1960, seja na sua expressão mais propriamente política, seja na contracultura, ou mesmo nos modos em que combinaram essas expressividades, tiveram como traço característico a transgressão de padrões de valores estabelecidos. Transgressão não no sentido de uma pura negatividade, ou de uma negação absoluta dos limites estabelecidos, mas de um movimento que os atravessa afirmando novos limites. Em outros termos, um movimento que é de negação de valores estabelecidos, mas que na sua face positiva se lança no risco da afirmação de novos valores.

Os movimentos de contracultura²⁵ da década de 1960, estavam em seu auge nessa época, sendo, do ponto de vista de Sterling (1986) associado à sua visão romantizada e principalmente anticapitalista, antitecnológica e anticiência, mas que sempre encontrava alguma contradição, uma antítese a sua essência. No entanto nunca houve uma única e unificada contracultura (STERLING,1986; TURNER,2006; STREETER,2010)

Em janeiro de 1968 Jerry Rubin (1938-1994) juntamente com Abbie Hoffman (1936-1986), um ativista social e político dos Estados Unidos nascido em Long Island, fundaram o *Youth International Party* (Partido Internacional da Juventude), também chamados de *Yippies*, uma variante dos *Hippies*, considerados “hippies politicamente engajados”²⁶. Entre os fundamentos do movimento está a cooperação, a falta de hierarquia, a liberdade, o pacifismo, o sentido de comunidade e um “contraditório” senso de desobediência civil.

Em agosto de 1968, as barricadas que ocorriam na cidade de Chicago, foram amplamente televisionadas e Hoffman aprendeu a utilizar os meios de comunicação ao seu

²⁵ Os movimentos de contracultura, segundo Zappa (2011) teriam tido “ sua origem em meados da década de 1950 com os *beatniks*, grupos de jovens escritores e poetas que manifestavam seu inconformismo com os valores tradicionais cultuados pela classe média americana”, sendo uma das principais bases da filosofia dos hippies uma década adiante.

²⁶ Segundo Zappa (2011), os hippies repudiavam as instituições estabelecidas e valores da classe média. O movimento recebia duras críticas tanto de setores conservadores quanto de movimentos sociais e políticos em função de sua falta de organização.

favor. O mais importante segundo Wainberg (2015, p.16) era aparecer na televisão enquanto estavam sofrendo algum tipo de repressão policial e advertir que “o mundo estava olhando”.

Hoffman se tornou uma das figuras mais importantes do movimento de contracultura. Uma de suas obras mais conhecidas “*Steal this Book*” (“Roube este livro” de 1971) é dividido em três partes: *Survive* (com orientações para conseguir dinheiro, alimento, roupa e moradia de graça); *Fight* (com orientações de defesa pessoal) e *Liberate* (com dicas de sobrevivência e roteiros culturais e artísticos em Los Angeles, Nova York, Chicago e São Francisco). Um livro que segundo Sterling (1994) teria sido o “ancestral espiritual do vírus de computador”

Como aponta Flory (1990), as Blue-boxes eram usadas por diversos grupos com agendas muito variadas. Contudo parece contraditório pensar que uma prática como o *phreaking* tenha se desenvolvido neste meio ou que tivesse alguma relação como o movimento de contracultura, mas foi o que aconteceu. Clough e Mungo (1992, p. 21) afirmam que “um passatempo que antes era apolítico, foi adotado por um movimento radical. Era a mistura estranha, dos viciados da alta tecnologia ao lado de revolucionários teatrais da extrema esquerda, todos foram parte da contracultura”.

Sterling (1994) explica que houve uma sobretaxa nos serviços²⁷ de telefonia durante a Guerra do Vietnã (1955-1975) e que Hoffman acreditava que o *phreaking*, era uma forma de desobediência civil, já que não forneceria fundos para uma guerra que ele considerava imoral. (STERLING;1994).

Se tornou uma prioridade/ necessidade passar este conhecimento para outras pessoas na década de 1970 e, como Sterling (1994, p.28) destaca, em junho de 1971, Hoffman e um entusiasta do telefone, que era sarcasticamente conhecido como Al Bell²⁸, começaram a publicar um boletim chamado *Youth International Party Line* (YIPL)²⁹.

Segundo Lapsley (2013, p.470)

YIPL foi idealizada por Alan Fierstein e um dos fundadores dos Yippies, Abbie Hoffman. Fierstein foi um dos maiores engenheiros na *Cornell University* que no

²⁷ Segundo o editorial da YIPL/TAP Magazine de 1971, em abril de 1966, o congresso passou uma lei que aumentava a taxa nos serviços de telefonia em 10% e davam informações de como se recusar a passar este valor para as empresas.

²⁸ Pseudônimo. Nome verdadeiro: Alan Fierstein.

²⁹ A YOUTH não era a única revista que influenciou o meio *hacker*. Outra publicação declaradamente relacionada aos movimentos de contracultura, porém com raízes mais voltada a comunidade *hippie* foi o “*Whole Earth Catalog*”, que influenciou figuras como o próprio Steve Jobs e a região do Vale do Silício. Fred Turner na obra “*From counterculture to cyberculture*” descreve a história deste grupo e indivíduos que efetivamente fizeram a conversão da contracultura para a cibercultura. Steve Jobs em seu famoso discurso na Universidade de Standford em 2005 descreve que quando ele era pequeno uma das bíblias de sua geração foi o *Whole Earth Catalog* e que “tudo era feito com máquinas de escrever, tesouras e câmeras Polaroid”. Segundo Jobs “Em sua edição final em meados dos anos 70(...) Na contracapa havia uma fotografia de uma estrada de interior ensolarada, daquele tipo onde você poderia se achar pedindo carona se fosse aventureiro. Abaixo, estavam as palavras: Continue com fome, continue bobo. Foi a mensagem de despedida deles.(...) E eu sempre desejei isso para mim mesmo”. (JOBS,2005)

final da década de 1960, passou a se interessar pelo sistema de telefonia. Com base em suas próprias investigações e através de conversas com seus colegas estudantes de engenharia, descobriu diversas formas de se fazer chamadas telefônicas gratuitas. Mas Fierstein diferia de muitos *phreakers* de telefone de uma maneira importante: ele era fortemente politizado. Como um estudante liberal³⁰ no final de uma década tumultuada, ele lembra que a sua missão era “acabar com a Guerra do Vietnã e se opor a Nixon de qualquer maneira possível.”

Published Monthly June, 1971

THE YOUTH INTERNATIONAL PARTY LINE'S FIRST ISSUE

We at YIPL would like to offer thanks to all you phreaks out there. Host of you who are not receiving this yet us in Washington on Monday, where we distributed 10,000 phone flyers. So far we have received over 50 responses, complete with contributions, encouragement, and spirit. We may not have done well percentage-wise, but the fact that there are 50 people all over the country willing to fight back speaks for itself. We are sure that from the spirit of the response, YIPL membership will really skyrocket. However, more important than our numbers in our opinion, is the swelling and motivation for this movement. The disappointment we feel toward Amerika has turned to hatred as we saw the futility of the movement to improve it, and to frustration as our outside efforts were repressed and forbidden. But did not turn our backs on the movement for change. YIPL believes that education alone cannot affect the system, but education specifically, YIPL will show you why something must be done immediately in regard, of course, to the improper control of the communication in this country by none other than the BELL TELEPHONE COMPANY.

So if your friends want to get in on the fun, let them read your newsletter, and you might want to research your own questions in your local library, and help to start the education of your community of the phone company's part in the war against the poor, the non-white, the non-conformist, and in general, against the people. Show your neighbors, friends and representatives of your area how the Bell System and the government are co-conspirators. If your friends can't subscribe to YIPL, that's cool, is convenient for our small staff, and is right on need stamps, letters, and envelopes, which maybe they can get from their office at work. Because we are already sending out issues to people short on bread, we really do need this kind of help. We will report on all of our finances from time to time, and if you can do it, we will probably need some kind of bail fund set up. If any YIPL busts happen, we'd like to ask you all in advance to work extra hard for the cause. People, thanks again. Love

THE CREDIT CARD CODE

The 1971 Credit Card system works as follows: The telephone number (7digits) of the number to be billed is followed by the secret number for the area code of the number. They are listed below for several cities. At the end of the number comes a letter that matches the sixth digit of the telephone number. Many people look up the number of a large company in the area and use their number, cause using any old number might lead to that person refusing to pay, and the phone company's hasseling the person to whom the call was placed. They should say that others use that phone, and they don't know anything. Fraud is illegal, so we don't think you should make free calls. This Code has already been written in many underground papers, as you know.

Detroit-003	Boston-001	Phila.-041	1-Q	4-H	7-S
Washington-032	San Fran-93	Fitts-030	2-A	5-J	0-U
New York-021	Chicago-097		3-E	6-N	9-W

Example- 760-1900-069-Z (I.B.K. Jant,N.Y.)

In April of 1966, as the government was escalating the Vietnam war, Congress passed a law raising the Federal tax on telephone service to 10%. "It is clear," said Rep. Wilbur Mills, Chairman of the House Ways and Means Committee, "that Vietnam and only the Vietnam operation makes this bill necessary". -Congressional Record, February 23, 1966.

The War Tax Resistance is showing people how to refuse to pay this war tax. In most cases, the IRS will come to collect with 6% interest, but your phone service will continue. But the more it's done, the more it costs them in time, trouble and subarmanent for Uncle Sam. Do it, and tell your friends, relatives and neighbors to do the same. Include a letter to this effort to the phone company and your congressman.

IN NEED

How do we communicate with our people serving time in Lam? WPAX has a way. They're putting rock and soul and rap and education tapes on the air through Radio Hanoi, who is donating free air time to broadcast these "subversive" sounds, now banned by our government's stations. But WPAX needs your blank and recorded tapes, and of course, bread. Send what you can. If you want to record your own show to be aired, ask them for details and they'll be happy to supply them. WPAX, Box 110, Cooper Station, N.Y., N. 10003

GETTING PAST ISSUES OF YIPL

Obviously, as people join up later on they're going to want info that was already published. So we'll have a stock of past issues, available at the ridiculous (?) price of 50¢ each. This might start to erase our deficit but we'll lower the price if we can get enough contributions.

IN OUR NEXT ISSUE

We will have more letters, info, shit and our man on the scene, Al Bell, who have some inside info on the "Blue 20" that people all over the country are using on the Bell. Plus a dialogue with Russel Baker and Abbie Hoffman on Phone

BECAUSE OF THE BRUTAL AND AGGRESSIVE war the United States government is conducting against Vietnam, the amount of the Federal excise tax, \$1.00, has been deducted from my pay. I have opposed this war and protest against it in many ways. Now I must testify to my opposition by refusing to pay this tax.

The telephone excise tax was raised in April, 1966, only in order to help pay for the war in Vietnam. Paying the tax means helping to pay for outright atrocities, for the murder of innocent women and children, for means helping to pay for the indiscriminate bombing and reaping of senseless villages. It means helping to finance the shipping of American boys half way around the world to die defending an unpopular, totalitarian and corrupt regime.

I am sorry for any inconvenience my tax refusal may cause your office and hope you will understand that this protest is not directed against the telephone company. I hope also that you will soon join me and the many others who have decided that it is no longer necessary to oppose the war by refusing to pay the telephone excise tax that helps finance it.

Sincerely in peace.

Distributed by
WAR TAX RESISTANCE
339 Lafayette Street
New York, N.Y. 10012

TAP is YIPL's new name.

We beg you consider donating a small percent of what TAP helps you save. One year of newsletters is a \$2 check. TAP, Room 504, 152 W. 42 St., N.Y., N.Y. 10008

Ilustração 07: Fragmento da primeira edição da *Youth International Party Line*
Fonte: Youth International Party Line

Hoffman também fundou a revista *Chicago 7*³¹ e ofereceu apoio a John Draper que havia sido preso em 1972 (TAYLOR;1999) . A YIPL posteriormente passou a ser chamada de *TAP Magazine* (*Technological American Party* ou *Technological Assistance Program*) e seguiam um modelo semelhante a um *fanzine*, mantendo um modelo de publicação que mesclava a parte técnica com debates políticos. Estima-se que haviam cerca de 1400 leitores do boletim na década de 1970 (STERLING;1994).

Segundo Triggs (2006) originalmente, os *fanzines* teriam surgido no início da década de 1930, sendo caracterizados como parte de uma comunicação independente, feita por uma cultura *underground*, especializados em divulgar e compartilhar informações, conteúdo de

³⁰ Nos Estados Unidos, ser liberal equivale a ser de esquerda.
³¹ Em referência ao próprio Abbie Hoffman, Jerry Rubin, David Dellinger, Tom Hayden, Rennie Davis, John Froines e Lee Weiner, formando os sete acusados de conspiração, incitação à revolta e protestos contraculturais em Chicago (Illinois) durante a Convenção Nacional Democrática 1968 (Wainberg, 2015 p.17). Para mais informações sobre os yippies, o Massacre de Chicago e o julgamento dos 7: “1968: eles só queriam mudar o mundo” de Regina Zappa e Ernesto Soto

temas variados que interessam a estes indivíduos, além de opiniões pessoais de membros envolvidos em alguma rede ou comunidade específica.

Geralmente eles são feitos à mão ou datilografados em uma folha A4, com recortes e colagens, criando uma identidade visual reconhecível do *do-it-yourself (DIY)*³² e são popularmente associadas ao Movimento de Contracultura do final da década de 1960 e largamente utilizados pelos *punks*³³ da década de 70 (TRIGGS;2006).

Em 1974 o FBI abriu uma investigação³⁴ contra a YIPL/ TAP.

A partir das publicações da TAP criou-se uma verdadeira rede de contatos ao redor do mundo³⁵, com informações técnicas que possibilitavam a exploração das linhas telefônicas. Graças a estas publicações, que vieram antes mesmo da comercialização e popularização dos computadores, permitiu que uma verdadeira cena hacker *underground* fosse desenvolvida fora do meio acadêmico, do controle do governo ou de interesses comerciais. Segundo Turgeman-Goldschmidt (2010)

"As culturas *underground* de computadores existem em todo o mundo, com membros que operam em ambientes sociais fornecendo apoio, conhecimento, desenvolvimento profissional, literatura, web sites, e conferências (Jordan & Taylor, 1998). Hackers são um grupo distinto, com suas próprias éticas (embora diversificada), cultura, estilo de vida, dialeto, filosofia, etc. Eles se veem como diferentes, especiais, e até mesmo superiores. Eles operam em grupos, e há muitos sites na Internet dedicados a filosofia e as atividades dos hackers. (...) Como Holt (2008, p 352) estabeleceu: "Os laços sociais *on* e *offline* entre hackers foram usados para compartilhar informação, ferramentas, e introduzir normas sub-culturais para novos hackers." Hackers, então, desenvolveram uma identidade social construída por eles mesmos. Como as redes sociais, eles conseguiram criar uma identidade única, distinta, e positiva, que "vendem" para os outros."

O período que marca o declínio do *phreaking* (1976-1983) foi ao mesmo tempo a época em que houve o início da comercialização dos videogames e dos computadores pessoais. O que fez com que *phreaking* e *hacking* de computador se convergissem entre a década de 1970 e o início da década de 1980.

³² Faça você mesmo

³³ Fanzines eram chamados de "Zines" pelos punks.

³⁴ Cópia da investigação disponível em: <http://www.historyofphonephreaking.org/docs/yipl-fbi.pdf>

³⁵ A TAP ainda oferecia um espaço, para cartas e informações enviadas pelos leitores.

Em 1983 foi lançado o filme *War Games* (Jogos de Guerra) que narra a história de David, um jovem curioso e apaixonado por videogames que acaba descobrindo sem querer um jogo de simulação, e após muita pesquisa consegue acessar pelo seu computador o jogo “Guerra Termonuclear” desafiando os Estados Unidos e a União Soviética, sem saber que abriu uma contagem regressiva para uma possível Terceira Guerra Mundial, uma simulação que nem ele, nem mesmo o governo sabiam.

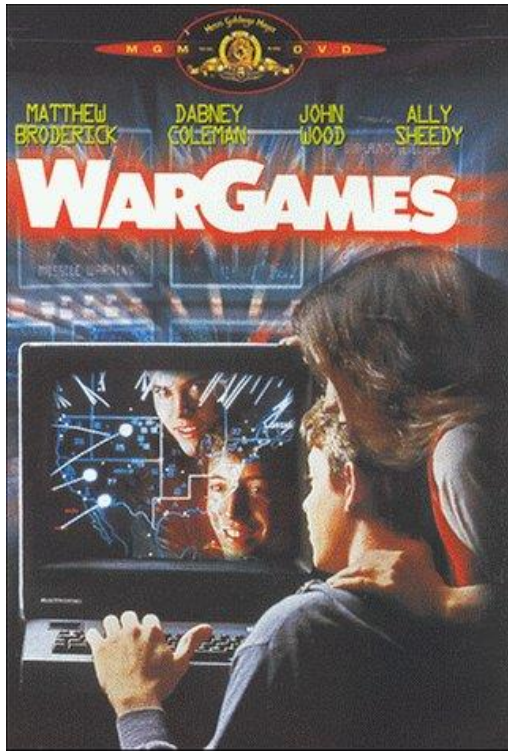


Ilustração 08: Cartaz do filme WarGames
Fonte: Divulgação

O filme teve um papel primordial para popularizar o meio hacker, principalmente entre os jovens que em alguma medida, queriam ser como David, personagem do filme. Foi um período que ambas práticas passaram a se popularizar (inclusive no Brasil) e ter uma conotação negativa por parte da mídia.

Segundo o Jargon File de 1983, a prática teria perdido completamente seu "*ethos*"³⁶ na década de 1980, quando o phreaking passou a ser praticado de maneira criminosa levando a diversas punições contra grupos como o 414³⁷. Alguns membros da atual geração de hackers, sequer conhecem uma blue-box. (JARGON FILE; 1983)

³⁶ Modo de ser

³⁷ 414 era o número do código telefônico de *Milwaukee*, e a escolha do nome foi associada a práticas de gangs, que tiram seus nomes dos números das ruas. Grupo detido em 1983.

Em janeiro de 1984, a revista estadunidense 2600³⁸ começa a circular, e em seu editorial “AHOY!³⁹” explica que a publicação surgiu por uma necessidade “daqueles que realmente apreciam o conceito de comunicação, os entusiastas da tecnologia”. Demonstrando assim como termos como *hackers* ou *phreakers* estavam sendo utilizados para denotar termos como “criminosos ou anarquistas” e buscavam não julgar ninguém, apenas expor ideias e informação. Ainda segundo o editorial:

“Muita coisa mudou desde que o filme Jogos de Guerra foi lançado e a 414 foi pega. Eventualmente todos estão falando de *hackers* e *phreakers*. Embora tenha havido uma espécie de salto daqueles que queriam ficar em evidencia, outros ficaram mais cautelosos. Na verdade, ficaram bem chateados. Claro, a publicidade é divertida, mas qual seria o custo? Bem o tempo passou e o custo foi alto. Muitos *hackers* e *phreakers* foram forçados a um isolamento virtual. A única revista direcionada (a TAP) sumiu misteriosamente no auge da crise levando a rumores que eles também teriam sido pegos. No entanto a revista ressurgiu em novembro com a desculpa de que um incêndio destruiu sua lista de contatos.⁴⁰

Mesmo que atualmente, muitos hackers de uma nova geração, sequer conhecem a história do *phreaking*, as contribuições para a construção da cena hacker *underground* que se sucedeu na década de 1980 foram muito férteis: seu sentido de comunidade, de compartilhar informações, de pesquisar limites de um sistema, sua falta de hierarquia e liderança e até mesmo seus traços de “desobediência civil” e políticos podem ser melhor compreendidos, quando se conhece com mais profundidade a história do *phreaking*.

2.4 Conclusões:

Parte deste capítulo se voltou para a narrativa do *phreaking* nos Estados Unidos, uma vez que estudos aprofundados da prática em outros países ainda são escassos. Não temos dados suficientes que tenham analisado os impactos econômicos e sociais do *phreaking* em outros países como Reino Unido, França, Austrália, Espanha, Suécia, entre outros. As informações aqui reunidas fóruns da comunidade década das décadas de 1980 e 1990⁴¹.

Sabe-se que o *phreaking* se manteve em países como a Alemanha, ainda em 1991, no período de reunificação do país, em especial, do antigo lado comunista, em que os equipamentos permaneciam mecânicos, logo, mais obsoletos, como debatidos em antigos fóruns.

³⁸ Justamente em referência a frequência de 2600Hz utilizada por *phreakers*

³⁹ Segundo o editorial da 2600, Alexander Graham Bell costumava atender o telefone dessa forma e por alguma razão não pegou. “AhoY” é um cumprimento corriqueiro entre hackers e membros do Partido Pirata (fundado em 2006)

⁴⁰ Tradução nossa.

⁴¹ Em sites como textfiles.com

Em agosto de 1993, o *phreaking* foi definitivamente extinto quando a AT&T introduziu um novo sistema de telefonia digital, que rapidamente identificava e recolhia informações sobre quem emitisse a frequência de 2600Hz. Em 1994, as empresas de telefonia da Dinamarca passaram a registrar todas as ligações nacionais.

Ainda hoje, diversas características e traços tanto do *phreaking*, quanto de movimentos do final da década de 1960, podem ser identificadas em grupos, associações e coletivos que compõem a cena hacker, principalmente quando saímos dos estudos da voltados para os Estados Unidos e nos viramos para tal construção em países na Europa, que por exemplo, ainda mantem um sentido de comunidade e compartilhamento de informações livres. Um ponto que segundo Alberts e Oldenziel (2014), nos permite ainda compreender de que forma “a cultura tecnológica se incorporou em outros contextos sociais e políticos”.

3 HACKERS DE COMPUTADOR

O *hacker* existe antes mesmo da Cultura da Internet. Samuel (2004, p.39) expõe o fato de que os aspectos da chamada “Cultura Hacker” estão bem documentados na rede, e que a “a Cultura da Internet estabelece um novo padrão para documentação sociológica, uma vez que tal cultura tem sido continuamente articulada, documentada e discutida em relação a sua linguagem, tecnologias e normas.”

Durante a realização do levantamento bibliográfico deste capítulo, percebemos que parte considerável das pesquisas acerca do meio *hacker* são voltadas para o pioneirismo de membros de grupos como o TMRC, nos Estados Unidos. Considerado por autores como Steven Levy (2012), Taylor (1993) e Castells (2003) a principal origem do conceito popular do *hacker*, os definindo, segundo Vilbig (2013), como “gênios solitários” que desenvolveram sua ética como produto de um ambiente institucional.

Buscamos assim analisar qual teria sido a possível influência do meio ao qual eles estavam inseridos para moldar o seu perfil, procurando compreender, como traços e características destes programadores e “pioneiros” da computação, primeiramente inseridos dentro das Universidades, teriam sido absorvidos por indivíduos fora do ambiente acadêmico, dando um novo sentido à prática a partir da década de 1970.

3.1 Modelo aberto como estratégia da Guerra Fria

O desenvolvimento dos computadores ocorre em um período conturbado da história, entre o fim da Segunda Guerra Mundial e o pelo início da Guerra Fria em 1947. Boa parte dos estudos referentes à construção da “Cultura hacker” envolvem a perspectiva estadunidense, em função da estratégia utilizada pelo país em comparação a União Soviética (URSS) em relação aos investimentos no setor de tecnologia.

A estratégia utilizada pelo governo dos Estados Unidos foi oferecer e obter investimentos financeiros para os setores de tecnologia e ciências, com recursos livres e pouca burocracia. Atraindo, assim, diversos pesquisadores em diferentes níveis de escolaridade, que se sentiram livres para desenvolver ferramentas essenciais que possibilitaram o pleno funcionamento dos computadores e da elaboração da ARPAnet (*Advanced Research Project Agency Network*), uma das primeiras redes do mundo desenvolvida nos EUA, que começou a operar em 1969. (CASTELLS;2003, PETERS;2016)

O sucesso do modelo aberto dos EUA se deu por subsídios estatais bem geridos com pouca burocracia em ambientes colaborativos de pesquisa. A URSS que disputava a hegemonia política, econômica e militar contra os Estados Unidos, não teve o mesmo interesse e visão para o desenvolvimento, ampliação e investimento nem nas redes nem nos computadores. Pelo contrário, o modelo fechado soviético se mantinha limitado ao controle dos militares e do Estado e ainda tropeçava em interesses pessoais e burocráticos, que idealizavam uma rede capaz de controlar a própria economia (PETERS,2016).

Peters (2016) afirma que o foco dos investimentos soviéticos esteve voltado para áreas como matemática, ciência e uma tecnologia que tinha como prioridade o desenvolvimento e aperfeiçoamento da energia nuclear e de foguetes. Tais investimentos soviéticos geraram uma reação do governo dos EUA. Porém, segundo Powanki (2000, p.95):

Nem todo mundo estava disposto a abandonar a tentativa de chegar a um entendimento com os soviéticos. Em uma carta de 5000 palavras para Truman, datada de 23 de julho de 1946, o ministro do Comércio, Henry Wallace, disse que os soviéticos tinham razões legítimas para temer os Estados Unidos, incluindo a posse da bomba atômica e a criação de bases militares dos EUA em torno da periferia da União Soviética. De acordo com Wallace, a única solução para evitar uma corrida armamentista nuclear seria o "desarmamento nuclear" e a criação de um sistema eficaz que se encarregasse de cumprir tal meta. Oito dias após Wallace novamente criticar a política externa de Washington em um discurso proferido em 12 de setembro no *Madison Square Garden*, Truman o demitiu.

Ter-Ghazaryan (2014) afirma que em 1950 a URSS havia estabelecido uma indústria de computação moderna, chegando a desenvolver na década de 1960 os primeiros computadores pessoais (MIR-1, MIR-2 e MIR-3). Mas os modelos não seguiam um padrão em comum, o que fazia com que versões mais atualizadas não reconhecessem os sistemas dos modelos mais antigos. Segundo Carvalho (2006, p.37) :

Padrões técnicos podem surgir a partir de uma variedade de fontes. Às vezes, a primeira versão de uma tecnologia bem sucedida no mercado define um padrão; outros podem ser negociados via regulamentação ou especificação de normas técnicas; e há ainda os padrões criados e disseminados pelos fornecedores de determinada tecnologia. Os debates sobre padronização aparentemente podem parecer puramente técnicos, porém uma análise mais minuciosa sempre revela a mistura de questões econômicas, políticas e culturais que motivam os argumentos.

A falta de normas e padrões levou a indústria soviética ao atraso, principalmente a partir de 1970, quando o governo resolveu colocar no fim os investimentos no setor de informática e passou a fazer cópias dos sistemas ocidentais. Em 1980, a indústria de computadores soviéticos simplesmente estagnou. (TER-GHAZARYAN;2014). A rede só se popularizou na região após o colapso da União Soviética (entre 1990 e 1991).

Peters (2016) propõe, em sua obra “*How Not Network a Nation*”, uma das análises mais completas do motivo pelo qual a rede criada na URSS não desenvolveu raízes, dizendo que “as primeiras redes de computadores civis foram desenvolvidas por capitalistas de cooperação, não

entre socialistas competitivos. Os socialistas se comportaram como capitalistas e os capitalistas como socialistas” (PETERS, 2016, p.2).

Mas o projeto inicial dos Estados Unidos não teria sido diferente. Streeter (2011, p.22) propõe que a rede surgiu dentro de um contexto militar e sua intenção inicialmente não era a ampliação para dentro do contexto social, talvez pelo alto custo dos equipamentos. Segundo Levy (2010) o preço varejo do computador no início da década de 1960 era de 120 mil dólares. A origem da rede teria ocorrido, de certa forma, acidentalmente, tal como foi com o telefone ou com o rádio, e que só depois que foi desenvolvida, sua aplicabilidade se tornou eficiente dentro de outros contextos, levando governo estadunidense a optar pelo modelo aberto. (STREETER;2011)

Ao mesmo tempo, pensava-se em como desenvolver um código que fizesse uma computação mais interativa e simbiótica, conectada a uma rede operacional de um sistema global integrado.

O lançamento do primeiro *Sputnik* foi a justificativa que o governo do EUA precisava para conseguir ainda mais recursos para os investimentos em alta tecnologia. Foi o auge do chamado “mito pós nuclear”.

3.1.1 O mito pós-nuclear

Poucos trabalhos argumentam a influência da Guerra do Vietnã (1955-1975) e da Guerra Fria para construir o cenário que teria colocado os Estados Unidos no centro da construção da cena *hacker*.

São igualmente escassos os trabalhos que debatam acerca da visão coletivista e os princípios liberais aplicados na política científica do Pós-Guerra, idealizada pelo cientista e administrador do MIT, Vannevar Bush, um político conservador e autor da obra “*Science, Endless Frontier*”(1945). A obra desenha sua própria experiência durante a Segunda Guerra Mundial, particularmente seu envolvimento no Projeto Manhattan⁴², que ele acreditava ter sido bem sucedido e que poderia servir de modelo para outros projetos, ajudando e inspirando na criação de Instituições como a *National Science Foundation* (NSF), que moldaram o pensamento tecnológico nos Estados Unidos nos 50 anos seguintes (STREETER,2011).

Streeter (2011) afirma que parte do “folclore” criado sobre a origem dos computadores e a própria rede pode ser relacionado ao chamado mito pós-nuclear, em referência a uma tática

⁴² Projeto responsável pelo desenvolvimento das primeiras bombas atômicas durante a Segunda Guerra Mundial.

utilizada pelo governo dos Estados Unidos para obter e fornecer investimentos em áreas consideradas estratégicas, com recursos livres.

Porém, era vital que o Governo apresentasse a importância e os benefícios para que empresas privadas investissem em pesquisas avançadas, uma vez que estas acreditavam que não valia a pena correr o risco, sendo necessário criar um “liberalismo corporativista”. Idealizado também por Vannevar Bush, O “liberalismo corporativista” compreendia a importância da cooperação entre Governo e empresas privadas em momentos chave, em nome do desenvolvimento econômico e tecnológico. (STREETER,2011)

Segundo Powanki (2000, p.94) :

Para piorar as relações entre os soviéticos e os americanos durante 1946 diminuiu-se as perspectivas de evitar uma corrida às armas nucleares. Em 14 de Junho de 1946, Bernard Baruch, o representante dos Estados Unidos na Comissão de Energia Atômica da ONU, apresentou o plano americano para o controle internacional da energia nuclear. Como esperado, a União Soviética considerou que o plano era inaceitável. (...) A contraproposta Soviética foi apresentada por Andrej Gromyko à ONU em 19 de Junho de 1946, sendo considerada igualmente inaceitável pelos americanos. Os soviéticos insistiram que os Estados Unidos deveriam desistir de sua vantagem nuclear em troca de uma promessa vaga para os Soviéticos para participar de um sistema de controle internacional. Em 30 de dezembro de 1946, a Comissão de Energia Atômica da ONU aprovou o Plano Baruch, e sua rejeição pela União Soviética fez esta vitória americana não ter sentido e que a corrida armamentista nuclear era inevitável. Além disso, ao rejeitar o Plano Baruch, os soviéticos confirmaram a impressão de que eles eram o principal obstáculo para a paz mundial. Devido a isso, a maioria dos americanos gradualmente aceitaram o argumento do governo Truman no sentido de que o confronto devia ter precedência sobre uma política conciliatória em relação à União Soviética.

Fred Turner (2006) afirma que as Universidades e os adolescentes nos Estados Unidos cresciam em uma época de oportunidades, que seus pais que vieram do período da depressão não puderam acompanhar: eram aparelhos mais sofisticados, automóveis e um maior acesso à educação.

Antes da Segunda Guerra Mundial, do ponto de vista de Turner (2006), o percentual de jovens nas universidades era de 14%. Em 1961, este número subiu para 38% e em 1970 já estava em 50,62%. Isso representava 3 milhões de americanos no Ensino superior em 1959 e 8,5 milhões em 1973. Foi um período com alto financiamento em pesquisas por parte do Governo e os jovens se viam inseridos em um local de exploração e trabalho em conjunto. O mundo, que essa geração crescia, vivia com um sentimento de ansiedade em um mundo com um ataque nuclear eminente, repassando tal temor para os futuros profissionais.

O que mostrava que as universidades estavam bem alinhadas com as políticas implantadas pela Guerra Fria (TURNER;2006) é o fato de que parte das pesquisas tinham como base justamente o mito pós-nuclear: o modelo de rede de Paul Baran, que será exposto mais

adiante, pensava justamente em um cenário de uma nação após um ataque, perdendo sua capacidade de comunicação.

Os próprios jogos (como o *SpaceWar*) descritos por Levy (2012), que funcionavam como programas de computador, simulavam um cenário que usuário estava perdido e modificava os parâmetros dando novas instruções. Os princípios do jogo estavam em acertar torpedos com uma estratégia semelhante a um jogo de xadrez e aulas do MIT: “a programação não é simplesmente uma busca pela técnica, mas uma abordagem para os problemas da vida” (LEVY, 2012, p.48). Bem semelhante a ideia do filme *Jogos de Guerra* (1984) lançado anos adiante.

O Brasil era um dos beneficiados por tal tecnologia, em que a Guerra Fria também se refletia. Segundo Powanski (2000, p. 95) o governo brasileiro, juntamente com outros dezenove Estados latino-americanos, assinaram o Tratado Interamericano de Ajuda Mútua - o “Tratado do Rio” no Rio de Janeiro, em setembro de 1947 - para impedir o avanço do comunismo na região. “O Tratado do Rio foi uma aliança de duração indeterminada e se destinava a proteger contra a agressão de qualquer lugar, mesmo nos países que a assinaram”.

Segundo o jornal *O Globo*, datado de 09 de março de 1961, o Brasil, mais especificamente a Universidade de São Paulo, se tornava uma referência na área de pesquisa, justamente em áreas como a de Física Nuclear e contava com a adesão de equipamentos que facilitavam no processamento de dados científicos e permitiam o envio destes dados a laboratórios que não possuíam tal tecnologia. O setor de pesquisas, foi uma das áreas que posteriormente sofreria cortes e mudanças estruturais profundos durante a Ditadura Militar no Brasil entre 1964-1985. Boa parte dos trabalhos só foi retomada ao fim do regime, segundo a Empresa Brasil de Comunicação (EBC)⁴³.

Desenvolveu-se ao longo da construção dos computadores, a aplicabilidade e utilização de tais equipamentos, oferecendo soluções rápidas e precisas para diversas áreas, de forma que também facilitassem seu uso, proporcionando o desenvolvimento de um processo de simbiose entre homens e máquinas. Esse processo se deu nos Estados Unidos por outra estratégia falha dos soviéticos, influenciada pelo monopólio marxista ainda no período da Revolução Russa.

3.2 Simbiose entre homens e máquinas

⁴³ <http://www.ebc.com.br/ditadura-militar/2014/03/confira-os-impactos-da-ditadura-militar-no-brasil>

Shilov e Silantiev (2014) pesquisaram o trabalho do Professor Alexander Schukarev, formado na Faculdade de Física e Matemática da Universidade de Moscou em 1889, responsável por aperfeiçoar a ideia da Máquina Lógica ou máquina de Jevons, criada para realizar comparações entre objetos e diagramas. Segundo Cestari *et al* (p.23, 2014) :

A máquina de Jevons recebe as premissas na forma de equações lógicas, ou identidades. Somente um número limitado de letras diferentes entram nessas equações – de fato, qualquer tentativa de estender a máquina para além de quatro letras a complicaria intoleravelmente. A máquina tem um teclado, com duas teclas para a forma afirmativa e negativa de cada letra a ser usada no primeiro lado da equação, e duas outras para o segundo lado da equação, havendo quatro vezes mais teclas que letras. Há também uma tecla para o signo de adição lógica ou agregação para cada lado da equação, uma tecla para o signo de igualdade e duas teclas de ponto final, cujas funções não precisam ser explicadas aqui. As teclas são apertadas sucessivamente, na ordem em que letras e signos ocorrem na equação.

O que Schukarev fez em 1913, foi dar dimensões menores e arrumar defeitos estruturais, conectando uma tela ao instrumento, de forma que exibisse os resultados das operações realizadas pela máquina.

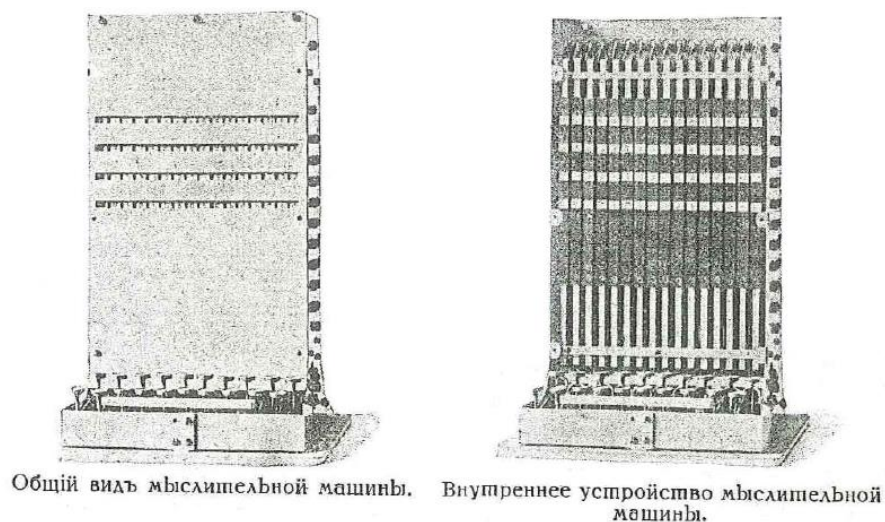


Ilustração 09: Máquina Lógica de Schukarev

Fonte: Reasoning vs. Orthodoxy, or, The Lesson from the Fate of Russian “Reasoning Machine”

Segundo Shilov e Silantiev (2014), o trabalho de Schukarev conseguia exibir resultados lógicos, sem erros humanos. Porém, foi durante a Revolução Russa que a lógica formal entrou radicalmente em revisão, e determinaram que seu trabalho contradizia o materialismo dialético⁴⁴ o que acarretou duras críticas ao seu trabalho.

⁴⁴ Segundo Johnson (1997, p. 140) “ Uma das aplicações mais conhecidas é a teoria de mudança social conhecida como materialismo dialético. Marx associa o materialismo ao conceito de uma dialética- luta entre ideias opostas sobre forças sociais (tese e antítese) - que resulta em uma nova síntese. Marx argumentava que os sistemas sociais mudam através de um processo contínuo, no qual contradições internas socialmente geradas criam tensão, nas sociedades capitalistas industriais e isso acarreta a mudança social.

Além disso, a indiferença política do professor era tratada de forma hostil pelos soviéticos, criando-se uma campanha ideológica contra ele, que acabou se aposentando em 1930. Somente na década de 1960 que os trabalhos do professor foram lembrados. (SHILOV, SILANTIV, 2014)

Entre 1946 e 1947, pouco após o fim da Segunda Guerra Mundial (1945) que os primeiros computadores foram enfim desenvolvidos na Inglaterra e nos Estados Unidos, por cientistas como o inglês Alan Turing, considerado pai da computação moderna. Segundo Almeida (2008, p.30):

O período posterior à Segunda Guerra Mundial, a grande revolução foi protagonizada pelas tecnologias computacionais. Em finais da década de 1940 Norbert Wiener, na época professor de Matemática do MIT - Massachusetts, discute os impactos sociais das possibilidades de transmissão de mensagens e controle à distância, ou seja, a possibilidade de o indivíduo, enquanto informação, estar virtualmente existindo e atuando para além dos limites do corpo físico, através dos meios de comunicação

Mesmo com o desenvolvimento do transistor⁴⁵ na *Bell Laboratories* em 1947 e do circuito integrado⁴⁶ entre 1958/59 - tecnologias que deram base para o desenvolvimento do primeiro microprocessador⁴⁷ em 1971 - entre as décadas de 1950 e 1960, a comunicação *online* e a interação entre computadores e homens ainda eram dificultadas por fatores econômicos, e, por isso, ainda estavam limitadas às universidades e ao Governo, em especial ao Departamento de Defesa.

Licklider e Clark (1962) apontavam grandes vantagens em investir nesta área, principalmente em relação à velocidade no processamento e transmissão de informações que esta tecnologia proporcionava, além de uma relação complementar - uma espécie de simbiose que traria vantagens em diversas áreas, como educação, economia, ciências exatas, ciências da saúde, entre outras.

Também se pensava em formas de melhorar o prazer e a satisfação ao usar o computador e as inúmeras vantagens que esta interação poderia proporcionar. Selecionar hipóteses, relevância de metas e critérios, que são habilidades humanas, aliadas a precisão e a rapidez nos cálculos, na identificação de padrões e de um grande armazenamento de informações que são habilidades do computador (LICKLIDER E CLARK, 1962).

Todo esse processo também trouxe novos debates envolvendo “uma máquina que pensava, mas com carne artificial” (TURING, 1950), nos quais o computador era visto

⁴⁵ Peça responsável pela amplificação do sinal, que também funciona como um controlador que libera ou interrompe uma corrente elétrica. Foi desenvolvido em 1947 pelo laboratório da Bell Telephone.

⁴⁶ CI ou Circuito Integrado incorpora diversos componentes em um chip de silício, conectado por fios condutores e fixados nas placas de um circuito.

⁴⁷ Também definido como *Central Process Unit* (CPU), dispositivo que controla as informações e permite o funcionamento do computador.

espelhando as próprias potencialidades humanas e sua capacidade de armazenar informações. Dessa forma, as máquinas se tornariam gradativamente mais presentes, úteis e acessíveis como uma extensão da própria vida do homem (TURING;1950, MCLUHAN 1964, LICKLIDER,1960).

Como ainda não havia na década de 1950 um curso de ciência computacional, a maioria dos estudos relacionados ao computador estavam voltados à área de engenharia elétrica. O primeiro curso foi oferecido no final dos anos 1950 e membros do TMRC passaram a se dedicar e aprender melhor sobre o computador e, como detalhado no site do MIT *Museum*, alguns destes indivíduos passaram também a testar e ajudar no aperfeiçoamento de equipamentos como o TX-0⁴⁸, desenvolvendo por exemplo, os primeiros *softwares*⁴⁹.

Levy (2012) descreve que havia um fervor raramente visto fora dos mosteiros e tornaram a vanguarda em processo de construção simbiótica entre o homem e a máquina, construindo elementos de uma nova cultura em formação: a Cultura Hacker.

A visão do mosteiro é uma metáfora para o modelo de fonte aberta, na qual pesquisadores divulgam seus trabalhos abertamente para que sejam utilizados livremente, opondo-se ao modelo fechado que só permite pouco ou nenhum acesso às informações, sendo este considerado um modelo ditatorial. Segundo Pekka Himanen (2001, p. 72), esta metáfora do mosteiro é resumida “pela regra de São Basílio, o Grande do século IV: ‘Ninguém precisa se preocupar com o método de administração do superior’. O modelo fechado por outro lado, não permitia iniciativa crítica, atos que poderiam tornar uma atividade mais criativa e autocorretiva”.

Alguns destes *softwares* eram capazes de enviar ruídos a uma caixa de som, outros eram facilitavam o uso da própria máquina, além do desenvolvimento de algo semelhante às atuais plataformas online.⁵⁰ (LICKLIDER E CLARK, 1962; POOLE, 2005)

Autores como Marshall McLuhan já percebiam as possíveis consequências e impactos desta nova tecnologia na própria sociedade ainda na década de 1960. Especialmente na obra “Os Meios de Comunicação como Extensões do Homem” (1964), na qual McLuhan descrevia que a “velocidade elétrica” seria capaz de trazer funções sociais e políticas com uma implosão súbita que intensificaria a consciência de responsabilidade humana.

⁴⁸ Transistorized Experimental Computer Zero

⁴⁹ Programas que comandam o funcionamento de um computador sendo esta sua parte lógica. Se divide em softwares de sistema que se divide em operacionais (como o Windows ou Linux) e utilitários (que executam por exemplo a verificação de disco, acesso à Internet) e os softwares aplicativos (como editores de texto, navegadores)

⁵⁰ Um dos primeiros cursos desenvolvidos foi o de ensino em alemão.

Durante este processo, se alterariam as posições sociais de grupos como os negros, adolescentes e mulheres, de forma que estes não poderiam mais ser mantidos dentro de uma associação limitada, o que faria com que estes grupos e suas lutas estivessem gradativamente mais presentes na vida da sociedade de uma forma mais ampla (MCLUHAN,1964). Ainda segundo o autor, “cada cultura e cada época teriam seu próprio modelo de percepção do conhecimento” e a sociedade no qual ele enxergava vivia uma cultura de repulsa a padrões impostos, acostumados a separar e dividir todas as coisas como meio de controle.

As grandes inovações tecnológicas construídas neste período, em especial nesta relação dos homens com os computadores, viriam futuramente a estar no epicentro de debates políticos e filosóficos no final do Século XX e início do Século XXI.

3.3 Relação do hacker com a informática

Em 1962, Joseph Carl Robnett Licklider, professor associado do MIT desde 1950 e responsável por criar uma comissão que estabeleceu o *Lincoln Laboratory* e diversos outros projetos, se tornou o primeiro diretor da *Information Processing Techniques Office* (IPTO), criado em 1962 como uma divisão da *Advanced Research Projects Agency* (ARPA), fundada em 1958 pelo Departamento de Defesa dos Estados Unidos.

O IPTO esteve envolvido no desenvolvimento de um meio de interação informacional para governos, instituições, corporações e indivíduos, e, segundo Castells (2003, p.13), tinha como principal missão “mobilizar recursos de pesquisa, particularmente no mundo universitário, com o objetivo de alcançar a superioridade tecnológica e militar em relação à União Soviética na esteira do lançamento do primeiro *Sputnik*⁵¹, em 1957”.

Segundo Samuel (2004, p.40), logo no início da década de 1960, começa a surgir uma ideia de associar os *mainframes* de maneira conjunta, pensando em uma estratégia de sobrevivência das comunicações, para o caso de ataques mais sérios, como um ataque nuclear.

Em agosto de 1964, Paul Baran, associado a RAND (*Research and Development*) responsável em desenvolver análises para a Força Aérea e o Departamento de Defesa dos Estados Unidos, apresentou o memorando “*On Distributed Communications*”, propondo uma possível alternativa para essa questão.

51 O primeiro satélite artificial da Terra lançado pela União Soviética em 4 de outubro de 1957

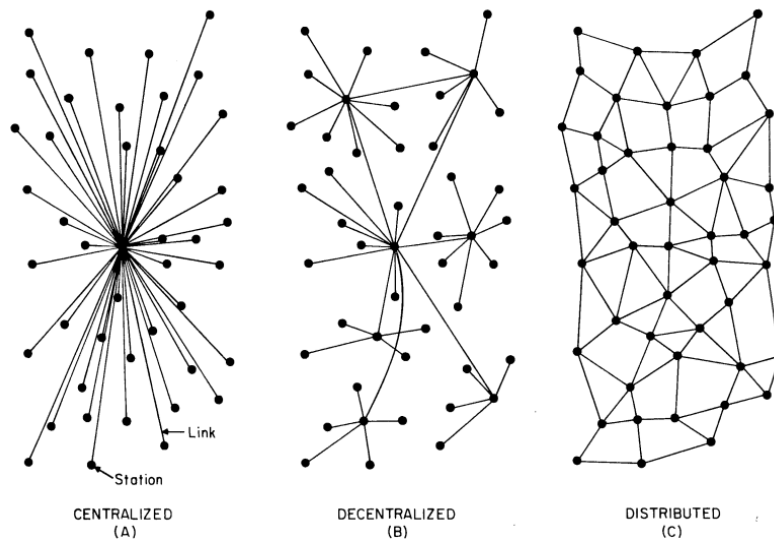


FIG. 1 – Centralized, Decentralized and Distributed Networks

Ilustração 10: Centralized, Descetralized and Distributed Networks

Fonte: *On Distributed Communications*

Baran apresentou três tipos de comunicação, de acordo com a figura 8: a centralizada (A), que concentra em um único ponto a transmissão de uma informação; a distribuída (C), que apresenta um modelo de transmissão sem nenhum comando central; e o sistema descentralizado (B), apontado como melhor opção no caso de um possível ataque, uma vez que não possui apenas um controle central, e, portanto, permitiria que qualquer ponto sobrevivente pudesse reestabelecer a rede, mesmo que houvesse um dano, não prejudicando sua totalidade. (BARAN;1964). Apesar do projeto ter sido inicialmente rejeitado pela AT&T, foi a base da ARPAnet. Seu modelo foi uma grande evolução para a época.

Posteriormente, em 1966, Licklider foi substituído por Robert William Taylor, transferido da NASA e que também estava relacionado ao projeto desde 1965, planejando construir uma rede capaz de interligar/ conectar os projetos da ARPA.

A primeira rede começou a operar em 1969, com o nome de ARPAnet (*Advanced Research Project Agency Network*), nesta época ainda fechada para a população em geral. Segundo Seel (2012) era composta por quatro nós⁵²: SRI (*Stanford Research Institute*), UCLA (*University of California at Los Angeles*), UCSB (*University of California, Santa Barbara*) e UTAH (*University of Utah*) e, logo em 1970, a AT&T instalou um link cruzando o país que operava a uma velocidade de 56kbs. Quando a rede foi criada, esteve focada na experimentação técnica por acadêmicos, cientistas e estudantes (SAMUEL;2004).

⁵² Meio de conexão dos dispositivos de redes

Segundo Castells (2003,p.22), a sorte da história da ARPAnet se deu por um “caso raro de inteligência organizacional, que instituiu a ARPA(*Advanced Research Projects Agency*) como uma agência financiadora e orientadora de pesquisas dotada de uma considerável autonomia”, uma vez que permitiu o envolvimento de cientistas, acadêmicos, seus alunos e amigos em diversos projetos, criando uma rede de contatos com liberdade para produzir inovações tecnológicas, com a qual o próprio governo poderia se beneficiar.

Tais benefícios se efetivaram em 1975, quando o “Departamento de Defesa desenvolveu um interesse político em comercializar a rede e distribuí-la gratuitamente, subsidiando sua adoção por fabricantes de computadores americanos”, como aponta Castells (2003,p.23). Sem recursos, essa liberdade (estratégica) certamente não despertaria interesse ou envolvimento de parte do grupo de cientistas e *hackers* envolvidos nestes projetos.

Porém, segundo Streeter (2010) no final da década de 1960, o entusiasmo do militarismo da Guerra Fria, que anteriormente promovia a “cola” cultural que mantinha o complexo industrial-militar começou a enfraquecer:

Muitos intelectuais de associações universitárias e um número substancial de engenheiros começaram a ser influenciados por correntes ligadas a contracultura. Boa parte da história da computação faz referência aos sintomas desta relação: programadores da Arpanet que calçavam tênis e usavam broches antiguerra com seu estilo contracultural ajudaram a mudar o centro de gravidade nas visões dominantes do que os computadores eram, como eles poderiam ser construídos e utilizados.

Mungo (1993) aponta que empresas e organizações passaram a controlar os dados e limitar o acesso de pessoas que pudessem ter acesso aos seus sistemas. Este é um período que segundo o autor, idealistas da cena hacker passaram a questionar sobre o poder da informação e que uma revolução por meio dos computadores seria bem-sucedida quando dados de todas as pesquisas disponíveis estivessem acessíveis para qualquer pessoa.

Os reflexos dessa mudança podem ser demonstrados quando Licklider voltou ao IPTO em 1974 e o governo não estaria mais de acordo com suas visões de futuro. Poole (2005) afirma que ele percebeu que havia se instalado uma cultura muito diferente daquela que havia presenciado há cerca de dez anos, baseada em uma total liberdade em explorar e uma computação em plena fase de crescimento. Ele teria percebido que eles estavam bem mais burocráticos e em busca de mais resultados do que de ideias.

Este foi também um período de mudança significativa na postura do próprio *hacker* em especial em relação à Guerra do Vietnã, sob grande influência dos movimentos de contracultura do final da década de 1960, pois eles passaram a questionar a maneira com a qual a tecnologia que eles ajudaram a desenvolver estava sendo utilizada de uma forma negativa. (STREETER,2010; MUNGO,1993; TURNER,2006)

Foi justamente na década de 1960 que valores tais como a Ética Hacker e a relação com o tempo⁵³ começaram a ser mais claramente construídos. (HIMANEN;2001)

Acreditamos que acima de tudo, a Ética Hacker deve ser vista como um jogo de disputas e jogos de poder desenvolvidas pelos primeiros hackers em tentativas de legitimar seu discurso dentro da sociedade.

Do ponto de vista de Levy (2001, p.34) teria sido nesta estrutura que gradativamente foi pensado um sistema descentralizado que desconfiava da autoridade, nele graças a troca de informações livres seria possível não limitar as habilidades de um programador: “A última coisa que se precisa é uma burocracia”, pois as Instituições são consideradas sistemas falhos, que limitam o livre acesso à informação.

Para Castells (2003):

Os hackers e sua cultura são as fontes essenciais da invenção e contínuo desenvolvimento da Internet. Os hackers não são o que os meios de comunicação e os governos dizem que são. São, simplesmente pessoas com conhecimento técnico informático cuja paixão é inventar programas e devolver novas formas de processamento de informação e comunicação eletrônica (Levy, 2012, Raymond 1999). Para eles, o valor supremo é a inovação tecnológica da informática. E, portanto, necessitam também de liberdade. Liberdade de acesso aos códigos fonte, liberdade de acesso à rede, liberdade de comunicação com outros hackers, espírito de colaboração e de generosidade (colocar à disposição da comunidade de hackers tudo o que eles sabem, e em reciprocidade receber o mesmo tratamento de qualquer colega).

Faz parte do perfil de um *hacker* querer consertar algo que está quebrado e precisa ser melhorado. Toda a informação produzida deveria ser livre pois, se não há acesso a uma informação, como você poderá corrigi-la? (LEVY;2012)

Segundo Himanem (2001, p.72):

Tanto cientistas quanto hackers aprenderam na prática que a ausência de estruturas fortes é uma das razões que torna esse modelo tão poderoso. Os hackers e os cientistas só têm de concretizar suas paixões e trabalhar em grupo com outros indivíduos com quem as compartilham. Esse espírito se difere claramente do espírito encontrado em empresas e governos. Nos órgãos do governo, a ideia de autoridade subsiste muito mais forte que em empresas. Para os hackers o método típico utilizado pelo governo para realizar intermináveis reuniões, organizar incontáveis comitês, minutar estratégias enfadonhas, etc. É no mínimo um sofrimento tão grande quanto fazer propaganda para justificar uma ideia antes de começar a cria-la. (Cientistas e hackers também irritados quando as universidades são transformadas em uma burocracia governamental ou em um mosteiro)

Enquanto Mattos (2014) aponta:

Coleman e Golub (2008) ressaltam o fato de o que significa ser livre e o que é liberdade constitui um discurso moral para hackers em distintos contextos e práticas, através da relevância de questões de comprometimentos liberais como oportunidades igualitárias, meritocracia, autonomia individual, tolerância e proteção das liberdades civis.

⁵³ Pekka Himanen afirma que a relação que o hacker faz com o tempo é diferente da lógica da ética protestante. Para o hacker o tempo é flexível (eles precisam de liberdade para organizar seu próprio tempo) e a lógica de “Tempo é dinheiro” é substituída por “tempo é vida”.

A década de 1970 é compreendida como o período da revolução da tecnologia da informação, que possibilitou a criação dos primeiros microcomputadores⁵⁴ e sua consequente produção em massa, que integrou a tecnologia dos microchips nos computadores domésticos e nos videogames (CASTELLS,2011).

3.4 “Eles são uma Legião”: os hackers de hardware⁵⁵

Os limites institucionais, aos quais os *hackers* estavam inseridos, estavam prestes a serem definitivamente rompidos, quando os primeiros computadores pessoais e videogames foram produzidos graças ao desenvolvimento do microprocessador.

Segundo Malone (2014), em abril de 1969, a companhia japonesa Busicom contratou a recém-criada empresa *Intel*⁵⁶ para desenvolver um *chip* de baixo custo para suas calculadoras⁵⁷, investindo cerca de US\$ 60.000 no projeto.

O resultado do trabalho foi apresentado em março de 1971, porém a Busicom entrou em dificuldades financeiras e a Intel conseguiu os direitos para comercializar o produto e ampliar sua aplicabilidade (MALONE,2014). Em 15 de novembro de 1971 anunciou na revista *Electronic News* o lançamento do 4004, seu primeiro microprocessador que media 3,2 mm, sendo capaz de executar cerca de 60 mil operações por segundo⁵⁸.

⁵⁴ Termo técnico utilizado anteriormente. Atualmente utiliza-se computador pessoal ou PC (Personal Computer)

⁵⁵ Parte física da máquina

⁵⁶ Fundada em julho de 1968 por Gordon E. Moore e Robert W. Noyce com o nome de NM Eletronics modular posteriormente mudou o nome para INTEL (Integrated Eletronics).

⁵⁷ A ideia de Tadashi Sasaki, um executivo para *Sharp Corporation* outro grande fabricante de calculadoras eletrônicas da época, que dava assistência técnica a Busicom deu a ideia de colocar um computador em um único chip (MALONE;2014)

⁵⁸ Os atuais modelos executam até 4 bilhões de operações por segundo.

Announcing a new era of integrated electronics

A microprogrammable computer on a chip!

Intel introduces an integrated CPU complete with a 4-bit parallel adder, sixteen 4-bit registers, an accumulator and a push-down stack on one chip. It's one of a family of four new ICs which comprise the MCS-4 micro computer system—the first system to bring you the power and flexibility of a dedicated general-purpose computer at low cost in as few as two dual in-line packages.

MCS-4 systems provide complete computing and control functions for test systems, data terminals, billing machines, measuring systems, numeric control systems and process control systems.

The heart of any MCS-4 system is a Type 4004 CPU, which includes a powerful set of 45 instructions. Adding one or more Type 4001 ROMs for program storage and data tables gives you a fully functioning micro-programmed computer. To this you may add Type 4002 RAMs for read-write memory and Type 4003 registers to expand the output ports.

Using no circuitry other than ICs from this family of four, you can create a system with 4096 8-bit bytes of ROM storage and 5120 bits of RAM storage. When you require rapid turn-around or need only a few systems, Intel's erasable and reprogrammable ROM, Type 1701, may be substituted for the Type 4001 mask-programmed ROM.

MCS-4 systems interface easily with switches, keyboards, displays, teletypewriters, printers, readers, A-D converters and other popular peripherals.

The MCS-4 family is now in stock at Intel's Santa Clara headquarters and at our marketing headquarters in Europe and Japan. In the U.S., contact your local Intel representative for technical information and literature. In Europe, contact Intel at Avenue Louise 216, B 1050 Brussels, Belgium. Phone 492033. In Japan, contact Intel Japan, Inc., Parkside Flat Bldg. No. 4-2-2, Sendagaya, Shibuya-Ku, Tokyo 151. Phone 03-403-4747.

Intel Corporation now produces micro computers, memory devices and memory systems at 3065 Bowers Avenue, Santa Clara, Calif. 95051. Phone (408) 246-7301.

intel delivers.

Ilustração 11 : A microprogrammable computer on a chip
Fonte: Eletronic News (15 de novembro de 1971)

Este foi o primeiro dos três modelos⁵⁹, considerado o cérebro do computador, que permitiu a Intel ser líder no mercado nos 40 anos posteriores (MALONE;2014). Do ponto de vista de Lévy (1999, p.31):

O desenvolvimento e a comercialização do microprocessador (unidade de cálculo aritmético e lógico localizada em um pequeno chip eletrônico) dispararam diversos processos econômicos e sociais de grande amplitude. Eles abriram uma nova fase na automação da produção industrial: robótica, linhas de produção flexíveis, máquinas industriais com controles digitais, etc.”

Um computador com um preço mais acessível fez com que o Governos e Escolas de países como Alemanha, Holanda e Reino Unido investissem na inserção de tal tecnologia na sociedade, o que levou a um aumento do interesse de principalmente de jovens nesta área, e consequente ao meio hacker.

Tal como aconteceu com o *phreaking*, a publicação de uma matéria chamada “*Fanatic Life and Symbolic Death Among the Computer Bums*” em uma revista de grande circulação, neste caso, a Rolling Stone de 7 de dezembro de 1972, trouxe à tona uma comunidade que se desenvolvia desde o fim da Segunda Guerra Mundial, com forte relação com phreakers e *hackers* de telefonia.

A matéria de Stewart Brand falava abertamente quem eram os *hackers* e a inovação que estava por vir em relação aos computadores, os descrevendo como pessoas que viviam uma

⁵⁹ Os seguintes foram o 8008 (lançado em 1972) e o 8080 (de 1974).

relação de amor e ódio pelo computador, em que eles eram os técnicos desta ciência. Brand, descreve que:

Eles eram as pessoas responsáveis em transformar as necessidades humanas em códigos, que as máquinas fossem capazes de entender e agir. “Eles são uma legião”. Fanáticos com um brinquedo novo. Uma elite recém-descoberta, com o seu próprio aparato, linguagem e caráter, suas próprias lendas e humor. Aqueles homens magníficos com suas máquinas voadoras (...) onde as regras não são decreto ou rotina tanto como as demandas mais marcantes do que é possível. Uma ciência jovem viaja para onde o jovem a leva. Os mais sábios diretores de pesquisas de computação aprenderam que não confiando em seus jovens programadores com grande responsabilidade, pode levar imediatamente a pesquisa para lugar nenhum. (...) Para Les Earnest: “Às vezes é difícil dizer a diferença entre lazer e trabalho. Nós tentamos julgar as pessoas não por quanto tempo elas perdem, mas sobre o que elas realizam em longos períodos de tempo (...)”

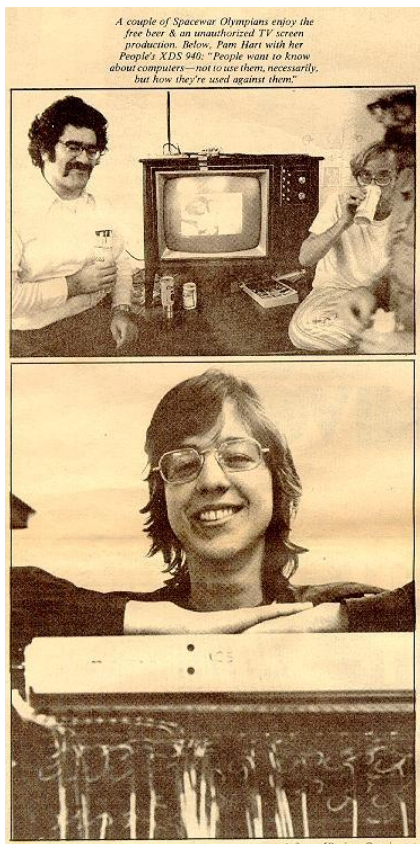


Ilustração 12: Fragmento da Rolling Stone (1972)
Fonte: Rolling Stone

Em 1976, o professor de ciência da computação do MIT chamado Joseph Weizenbaum publicou o livro “O Poder do Computador e a Razão Humana”, sendo o primeiro que associou abertamente o hacker à programação, criando o primeiro estereótipo e os definindo como programadores compulsivos com “seus braços tensos que esperam para disparar seus dedos, já prontos para atacar” (WEIZENBAUM,1976;ALBERTS e OLDENZIEL,2014; LEVY, 2012)

Levy (2012 p.123) aponta que a visão de Weizenbaum (que sequer convivia com frequência com os estudantes) trazia uma visão desumanizadora e irracional para os hackers citando um trecho da obra do autor:

Jovens homens brilhantes com aparência desgredada, sempre com olhos fundos e febris, podem ser vistos sentados, podem ser vistos sentados no console dos computadores; os braços tensos esperando para disparar seus dedos, já prontos para a guerra sobre teclas e botões nos quais sua atenção parece estar concentrada como jogador nos dados que rolam. Quando não estão magnetizados, eles se sentam à mesa diante das folhas de impressão do computador sobre as quais trabalham arduamente como se estivessem estudando textos cabalísticos. Trabalham até cair vinte, trinta horas de uma vez. A comida, quando se lembram de pedir, é levada até eles: café, refrigerantes e sanduíches. Se possível dormem em catres perto das máquinas. As roupas amarrotadas, o rosto sujo e barbudo, cabelo despenteado são todos testemunhas que eles esqueceram de seus corpos e do mundo em que vivem. Eles são os vagabundos da computação, os programadores compulsivos

A descrição feita por ele rapidamente trouxe a reação de membros da própria equipe, que sentiram ofendidos com a descrição feita por Weizenbaum.

Por essa razão, a estratégia e visão do professor Licklider foi compreendida tão bem por sua equipe. Foi dando liberdade, valorizando seus membros por suas habilidades⁶⁰, com pouca burocracia e recursos livres que o levou a obter resultados tão positivos.

Foi uma lógica que se construiu desde a década de 1960 e segundo Himanen (2001, p.30) e é bem semelhante a uma ética pré-protestante:

“(...) pode-se dizer que para os *hackers* o objetivo da vida está mais próximo do domingo do que de sexta-feira. Contudo, vale notar que a ética protestante não é, em última análise, igual a ética pré-protestante, cuja ideia de paraíso é viver no ócio. Os *hackers* desejam tornar concretas as suas paixões, e estão prontos a admitir que a busca por tarefas ainda mais interessantes talvez não seja assim tão fácil. Para os hackers, paixão descreve de forma geral o teor de suas atividades, embora sua realização não seja totalmente um jogo divertido em todos os seus aspectos.”

Ambientes colaborativos, “livres” e dinâmicos podem ser vistos ainda hoje em empresas do Vale do Silício, como o Google.

Entretanto, segundo Himanen (2001, p.73) “a relativa falta de estruturas não significa que elas não existam. A despeito do aparente caos, o hackerismo não sobrevive num estado de anarquia, nem a ciência. O projeto dos hackers tem pessoas que os guiam”, porém, suas pesquisas são abertas para qualquer pessoa dentro ou fora destes ambientes. Assim, os princípios destes hackers, tais como sua ética, teriam sido absorvidos e em alguns casos ampliados por grupos fora do meio acadêmico.

A ética foi descrita por Steven Levy em 1983 e seria um tipo de marcador que permite compreender os limites das atividades de um hacker e o que os diferencia de um criminoso: a forma com que ele utiliza os dados e informações que conseguem acessar. Associações como

⁶⁰ Segundo Himanen (2001, p.47) os hackers sempre respeitam o indivíduo, sempre se mostram contra o autoritarismo.

o *Chaos Computer Club* (CCC) fundado em 1981 na Alemanha ou o Laboratório Hacker do Senado Federal do governo Brasileiro, partilham princípios da ética descrita por Steven Levy (2012, p.27):

“Acesso a computadores e qualquer coisa que possa ensinar algo sobre a maneira ao qual mundo funciona, deve ser ilimitado e total.
 Todas as informações devem ser livres.
 Desconfie da autoridade- promova a descentralização.
 Hackers devem ser julgados pelo que eles fazem e não de acordo com critérios como graus, idade, raça, sexo ou condição social.
 Pode-se criar uma arte e beleza com o computador.⁶¹
 Os computadores podem mudar sua vida para melhor”

Alguns grupos que seguem perfis cyberpunks ou cypherpunks, que serão melhor descritos mais adiante, ainda partilham:

“Não roube os dados de outras pessoas
 Não ‘bagunce’ dados alheios
 Disponibilize dados públicos, proteja dados privados”

Atualmente, entidades como a *International Council of E-Commerce Consultants* (EC-Council) concedem certificado de hacking ético, compreendido segundo o site da entidade, como “pessoas que testam a segurança de redes e sistemas de computadores buscando vulnerabilidades e brechas com intuito de informar a falha às empresas, para que sejam reparados.”

Quanto mais o hacker, ou grupo, se aproxima desta construção histórica (seja por pesquisa ou contatos) e absorve esta filosofia mais ele tende a ser ético. Uma das primeiras informações de que a Ética partilhada por hackers estava sendo desenvolvida também fora do meio acadêmico, foi de um grupo britânico fundado por volta de 1975, chamado CRANK.

Segundo Mungo (1993) o “Capitão Crunch” teria sido o responsável por inserir a prática do *phreaking* na Grã-Bretanha em 1970, durante uma viagem para a região. Os sistemas de telefonia britânicos eram diferentes dos americanos e utilizavam uma frequência diferente (de 2280Hz), e a *Blue-Box* teve que ser adaptada, o que o levou a realizar o “*phreak* mais audacioso na Inglaterra.” Mas o interesse dos britânicos na prática rapidamente diminuiu, quando os computadores pessoais se tornaram disponíveis.

O grupo fez parte da primeira geração a aproveitar a revolução tecnológica que teve lugar em 1960 e 1970: todos tinham aprendido sobre computadores na escola, tendo beneficiado de uma súbita consciência de que a alfabetização computador era importante, não apenas uma especialidade secreta reservada para amadores e engenheiros. (MUNGO,1993 p..29)

Os boletins do *Computer Fraud & Security Bulletin*, entre 1980 e 1983, descreveram e analisaram um dos primeiros grupos de hackers que se tem notícia: o CRANK, com cerca de 20 membros que incluíam funcionários da indústria da computação e estudantes de escolas.

⁶¹ Um código de programação é visto como expressão de arte.

O grupo buscava identificar *bugs* (erros) dentro de sistemas operacionais e falhas nos sistemas de segurança dos computadores, conseguindo acesso a arquivos protegidos com senhas. O CRANK buscava arquivos dentro de empresas de Londres que “afirmavam que a segurança não poderia ser quebrada”. Eles garantiam que não tentavam nada malicioso, como deletar ou alterar arquivos que conseguiam acessar.

O meio utilizado por eles para descobrir as senhas não era “nada esotérico”, na verdade, eles descrevem que as senhas eram realmente óbvias, com nomes de personagens da ficção ou sequencias pouco originais. Para o grupo, os sistemas poderiam ser penetrados por qualquer pessoa com habilidades técnicas, pois as linhas ou transmissões de telefone e satélites geralmente são abertas para que dados sejam transmitidos.

Do ponto de vista de Sterling (1993) "os verdadeiros *hackers* podem precisar 'quebrar' sistemas de computadores particulares para saciar sua sede de conhecimento. Mas suas explorações intelectuais são inofensivas”, argumenta ele, e “não devem incidir em sanções penais”.

Outro grupo é descrito em um importante documentário de Ine Poppe (2001), mas estes já no final da década de 1980, os “*Hippies from Hell*” na Holanda.

Eles produziram uma *hackermagazine*⁶² chamada *HackTic*, que teria gerado os primeiros fóruns de discussão online. Já sendo consideradas piratarias *Old School* de sistemas de telefonia (*phreaking*), tiveram papel vital para que a Internet não ficasse nas mãos de grandes empresas e corporações, já que a rede começou a parecer muito interessante para o grupo e não poderia ficar limitada apenas às universidades. O princípio do *hacking* para os *Hippies* era muito simples: basicamente era encontrar soluções para um sistema que não funcionava.

Poppe, mãe de um destes *hackers* (Zoro), mostra as rotinas do grupo: frequentes relatos da chatice da vida escolar, uma visão comum entre pessoas desse meio, chamando atenção no documentário as variadas habilidades técnicas de cada um dos hackers, e como eles sentiam que eram ignoradas por seus professores.

Eles aplicam princípios básicos de suas rotinas, no computador, como por exemplo, um campeonato de abrir cadeados, “estamos interessados em segurança e como você pode se

⁶² Uma das primeiras *hackermagazines* identificadas no Brasil, trata-se da “Barata Elétrica” iniciada em 1994 após o congresso “*Hackers and Virus Writers Congress*” na Argentina no mesmo ano, como uma tentativa de informar e transmitir conhecimentos a outros interessados pelo assunto. A transmissão da cultura hacker no Brasil permaneceu limitada a grupos fechados por um longo período e atualmente, existem iniciativas como o “Ônibus Hacker” descrito como um laboratório sobre quatro rodas que visa ocupar espaços e compartilhar conhecimento, o tema é abordado por Guilherme Flynn Paciornik no trabalho “Movimentos sociais e as novas Tecnologias da Informação e Comunicação: um estudo de caso na zona sul da cidade de São Paulo, a Casa dos Meninos”

defender de uma forma não usual” relata Walter Bergers “e isso se aplica aos computadores e cadeados: em computador é chamado *hacking*”.

Mathide Mupe, do “*Hippies from Hell*”, relata que o *hardware hackeado* existe, “pois os eletrônicos vinham sem manual e se você deseja fazer algo com a máquina, ou tentar fazê-la funcionar você precisa quebrar o código e reiniciar o sistema, como as empresas eram contra isso, chamavam de hackear”, já que modificavam o sistema original.

O grupo se dedicava em criptografia⁶³, em quebrar códigos de segurança para que outras pessoas que não tinham o mesmo conhecimento técnico pudessem utiliza-los livremente, algo depois compreendido como *cracking*⁶⁴. Eles possuíam listas de contatos para troca de informações que deram origem aos fóruns *online*, além de realizar um dos primeiros encontros presenciais de *hackers* (comuns na Europa, como acampamentos organizados pelo CCC).

Esta nova demanda de usuários, que utilizavam o computador para finalidades diferentes, causou confusão dentro da própria comunidade e dificuldade de compreensão para a população em geral, que não percebia como *hackers* eram diferentes em suas individualidades e posturas, além de serem um reflexo da própria sociedade ao seu redor, de uma maneira reativa. “Os sistemas tecnológicos são socialmente produzidos. A produção social é estruturada culturalmente. A Internet não é exceção. A cultura dos produtores da Internet moldou esse meio. Estes produtores foram, ao mesmo tempo, seus primeiros usuários” (CASTELLS, 2003, p.34)

Na década de 1980, com tal tecnologia cada vez mais presente na realidade de uma parcela maior da população, temáticas envolvendo *hackers* passaram a se tornar gradualmente mais importantes, uma vez que para que ocorra um processo de integração na sociedade é necessário que faça sentido na vida das pessoas (STREETER,2011).

Parte significativa dos trabalhos da década de 1980, trabalham com a “Cultura Hacker” dentro de uma perspectiva de uma subcultura estadunidense, buscamos compreender como teria sido o início da cena *hacker* no Brasil seus desafios e dificuldades.

⁶³ Criptografia, do grego “*Kryptós*” e “*gráphein*”, que significa “oculto” e “escrever”. Consiste de um conjunto de regras que codificam uma informação, em que somente o emissor e o receptor conseguem ler, protegendo dados sigilosos e comunicações.

⁶⁴ O Cracker é alguém definido como aquele que “viola a segurança de um sistema” e tiveram sua ascensão na década de 1980. Boa parte da explosão de ocorrências policiais, foram envolvendo crackers, não hackers. Como aponta Castells (2003, p.46) “A Cultura Hacker vê o cracker com muita apreensão, uma vez que denigrem toda a comunidade com uma perspectiva analítica, amplificada pela mídia”. Samuel (2004, p.15) aponta, no entanto a incidência anos adiante do craqueamento político, “o craqueamento político é conduzido por hacktivistas por meio de um ativismo de programação hacker e consiste em formas de hacktivismo dentro de uma orientação “fora da lei” (como defacements, DDoS, etc.)”

Uma vez que os trabalhos sociológicos voltados a esta temática são escassos em nosso país, seguimos uma estratégia investigativa de procurar vestígios da origem e dos desafios encontrados para inserir a cena hacker e o indivíduo ciberpunk no Brasil na década de 1980, por meio de jornais e revistas da época.

Nosso objetivo é oferecer uma pequena base desta temática para estudos futuros, mostrando que o Brasil não foi alheio ao que acontecia em outros países, mas possuía limitações em função do valor dos computadores pessoais.

3.5 O hacker brasileiro da década de 1980

O início da cena hacker que se desenvolvia no Brasil na década de 1980 era bem diferente daquela que eventualmente temos conhecimento (em países como Estados Unidos). No Brasil, a comunidade hacker era mais fechada e limitada a empresas, universidades e pessoas com maior poder aquisitivo.

Durante esta pesquisa inicial, percebemos que boa parte das informações colhidas apontavam que a cena hacker esteve mais concentrada na região de São Paulo, apesar de estimativas que apontavam cerca de 10.000 computadores pessoais espalhados pelo país.

As barreiras e limitações técnicas eram muitas, como uma das consequências da PNI (Política Nacional de Informática), que atingia diretamente o valor e qualidade dos equipamentos comercializados no país. No entanto, tais limitações não impediram que houvessem discussões extremamente avançadas em relação a criptografia, segurança e Ética hacker.

O interesse por estes temas, iniciados por volta de 1981, estava em uma preocupação de que crianças e jovens acabassem cometendo algum tipo de transgressão em nome de sua própria curiosidade e desafio.

Pensava-se no desenvolvimento de manuais que facilitassem o uso destes equipamentos, em publicação e tradução de obras de interesses característicos desta comunidade, não apenas em relação à parte tecnológica, mas nas obras no estilo *cyberpunk*, uma subdivisão das obras de ficção científica. Além disso, havia um interesse em ocupar um nicho do mercado editorial em expansão neste gênero durante a década de 1980 e empregar estes jovens hackers para que eles pudessem eventualmente publicar livros sobre suas realizações, além de difundir o conhecimento e a necessidade em torno da Ética hacker. Dessa forma, compreendendo que as

transgressões seriam fruto de um desequilíbrio social de jovens dentro de uma sociedade que não conseguia acompanhar seu ritmo. Assim, foi fundada a Editora Aleph.

No decorrer desta parte do trabalho, poderemos acompanhar algumas das peculiaridades dos primeiros hackers brasileiros, a partir de matérias em revistas e jornais que buscavam dar um sentido e construir uma cena hacker no Brasil, mostrando que, apesar de suas limitações de ordem técnica, o país fazia parte de um cenário que se desenvolvia em diversas regiões de todo o mundo.

3.5.1 Desafios para inserir a cena hacker no Brasil

No Brasil, as primeiras informações sobre *hackers* começaram a chegar através de matérias em revistas especializadas e jornais. Parte deste interesse esteve atrelado ao aumento da comercialização dos computadores pessoais, iniciadas no final da década de 1970.

No entanto, o desenvolvimento desta comunidade no Brasil foi dificultado pelo alto custo dos equipamentos, que fazia com que uma parcela significativa da população não fosse atingida pelos benefícios que esta tecnologia poderia eventualmente proporcionar.

Deve -se levar em consideração dois fatos: o primeiro é que enquanto ocorria o início do período da revolução da tecnologia da informação (CASTELLS,2003), o país ainda estava vivenciado a Ditadura Militar (1964–1985). A Empresa Brasileira de Telecomunicações (Embratel) foi fundada em 1965, visando a implementação de uma rede nacional que passasse a gerir o setor, anteriormente controlado por empresas privadas nacionais e internacionais que prestavam serviços no país. O principal objetivo dos militares estava na necessidade de criar uma boa infraestrutura que pudesse garantir a segurança e a integração nacional (CARVALHO; 2006).

O segundo fato – e talvez o mais agravante – é que, em 29 de outubro de 1984, foi implementado o PNI (Política Nacional de Informática ou Lei 7.232/84), que tinha como principal objetivo desenvolver a indústria de informática no Brasil, disponibilizando uma reserva de mercado. Essa medida impedia legalmente o acesso de empresas do exterior tal como a importação de certos produtos, visando o investimento e desenvolvimento da indústria nacional.

Além disso, também forçavam a aquisição de equipamentos obsoletos, de qualidade inferior e de altos custo pelos consumidores deste período, outro grande obstáculo para o desenvolvimento de uma Cultura Hacker no Brasil.

Como afirma Castells (2003, p. 45)

É precisamente em situações de pobreza extrema, quando não tem acesso a nenhum recurso, que as pessoas criativas são obrigadas a inventar suas próprias soluções, e elas o fazem” (...) Mas o que é comum à cultura hacker, em todos os contextos sociais, é a premência de reinventar maneiras de se comunicar com computadores e por meio deles, construindo um sistema simbiótico de pessoas e computadores em interação na Internet. A cultura hacker é, em essência, uma cultura de convergência entre seres humanos e suas máquinas num processo de interação liberta. É uma cultura de criatividade intelectual fundada na liberdade, na cooperação, na reciprocidade e na informalidade.

Uma vez que o preço dos computadores era muito alto, boa parte desta tecnologia ficou voltada para o governo, universidades, empresas (modelo fechado) e uma parcela da população com alto poder aquisitivo, tanto para comprar estes equipamentos, quanto para pagar cursos nesta área.

Segundo Toussaint e Madrid (1992) o desenvolvimento e uso de *hardwares* e *softwares* se tornaram muito importantes em países como o Brasil, México, Chile, Argentina e Peru. Mesmo que o grau de extensão varie entre cada país, os autores não deixam de ressaltar os impactos da desigualdade, da falta de infraestrutura, de condições econômicas e sociais que também afetam diretamente tal desenvolvimento e investimento em pesquisas.

Os autores apontam que, segundo Rafael Roncagliolo, 17 países possuíam centros de investigação, inovação e formação de telecomunicações com “um esforço paralelo está sendo feito em alguns países, particularmente no Brasil e Cuba.” Assim: “Uma conclusão é clara: se as mudanças tecnológicas tendem a mudar radicalmente o horizonte da vida política, é lógico que é por meio da política que é possível acompanhar o significado destas inovações e onde as decisões são tomadas” (Mattelart e Schmucler;1983 *in* Toussaint e Madrid ;1992).

Em 1983, como anteriormente dito, foi lançado o filme *WarGames* (Jogos de Guerra), que despertou o interesse principalmente da imprensa para compreender o meio hacker. Foi justamente em agosto de 1983, que o Jornal O Globo divulgou uma matéria falando sobre um dos primeiros encontros presenciais de *hackers* Holandeses, reunindo palestrantes como John Draper e representantes da Alemanha Ocidental. A matéria indica que um dos principais impactos do lançamento do filme foi uma série de investigações e prisões, o que levou ao afastamento do público em geral do evento, e atraiu diversos policiais.

Em setembro do mesmo ano, a Folha de São Paulo publicou o artigo “Os Robin Hoods da era Eletrônica”, descrevendo superficialmente como “brincadeiras” de adolescentes nos Estados Unidos, haviam se tornado uma subcultura no país, apontando a proliferação de estudos psicológicos em torno do aumento de jovens envolvidos nesta prática.

Se por um lado, a matéria da Folha mostrava a preocupação de empresas e do próprio governo estadunidense, que ordenou uma “investigação de alto nível sobre a segurança de

computadores em instalações militares e de inteligência” contra os “*hackers*”, por outro, expressa o fato de um profundo debate que começava a se desenvolver em torno de temas como segurança e privacidade, após a invasão de 60 computadores de grande porte nos Estados Unidos e no Canadá e expõe o que o posicionamento dos *hackers*:

“(...) os dados eletrônicos em um computador não podem ser encarados como propriedade privada - são informações de domínio público. Para as empresas do capitalismo isto é obviamente um escândalo. Muitas, porém, com medo de mostrar sua vulnerabilidade, recusam-se a tornar públicos os casos de interferências em seus sistemas, especialmente em Instituições financeiras” (FOLHA;1983)

Mas foi em 1984, visando um mercado em expansão no Brasil na venda de títulos relacionados à área de computação, que foi aberta a Editora Urânia. Havia segundo um artigo de Mauricio Bonas “Nos livros todo o charme da tecnologia” da Folha de São Paulo de 1984, cerca de 300 títulos relacionados ao setor de informática, equivalendo a 1 milhão de exemplares vendidos e em plena expansão, atendendo por volta de 300.000 usuários de microcomputadores no Brasil.

O professor Pieluigi Piazzzi (1943-2013), um dos fundadores da Urânia, lamentava que o “lançamento de novos computadores antes que tivesse algum tipo de literatura sobre eles, impedindo a total utilização de suas potencialidades”, alegando ainda a falta de títulos nacionais, criticando pesquisadores brasileiros que se recusavam a transmitir seus conhecimentos, afirmando que apesar de serem lançados em média 10 títulos sobre o tema por ano, não tinham qualidade suficiente, apenas se aproveitando de uma demanda existente no setor.

Paulo Brito, também nesta mesma edição da Folha, retrata a dificuldade de encontrar livros que tivessem uma linguagem mais simples, menos técnica e mais didática, isto é, que de fato ensinassem as pessoas a usar um computador.

O Brasil sofreu uma grande falha no setor de pesquisas durante o período da Ditadura Militar, o que fez com que o país não produzisse, nem participasse ativamente do processo de criação e aperfeiçoamento desta tecnologia (informática) durante este período, mas apenas a consumisse, mesmo que de forma limitada, utilizando e tentando compreendê-la a partir dos manuais que vinham acompanhados com as máquinas e investindo pouco a consciência de que a alfabetização computacional era importante, como ocorria em outros países.

Por fim, João Clodomiro do Carmo (FOLHA,1984) faz uma dura crítica aos intelectuais e aos jornalistas brasileiros que insistiam em ignorar a temática da informática e as profundas mudanças que poderiam ocorrer até o fim do século XX em função deste setor. Segundo ele, muitos destes profissionais queriam apenas preservar seus próprios empregos.

Carmo (FOLHA,1984) indica títulos como “Adeus Proletariado” de André Gorz, para entender como o capitalismo eventualmente iria se organizar uma vez que as fábricas

estivessem cada vez mais automatizadas, reduzindo a mão de obra especializada e aumentando o tempo ocioso dos operários, e como a massa iria se contentar em ficar mais tempo em frente da Televisão. O autor alertava para a necessidade de se compreender como a tecnologia poderia ser utilizada para o benefício da sociedade e, como dilema latino-americano, compreender o “novo colonialismo tecnológico” garantindo a “independência de setores mais avançados da tecnologia capitalista” apontando a obra “*América Latina en la encruijada telemática*” de Héctor Schmucler.

A maioria das notícias sobre *hackers* que saíram no Brasil foi a partir de 1985, envolvendo notícias negativas em torno desta temática, reforçando um perfil de uma subcultura estadunidense (que envolvia jovens entre 13 a 17 anos e de classe média), distorcendo sua imagem como se fosse criminoso, sem levar em consideração toda a sua diversidade. Mas certamente, essa geração modificou e ampliou ainda mais o conceito do *hacker* em si.

Em uma notícia de 19 de julho de 1985, no jornal O Globo, “Gang do computador é formada por mais de 600 adolescentes”, descreve casos de *phreaking* e *cracking* como se fossem *hacking* e afirma que muitos jovens que começavam a descobrir os “segredos da computação” seriam desafiados por outros para “um feito marcante”:

É uma nova e estranha cultura, uma espécie de rito de iniciação entre jovens com mentalidade tecnológica (...) acrescentando que o recente filme Jogos de Guerra, em que um jovem quase prova uma guerra atômica ao entrar num computador do Pentágono, reflete as aventuras dessas ‘gangs eletrônicas’

Logo na metade da década de 1980, houve a necessidade de explicitar de maneira clara a “Ética Hacker”, a qual muitos hackers seguem⁶⁵, em uma tentativa de diferencia-los, por exemplo, dos crackers⁶⁶, por isso o trabalho de Steven Levy *Hackers: Heroes of the Computer*

⁶⁵ Porém não é incomum encontrar indivíduos que participam de mais de um grupo ou coletivo, e geralmente seguem regras ou condições internas, as quais os membros se comprometem.

⁶⁶ O termo cracker ganhou força, na metade da década de 1980 começaram a se declarar *hackers*, a exemplo do grupo *Legion of Doom*, fundado em 1984. Um dos membros do grupo, chamado Loyd Blankenship (conhecido como *The Mentor*), publicou, após sua detenção em 8 de janeiro de 1986, o “Manifesto *Hacker*”, ou “A consciência de um *hacker*”. Nele, *The Mentor* desenha o perfil das motivações que levam uma pessoa (em especial um jovem) a ser um *hacker*. Segundo ele, trata-se de pessoas dotadas de grande conhecimento que são frequentemente desprezadas: “(...) meu mundo começa na escola... Eu sou mais esperto que a maioria dos outros garotos, essa *porcaria* que nos ensinam me chateia. Estou no ensino fundamental ou o ensino médio. Eu escutei os professores explicarem pela décima quinta vez como reduzir uma fração (...). Eu fiz uma descoberta hoje. Eu encontrei um computador. Espere um segundo, isso é legal. Ele faz o que eu quero. Se ele comete um erro, é porque eu estraguei tudo. Não porque ele não gosta de mim (...). E então aconteceu. Foi aberta uma porta para o mundo. Correndo pela linha telefônica como heroína pelas veias de um viciado, uma pulsação eletrônica é enviada como refúgio para a incompetência do dia a dia (...). É isso... Aqui é onde eu pertença... Este é o meu lugar. Eu conheço todos aqui... Mesmo que nunca tenha conhecido ou nunca conversado, talvez nunca ouça falar deles novamente. Mas conheço todos vocês.”. *The mentor* destaca a curiosidade, e a forma com que se sentem frustrados ou entediados com normas estabelecidas socialmente.

*Revolution*⁶⁷, pois foi o primeiro a romper com o senso comum que estava se desenvolvendo, mostrando detalhadamente a real importância desta comunidade (no caso o TMRC) no sentido de inovação. O trabalho do jornalista só foi traduzido e lançado no Brasil em 2012.

O Jornal “Estadão” escreve os artigos “Mais 623 meninos participaram dos Jogos de Guerra?”, de 19 de julho de 1985 e “O Pentágono revisa sistemas eletrônicos” de 21 de julho do mesmo ano, falando sobre uma grande investigação que levou o Pentágono a modificar seus sistemas, após a prisão de sete jovens com idades entre 13 e 17 anos de Nova Jersey, envolvendo ligações gratuitas para o exterior, códigos informativos do sistema do Pentágono e da companhia AT&T, etc.

Segundo a matéria “Ladrão Eletrônico, um tipo que começa a preocupar” de Ana Maria Martins no jornal O Globo, de 14 outubro de 1985, havia no Brasil em torno de 10.000 computadores instalados nas residências, com softwares cada vez mais simples, o que facilitava sua utilização. Estes computadores despertavam a curiosidade das crianças e dos jovens, que tentavam descobrir senhas e códigos secretos, crescendo a necessidade de proteção de dados e de criptografia, uma cultura que teria surgido no Brasil por volta de 1981.

Na matéria, de Martins (1985) o professor Cláudio Leonardo Lucchesi (UNICAMP, atualmente professor Emérito em Ciência da Computação) destacou que a falta de domínios de softwares e hardwares nos equipamentos militares da Argentina teria favorecido a vitória da Inglaterra na Guerra das Malvinas (1982), demonstrando que a criptografia também poderia ser aplicada em operações militares e dificultar tentativas de quebrar códigos de segurança.

Eles chegaram a serem acusados de mudar a posição de satélites, posteriormente desmentida, afirmando um interesse crescente de psicólogos e sociólogos em explicar o fenômeno, descrevendo um perfil de “jovens comuns, vindo de lares de classe média- e com uma inteligência sempre e se não superior, pelo menos muito afinada com conceitos tecnológicos e matemáticos”.

Porém, no Brasil tais questões não eram efetivamente muito claras. Logo em 1985, a antiga editora Urânia, modificou o nome para Editora *Aleph*.

3.5.2 *Cyberpunk como indivíduo no Brasil*

⁶⁷ Lançado em português em 2012 pela editora Évora com o título “Os Heróis da Revolução”

Os avanços tecnológicos que levaram ao desenvolvimento dos computadores pessoais no final da década de 1970, tornaram o equipamento cada vez mais presente nas vidas de uma parcela cada vez maior da população na década de 1980. Mesmo com todos os desafios, anteriormente apresentados, não apenas a cultura hacker, mas também uma comunidade *cyberpunk* começou a se desenvolver no Brasil.

As análises do princípio da comunidade *cyberpunk* no Brasil, foram essencialmente baseadas em matérias publicadas em jornais de grande circulação no país. Por isso, esta parte da pesquisa foi um esforço de buscar informações capazes de fazer uma possível reconstrução histórica desta comunidade, também dos *cyberpunks* no país ainda na década de 1980.

Do contrário do que acontecia em outros países, tanto a comunidade hacker quanto a *cyberpunk* eram relativamente fechadas e poucos materiais foram efetivamente produzidos por eles próprios (como narrativas, manifestos, entrevistas), o que dificulta apresentar seu próprio ponto de vista.

Primeiramente é importante definir o termo *cyberpunk*. Lemos (2002, p.23) afirma que:

O prefixo *cyber* vem do termo cybernetics, originária do latim "gubernetes", que significa controlar ações ou comportamentos, direcionar, exercer autoridade ou ainda governar. Cibernética significa aqui a sociedade das redes telemáticas e da microinformática. Já o sufixo *punk* revela a atitude, típica do final dos anos 70, que pregava, sobretudo, a desobediência ao sistema vigente, às leis e às normas instituídas. A ficção científica apropriou-se do termo punk para designar a atitude de utilização do ciberespaço e das novas tecnologias digitais. Nesse sentido, *cyberpunk* significa o *zeitgeist*⁶⁸ contemporâneo, unindo distopia e pessimismo com a apropriação e vitalismo em relação as tecnologias contemporâneas. Podemos dizer que o cyberpunk realiza o imaginário tecnológico da cibercultura.

Os *cyberpunks* segundo Castells (2003; p. 46) “Fundam sua autonomia social na Internet, lutando para preservar sua liberdade contra a intrusão de quaisquer tipos de poderes, inclusive a tomada de controle de seus provedores de serviço de Internet pelas corporações da mídia”.

Jameson (2004) chama a atenção para as ficções científicas *cyberpunk*, que mesclam a realidade de grandes multinacionais com a “paranoia global”, com destaque para “as inovações representacionais de Willian Gibson”. E acreditava-se neste período que o computador não era uma máquina de produção e sim de reprodução.

A matéria “Cyberpunk”, do jornal O Globo de 21 de maio de 1989, afirma que alguns *cyberpunks* defendiam o ponto de vista de que o termo foi criado pela própria mídia em sua “sede inesgotável de classificar tudo”, em que eles se definiam dentro de quatro grupos

⁶⁸ Espírito da época

Radical Hard SF, The Outlaw Technologists, the Eighties Wave, The Neuromantics, The Mirrorshades Group.

Mas como afirma Bruce Sterling, na introdução da obra *Mirrorshades* (1986), teria sido o “*cyberpunk*” o rótulo que foi aderido, sempre buscando traçar um perfil de indivíduo, mas que nunca se encaixa perfeitamente ao mesmo, propondo explicar tal movimento, incluindo sua origem e seus devidos desdobramentos.

Mas segundo a matéria do jornal O Globo, quando a *Omni Magazine* (especializada em Ficção científica) cunhou os termos *cyber* da cibernética *punk* do movimento de rua dos anos 70, o rótulo ficou “irresistível e colou” (SIC) e os “pioneiros da tendência também são legião”, um ponto de vista defendido pelo próprio Bruce Sterling, um dos fundadores do gênero *cyberpunk*.

Sterling (1986) afirma que os “*cyberpunks*” são profundamente relacionados a um subgênero da ficção científica dedicado em uma profunda precisão científica (o que explica a riqueza de detalhes de obras como *Neuromancer*), em que muitos autores recebem influências de diversos estilos e gêneros musicais, tais como os punks ou o rock progressivo (dos quais muitos autores são declaradamente fãs).

A cultura *pop* remete à utilização de óculos espelhados, utilização de preto cromado ou fosco gerando o que o autor chama de uma integração, uma sobreposição de gêneros antes separados: o da alta tecnologia da cultura *pop underground*, integrando, por exemplo, o universo dos *hackers* a um tipo de “rock eletrônico”. (STERLING;1986)

O estilo está ligado à temática do futuro e uma forte tendência de troca e overdose de informações de maneira essencialmente rápida. Haveria uma tendência de que não existiria apenas uma organização controladora (como o *Big Brother* proposto na obra 1984 de George Orwell), mas diversas corporações sobre controle da informação, que se tornaria um bem valioso. Filmes como *Blade Runner* são apontados como grande referência do *cyberpunk* como estilo (GLOBO;1989).

Não houve muita dificuldade em inserir o debate em torno dos *cyberpunks* em um trabalho com uma temática hacker. Teria ocorrido ao longo de décadas, uma fonte fundamental de energia cultural relacionada a tecnologia, fornecendo um paralelo entre na cultura *pop* ao longo da década de 1980, integrando este submundo dos hackers, o hip-hop, o *scratch*⁶⁹, o sintetizador (no rock eletrônico) em Londres e Tóquio, um fenômeno que Sterling (1986) destaca ter um alcance global, em que o *cyberpunk* é a encarnação literária deste fenômeno.

⁶⁹ Técnica de arranhar discos de vinil.

Na moda, estilistas como o belga Walter Van Beirendanck introduziram o neon, cores e gráficos a suas coleções, inspiradas no “movimento *cyberpunk*” da década de 1980, estando diretamente ligadas à falta de profundidade e superficialidade da sociedade do consumo, uma vez que não captam toda a profundidade e complexidade do estilo ao qual é baseado.

A matéria do jornal O Globo de 21 de maio de 1989, finaliza afirmando que o Brasil é “cyberpunk e não sabe”, sob grande influência de publicações como *Neuromancer*, filmes como *Robcop* ou “O exterminador do futuro”, HQs como “*Watchman*” de Allan Moore (o mesmo de V de Vingança), na moda e estilo sob a influência da Cultura japonesa, o estilo de música é atribuído ao reggae, ao compositor Brian Eno, Laurie Anderson e ao Pop soviético. Cores, são atribuídas ao vermelho, preto e metálicos e o “Artefato” é um computador com um modem, uma câmera da Cannon que imprimia a partir de um “disquete”, “Disc Laser” (CD), e lugares: Japão, Los Angeles, Atlanta, Caribe e Brasil.

O pensador Timothy Leary, considerado uma referência em movimentos relacionados à contracultura, afirma que eles são a “última tribo urbana⁷⁰ do planeta”, dizendo que eles são “indivíduos que tem a inteligência e a coragem para procurar o acesso e o uso da tecnologia de *quantum* elevado para suas próprias finalidades de comunicação”, assumindo pessoalmente seus próprios futuros sem se reunir em grupos políticos ou se preocupar com questões morais.

O *cyberpunk* como consumo ou a apropriação por parte da literatura, mídia, moda e cinema de um gênero se tornou um estilo também no Brasil ao decorrer da segunda metade da década de 1980 e início da década de 1990. Assim podemos observar as tentativas de construir não apenas uma cena hacker no Brasil, mas também definir e dar sentido ao próprio indivíduo *cyberpunk*.

A afirmação de que o Brasil não saberia que era *cyberpunk*, se deu do próprio desconhecimento e até mesmo depreciação de muitos em relação a própria existência e capacidade de que uma comunidade hacker pudesse se desenvolver no país na década de 1980, envolvendo indivíduos que já enxergam a tecnologia como algo natural, que poderia ter sido facilmente integrada na sociedade.

⁷⁰ Sobre a utilização do termo “tribo urbana” Murillo (2011) aponta que segundo Machado Pais (2004,p.18): De facto (sic), da mesma forma que as antigas tribos se identificavam com determinados ‘meios ambientes’ (sic), também as novas tribos urbanas se identificam com asfalto, bairros, ruas, lugares de agrupamento de sociabilidades. O que a metáfora da tribo sugere é a emergência de novas formações sociais que decorrem de algum tipo de reagrupamento entre quem, não obstante as suas diferenças, procura uma proximidade com outros que, de alguma forma, lhe são semelhantes de acordo com o princípio ‘qui se ressemble s’assemble’ (V. Fournier). É, pois, em formas de sociabilidade que devemos pensar quando falamos de tribos urbanas, sociabilidades que se orientam por normas autorreferenciais (sic) de natureza estética e ética e que assentam na produção de vínculos identitários (PAIS, 2004, p.18).

Como anteriormente citado, Castells (2003) destacou as contradições de hackers que vivem em países mais pobres, diferentemente daqueles que viviam nos Estados Unidos por exemplo, uma vez que as adversidades os levariam a procurar alternativas para a prática de seu hacking.

Um dos maiores obstáculos no Brasil, como apresentado no início deste tópico, foi o PNI (Política Nacional de Informática), que atingia diretamente o valor e qualidade dos equipamentos comercializados no país. A capacidade de contornar os obstáculos e limitações sofridas por essa primeira geração de hacker no Brasil, demonstram seu potencial em relação a cena que se desenvolvia internacionalmente.

No jornal Estado de São Paulo de 01 de novembro de 1987, é publicada a matéria “Yes, nós não temos *cyberpunks*”, apresentando pequenas transgressões cometidas por jovens com idades entre 13 e 15 anos em São Paulo, como por exemplo reservar um voo inteiro da extinta companhia aérea Varig, após invadir o *software* da empresa.

Como não havia este perfil bem trabalhado no Brasil, surge uma preocupação por parte do professor Pierluigi Piazzi⁷¹ em tornar as habilidades que eram utilizadas para cometer transgressões em algo realmente produtivo. Como ele conhecia boa parte dos jovens que usavam computadores para este fim em São Paulo, ele resolveu abrir uma Editora e empregar estes hackers para que eles publicassem livros sobre estes feitos, revelando o resultado de seus *hacking*: A Editora Urania atualmente conhecida como Editor Aleph, uma das mais importantes nesta época na publicação de livros da área de inovação e ficção científica (sendo a responsável por publicar a versão em português do romance *Neuromancer*⁷²), assuntos que geralmente interessam *hackers* e *cyberpunks*.

O professor Piazzi via que as transgressões eram fruto de um desequilíbrio social, causado pelo sentimento de deslocamento destes jovens de uma sociedade que não conseguia acompanhar sua genialidade. A editora Aleph foi fundada visando a necessidade de se construir uma cena hacker baseada nos princípios da ética, gerando informações de forma que os hackers não precisassem cometer uma transgressão para aprender sobre ética.

O artigo do Estado de São Paulo ainda aponta que, segundo Luciano Cassalli, na época com 21 anos e morador do Jardim Paulista: “No filme *Brazil* (de Terry Gillian) um inseto entra em uma impressora, e provoca um curto circuito. Isso faz com que o nome de uma pessoa seja

⁷¹ É possível encontrar vídeos da década de 1980 do Prof. Pierluigi Piazzi disponíveis no Youtube. Eles teriam sido uma das principais bases para a formação dos primeiros programadores no Brasil. A exemplo do vídeo “Dominando o MSX” de 1987. Disponível em: <https://youtu.be/w28b6elAHho>

⁷² Romance de Willian Gibson publicado em 1984, sendo apontado como o primeiro a utilizar o termo “ciberespaço”

colocado acidentalmente em uma lista negra. Os computadores também podem ‘piratear’ a sociedade”. Enquanto Carlos Eduardo Salvato afirma que se não fosse pelo valor do modem “os hackers brasileiros seriam definitivamente elevados a *cyberpunks*”

Na Revista Super Interessante, de novembro de 1987, é feita uma matéria envolvendo as atividades do CCC, após a invasão dos computadores da NASA, e explicando como era atuação de alguns grupos na época, que utilizavam de práticas transgressivas para penetrar em grandes computadores e obter informações confidenciais:

Os hackers gostam dos computadores, acreditam que eles existem para tornar a vida das pessoas melhor. Por isso os sócios do Caos, que são pacifistas, denunciaram o envolvimento da NASA com armas. Não há dúvida de que essa atividade de furar os segredos alheios é ilícita e, com as provas materiais recolhidas pela polícia francesa, os hackers alemães correm sério risco de acabarem na cadeia. Mas isso não acabará com a preocupação de governantes e dirigentes de grandes organizações: se garotos utilizando computadores comuns conseguem tais façanhas, qual a garantia de que seus segredos podem ser mantidos realmente secretos?

Não danificar sistemas de computador que são invadidos, não mudar a informação desses sistemas e compartilhar sempre as informações obtidas, são práticas eventualmente defendidas por *cyberpunks*, *criptopunks* e por alguns *hacktivistas*.

A matéria de 27 de março de 1988, “A Invasão dos Piratas de computador” do Estado de São Paulo, descreve a atividade de cerca de 300 hackers, crackers e phreakers⁷³ paulistanos, associados a diversos grupos. É interessante pois a descrição que é feita desta comunidade no Brasil é muito diferente do senso comum frequentemente associada a Cultura Hacker estadunidense, como destaca Lemos (2002, p. 23):

Os primeiros *cyberpunks* eram garotos adolescentes poucos sociáveis e com grande conhecimento de informática que, vestidos em roupas que não possibilitavam a distinção entre os demais, podiam, dos próprios quartos, penetrar os bancos de dados de escolas ou órgãos do governo. A mídia exagerava propalando do que seriam capazes, somente para provar que eram capazes, de disparar uma centena de mísseis sobre a então União das Repúblicas Socialistas Soviéticas e detonar assim a Terceira Guerra Mundial. Essa possibilidade foi retratada no filme *War Games*, talvez a primeira expressão popular do imaginário dos *cyberpunks*.

No Brasil, além de procurar aulas de computação, de inglês e passar uma média de 12 horas em frente aos computadores “descobrimos coisas nem mesmo os fabricantes pudessem imaginar que existisse” eles:

“namoram, são fluentes em português, vestem-se na moda, convivem com os colegas de escola, em casa trocam a violência da televisão pelas teclas do computador. São contra a reserva do mercado para a informática e olham com desprezo as máquinas nacionais e costumam dizer ‘hacker que é hacker não copia programas. Inventam e tenta descobrir as senhas dos grandes computadores”

Ainda segundo a matéria, um dos *hackers* afirma que muitas de suas atividades são feitas por *hobby* (diversão) e a fragilidade dos sistemas e softwares brasileiros não oferecem um

⁷³ Apesar de serem descritos na matéria como “hackers”, pela descrição de suas atividades optou-se em diferenciar suas atividades.

desafio para esta comunidade. A estratégia apontada por empresas deste período, é que se algum *hacker* os invadisse, a melhor opção era tentar contrata-lo para desenvolver sistemas de segurança contra novos possíveis ataques.

Em 21 de maio 1988, no mesmo jornal, a matéria “Hackers dominam sistemas”, fala sobre práticas de *phreakers* e *crackers*, sem defini-los, apenas aponta que causar prejuízo a terceiros “fere o código de honra dos ‘piratas’ e nenhuma destas práticas se enquadra no perfil de um verdadeiro hacker”. Muitos indivíduos descritos nestas matérias, ou mudaram de área ou atualmente trabalham com alguma área relacionada à informática, em especial na área de desenvolvimento e segurança.

E enfim na Folha de São Paulo de 4 de novembro de 1988, a matéria “Clubes do Computador se multiplicam e atraem nova geração” pode ser vista como uma das matérias mais completas e mostrava efetivamente como foi a formação dos primeiros grupos de hackers brasileiros, mostrando diversos jovens que se reuniam para trocar informações (presencialmente ou *online*) e aprender mais sobre os limites que o computador oferecia, descrevendo a criação de programas desenvolvidos por diversão.

A grande maioria, era um perfil de jovens entre 14 e 19 anos, como Edi Kulinki, na época com 17 anos, que tentava juntamente com outros quatro amigos “montar um decodificador que traduzisse as ordens do micro em força motora”, além de desenvolverem um sistema operacional para o uso do grupo, que fazia parte do MISC (*MSX International Group*), um grupo de usuários do MSX ⁷⁴ fundado em 1987 que compartilhavam informações e conseguiam descontos na compra de jogos, e teriam cerca de 1800 associados no Brasil.

O diretor do MISC na época, Álvaro Mattar (com 49 anos na época) afirmava que ele percebia um interesse dos jovens em se associar ao grupo para obter informações sobre jogos, mas posteriormente eles acabavam se interessando em atuar profissionalmente na área.

O artigo descreve um segundo grupo o CBBS-SAMPinha⁷⁵, fundado em 1986 que mantinha seu contato basicamente *online* e era voltado ao envio de mensagens para tirar dúvidas, ofereceria um classificado de venda e troca de *hardwares* e *softwares* com mais de 352 membros cadastrados no Brasil e no mundo, e praticavam o hacking tanto de hardwares quanto softwares.

⁷⁴ Padrões de microcomputadores da década de 1980

⁷⁵ Baseado no *Bulletin Board System* (BBS) Softwares que permitem a conexão pelo telefone do computador a baixo custo e de maneira simples, permitindo a troca de informações e aplicativos. Muito utilizados entre 1970-1990, sendo considerada a primeira comunidade *online* não militar.

Sempre no aniversário do grupo ou quando o número de conexões virava um milhar⁷⁶, eles se reuniam para comemorar, principalmente pessoalmente, uma vez que eles só se conheciam pelo computador, em uma oportunidade de trocar experiências sociais.

Mas, certamente, o surgimento da *World Wide Web* (WWW), que possibilitou um maior acesso de usuários na rede, fez com que a maioria dos estudos voltados a cultura hacker no Brasil se dedicasse a compreender sua expansão a partir da década de 1990, principalmente em debates voltados a temáticas como a do software livre, do código aberto⁷⁷ entre outros.

Para finalizar, gostaríamos de destacar, mesmo que maneira superficial, que existem dois manifestos envolvendo os *cyberpunks*, porém, ambos são da década de 1990: o primeiro de Eric Hughes de 9 de março de 1993, demonstrando a importância da privacidade, da criptografia e da liberdade de expressão. Um segundo manifesto cyberpunk é datado de 14 de fevereiro de 1997, e escrito por Christian A. Kirtchev. Nele, há a afirmação de que os *cyberpunks* são rebeldes de pensamento livre, um discurso claramente de jovens afirmando ser “ratos de tecnologia nadando em um oceano de informações”, “garotos de colégio, sentados na última carteira, no canto da sala”, “adolescentes que todos consideram estranhos”, “rebeldes de pensamento livre” e que a “informação é o poder”.

Uma variante dos *cyberpunks* são os criptopunks (*cypherpunks*), dedicados em defender sua própria privacidade, construir sistemas anônimos e lutar contra a coleta de informações (HUGHES,1993; HIMANEM,2001) ao qual Assange (2013, p.5) define que:

Os *cypherpunks* defendem a utilização da criptografia e de métodos similares como meio de provocar mudanças sociais e políticas. Criado no meio dos anos 1990 o movimento atingiu seu auge durante as “criptoguerras” e após a censura da Internet em 2011, na Primavera Árabe. O termo *cypherpunk* -derivação (criptográfica) de *cypher* (escrita cifrada) e *punk* – foi incluído no *Oxford English Dictionary* em 2006.

Ainda segundo Assange (2013, p.28), a criptografia deve ocorrer de maneira confiável, automática e até mesmo inconsciente, totalmente “livre do controle do Estado”, protegendo a liberdade dos indivíduos (em sua esfera privada) de programas de vigilância e controle em massa. Também a margem do indivíduo cyberpunk, surgem os *crackers* e suas respectivas variações. (CASTELLS;2003)

A ascensão dos hackers e da construção de um indivíduo *cyberpunk* se deu graças a uma tecnologia cada vez mais presente nas vidas da população em geral, que popularizaram ainda mais características deste gênero, inclusive no Brasil.

⁷⁶ Prática posteriormente absorvida nos chans.

⁷⁷ Para mais informações para diferenciar Software Livre de Código aberto acesse: <https://goo.gl/rwMneh>

3.6 Conclusões

Neste capítulo apresentamos tópicos importantes da origem dos hackers de computador e é importante pontuar o fato de que um dos principais conflitos gerados dentro da própria comunidade é em relação a éticas, tipologias⁷⁸ e normas criadas pelos próprios hackers. Observa-se que buscam estabelecer um tipo ideal de hacker, excluindo ou não práticas e indivíduos que não se encaixam dentro destes princípios. Um dos principais objetivos deste capítulo foi oferecer uma base, para que fiquem claras as possíveis origens de certas posturas dos hackers, que são frequentemente recuperadas pela sua própria comunidade.

Buscando apresentar uma perspectiva diferenciada, mesmo que de forma inicial e investigativa, compreendemos que a partir da década de 1980, começou-se a construir uma cena hacker no Brasil, período no qual houve um aumento da venda dos computadores pessoais em diversas do mundo. Boa parte destes trabalhos apresentam a percepção de outros países, em especial nos Estados Unidos e países Europeus.

Uma vez, que os trabalhos voltados para esta temática no Brasil são escassos⁷⁹, fizemos o levantamento de informações a partir de revistas e jornais desta época, esperamos assim, que este breve trabalho abra um novo campo de investigação no país de forma mais aprofundada.

Apesar das adversidades do próprio cenário político do Brasil, tivemos a oportunidade de acompanhar, mesmo que de maneira exploratória e inicial, como os primeiros hackers brasileiros contornaram e reagiram a tais situações, construindo suas próprias soluções.

O hacker brasileiro dos anos de 1980 era visto de uma forma diferente do estereótipo comum baseado na experiência estadunidense. Os Clubes do Computador em São Paulo (1988) chamam atenção, pois se assemelham as estruturas dos *Hackerspace*, que surgiram a partir da década de 1990, a criação de uma editora preocupada em oferecer bases para um hacking ético e a própria posição de empresas em tentar contratar hackers que os invadissem para ajudar a desenvolver sistemas de segurança.

Dentro de um contexto geral, os capítulos foram uma tentativa de analisar a forma ao qual o hacker se tornou um problema social e a compreensão da diversidade existente nesta comunidade nos permite compreender em alguma medida, forças que tencionam as bases do hacktivismo e do próprio Anonymous.

Isso nos permite compreender possibilitam por meio de suas atividades, a criação de uma complexa rede, que amplia a ideia de “Cidade por Projetos” idealizada por Luc Boltanski

⁷⁸ Conforme o ANEXO 01

⁷⁹ Parte dos trabalhos são voltados para a construção do meio hacker a partir da década de 1990

e Eve Chiapello (2009), de forma que nos permita refletir como o Anonymous mudou e ampliou o sentido do próprio hacktivismo.

Gramsci *in* HALL (1993) demonstrou a importância de um estudo de estrutura, que seja capaz de determinar o que é orgânico (ou permanente) a partir de fenômenos de conjuntura, que aparecem de maneira ocasional ou acidental, buscando compreender a relação correta entre o que é fixo e o que é fluxo.

Toda a construção feita nos capítulos anteriores nos permitem compreender a complexidade envolvida quando nos referimos “aos hackers do Anonymous”.

4 HACKTIVISMO

Uma vez que os hackers existem fundamentalmente online (CASTELLS;2003), é importante compreender que, para essa comunidade, o ciberespaço ao qual estão inseridos, possui uma lógica diferente do “mundo real” (ou físico).

Muitos traços que serão identificados no Anonymous a partir de 2003, refletem o campo de atuação da própria cena hacker, em especial do desenvolvimento do hacktivism, que surgiu entre 1994-1996, visando descrever o hacking utilizado para fins políticos.

4.1 As definições do ciberespaço

Pouco depois da queda do Muro de Berlim em 2 de novembro de 1989, que marca também o fim da Guerra Fria, o físico britânico Sir. Tim Berners-Lee⁸⁰ procurava recursos no CERN (*Conseil Européen pour la Recherche Nucléaire*) para gerar um banco de dados que facilitasse ainda mais a troca de informações entre os cientistas pelo mundo. (CASTELLS;2003)

Sua proposta foi reescrita por Robert Cailliau e em maio de 1990 a *World Wide Web* (www) entrou em operação de forma aberta e gratuita, para que qualquer pessoa no mundo pudesse utilizá-la sem custo e sem qualquer que qualquer entidade pudesse controlar a Internet. (CASTELLS;2003)

Originalmente, o projeto consistiu em apresentar um modelo de rede com uma interface simples, que permitisse o acesso a informações pela população por meio de qualquer modelo de computador com acesso à internet de maneira padronizada e descomplicada, propondo que as informações ficassem reunidas em um único lugar (ou rede), uma vez que anteriormente estavam dispersas em variadas redes, o que dificultava eventuais pesquisas. (BERNERS-LEE; CAILLIAU; GROFF; 1992)

Foi justamente no início da década de 1990, que as teorias de rede voltaram a ser aprofundadas nas Ciências Sociais, sob grande influência destes novos avanços tecnológicos que permitiram que a rede fosse ampliada e comportasse um público ainda maior. Boltanski (2009) atribui que:

A recuperação do termo foi favorecida por uma conjunção histórica especial, marcada notadamente pelo desenvolvimento das redes informáticas que abriram a possibilidade de trabalho e colaboração a distância, mas em tempo real, e pela busca nas Ciências Sociais de conceitos capazes de identificar estruturas pouco ou nada

⁸⁰ Em 2004 Berners-Lee recebeu da rainha Elizabeth o título de cavaleiro por seu papel fundamental na criação da rede.

hierárquicas flexíveis e não limitadas por fronteiras traçadas à priori (BOLTANSKI, p134, 2009)

Scott (1991) destaca o interesse que as análises de redes sociais desenvolveram nas Ciências Sociais, mas alerta sobre a importância e atenção que os pesquisadores que pretendem seguir esta área devem ter, uma vez que muitas destas definições possuem um significado diferente: “só se o pesquisador tiver um claro entendimento da lógica de uma determinada medida ele poderá fazer um julgamento sociológico informando sua relevância para uma determinada peça de investigação” (SCOTT, 1991, p.3)

Do ponto de vista dos hackers e de membros de comunidades virtuais, o ciberespaço, ao qual estão inseridos, possui uma lógica diferente, com características muito próprias que foram construídas ao longo do tempo, em especial a partir da década de 1980, período no qual a população em geral começou a ter acesso às redes, graças ao início das vendas dos computadores pessoais.

O termo ciberespaço também foi utilizado pela primeira vez justamente por Gibson em 1984 no romance de ficção científica “*Neuromancer*”, que apresenta um indivíduo *cyberpunk* que utiliza de seu conhecimento acima da média para realizar protestos. O conceito de ciberespaço é o de uma “alucinação consensual que pode ser experimentada por *softwares* especiais em uma representação gráfica de dados, retirada de todos os computadores do sistema humano” (GIBSON, 1984, p. 260).

As muitas informações técnicas desta obra foram tão precisas que teriam inspirado a NASA a desenvolver tecnologias voltadas à realidade virtual. Não se pode confundir ciberespaço com realidade virtual: o primeiro faz referência a rede atual de linhas de comunicação. A realidade virtual é uma série de impulsos elétricos dentro do circuito dos computadores, como simulações do mundo real.

Do ponto de vista de Pierre Lévy (2000, p. 17) o ciberespaço ao qual ele também chama de rede é definido como:

“novo meio de comunicação que surge da interconexão mundial dos computadores. O termo especifica não apenas a infraestrutura material da comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo”.

Foram estes usuários e hackers inseridos em comunidades virtuais e subculturas que compuseram a Cultura da Internet, uma vez que segundo Castells (2003, p.34) “os sistemas tecnológicos são socialmente produzidos. A produção social é estruturada culturalmente. A Internet não é exceção. A Cultura dos produtores da Internet moldou o meio”.

Kim (2004) destaca a definição de ciberespaço descrita por Sterling (1992):

Ciberespaço é o “lugar” onde a conversação telefônica parece ocorrer. Não dentro do seu telefone real, o dispositivo de plástico sobre sua mesa. [...] [Mas] O espaço entre

os telefones. O lugar indefinido fora daqui, onde dois de vocês, dois seres humanos, realmente se encontram e se comunicam. [...] Apesar de não ser exatamente “real”, o “ciberespaço” é um lugar genuíno. Coisas acontecem lá e têm consequências muito genuínas. [...] Este obscuro submundo elétrico tornou-se uma vasta e florescente paisagem eletrônica. Desde os anos 1960, o mundo do telefone tem se cruzado com os computadores e a televisão, e [...] isso tem uma estranha espécie de fisicalidade agora. Faz sentido hoje falar do ciberespaço como um lugar em si próprio. [...] Porque as pessoas vivem nele agora. Não apenas um punhado de pessoas, [...] mas milhares de pessoas, pessoas tipicamente normais. [...] Ciberespaço é hoje uma “Rede”, uma “Matriz”, internacional no escopo e crescendo rapidamente e constantemente. (Sterling, 1992, p. XI-XII in Kim, 2004)

Entre os princípios inseridos no ciberespaço estão: a gratuidade, a liberdade (em especial de informação), ação e expressão, a ausência de hierarquias e o anonimato, uma vez que a identidade pessoal não é algo relevante dentro de comunidades virtuais, fato que permitiu que os usuários “se encontrassem em salas de bate papo para discutir tópicos de interesse mútuo” (GIDDENS, 2005, p;382).

Em 8 de fevereiro de 1996, John Perry Barlow, um dos fundadores da Electronic Frontier Foundation (EFF), publica em Davos, na Suíça, a “Declaração de Independência do Ciberespaço” entre os pontos principais da declaração:

“(...) Nós não temos nenhum governo eleito, nem estamos propensos a ter um, então eu me dirijo a vocês sem autoridade maior do que aquela com a qual a liberdade por si sempre se manifesta. Eu declaro como um espaço social global aquele que estamos construindo para ser naturalmente independente das tiranias que vocês tentam nos impor. Vocês não têm direito moral de nos impor regras, nem ao menos de possuir métodos de coação a que tenhamos real razão para temer. Os governos obtêm seus justos poderes pelo consentimento de seus governados. Você não solicitaram nem receberam nosso consentimento. Nós não te convidamos. Você não sabe nós, nem sabe sobre o nosso mundo. O ciberespaço não se encontra dentro de suas fronteiras. Não pense que você pode construí-lo, como se fosse um projeto de construção pública. Você não pode. É um ato de natureza e cresce por si próprio por meio de nossas ações coletivas. Vocês não se engajaram em nossa grande e aglomerada conversa, e também não criaram a riqueza de nossa reunião de mercados. Vocês não conhecem nossa cultura, nossos códigos éticos ou falados que já proveram nossa sociedade com mais ordem do que se fosse obtido por meio de qualquer uma de suas imposições. Vocês alegam que existem problemas entre nós que somente vocês podem solucionar. Vocês usam essa alegação como uma desculpa para invadir nossos distritos. Muitos desses problemas não existem. Onde existirem conflitos reais, onde existirem erros, iremos identificá-los e resolvê-los por nossos próprios meios. Estamos formando nosso próprio Contrato Social. Nossa maneira de governar surgirá de acordo com as condições do nosso mundo, não do seu. Nosso mundo é diferente. O ciberespaço consiste em ideias, transações e relacionamentos próprios (...). Estamos criando um mundo que todos poderão entrar sem privilégios ou preconceitos de acordo com a raça, poder econômico, força militar ou lugar de nascimento. Estamos criando um mundo onde qualquer um em qualquer lugar poderá expressar suas opiniões, não importando quão singular, sem temer que seja coagido ao silêncio ou conformidade. (...). Nossas identidades não possuem corpos, então, diferente de vocês, não podemos obter ordem por meio da coerção física. (...). Precisamos nos declarar virtualmente imunes de sua soberania, mesmo se continuarmos a consentir suas regras sobre nós. Nos espalharemos pelo mundo para que ninguém consiga aprisionar nossos pensamentos. Criaremos a civilização da Mente no espaço cibernético. Ela poderá ser mais humana e justa do que o mundo que vocês governantes fizeram antes.”⁸¹

⁸¹ Texto original (em inglês) <https://goo.gl/wvVF1P> em português: <https://goo.gl/IBvHQV>

Comunidades virtuais são diferentes de redes sociais estabelecidas pela Internet. As comunidades estabelecem vínculos, relações e valores próprios enquanto as redes sociais englobam a sociedade de uma forma mais generalizada estabelecendo uma estrutura compartilhada por pessoas e organizações, reproduzindo, muitas vezes, valores “do mundo real” (*off-line*) e não necessariamente compreende de maneira clara a lógica estabelecida ao longo dos anos no ciberespaço.

Porém, essas noções de valores virtuais ou reais, são definições que geram certa confusão, como destaca Berger e Luckmann *in* Kim (2004, p.213), a partir das próprias percepções oferecidas por Sterling (1992):

A preocupação de Sterling com o estatuto de “realidade” tem a ver com a natureza do ciberespaço atualmente conhecida como “virtual”. Esse “virtual” é apreendido, em muitos casos, como uma oposição à natureza “real” da “realidade”. Entretanto, o reconhecimento de que a “realidade” é “uma qualidade pertencente a fenômenos que reconhecemos terem um ser independente de nossa própria volição (não podemos ‘desejar que não existam’)” (Berger; Luckmann, 1998, p. 11) basta para ver que essa oposição “virtual” versus “real” é ilusória e bastante confusa. Os crimes “virtuais” estão aí para nos mostrar de uma forma bem dura que a “virtualidade” do ciberespaço possui uma inegável natureza coercitiva de “realidade”. O fato é que já somos seres “virtuais”, queiramos ou não, ao menos dentro dos grandes bancos de dados de corporações e governos, e cada vez mais temos o conhecimento – “a certeza de que os fenômenos são reais e possuem características específicas” (Berger; Luckmann, 1998, p. 11) – de que o ciberespaço, apesar de virtual, é bastante “real”.

Para Kim (2004), quanto mais estreitamos nossas relações com o ciberespaço como um campo de ação prática e nos tornamos uma extensão dele, crescendo a “fascinação e o temor em relação aos hackers que tanto trafegam como sujeitos virtuais do ciberespaço como manipulam os códigos “secretos” por trás das realidades virtuais” (KIM,2004, p.217). Os hackers são segundo Kim (2004), jovens, na maioria adolescentes; considerados uma figura ambígua que transitam entre as zonas mais indefinidas do ciberespaço, sendo uma “referência emblemática da cibercultura”, capazes de superar o estranhamento de uma vida cada vez mais em interação com o ciberespaço.

Tal hipótese, pode ser aplicada em 2008, quando os *Anonymous* foram para as ruas pela primeira vez estabelecendo um código de conduta, compreendendo que o “mundo real” não era é o deles e que estas regras do mesmo deveriam ser respeitadas. É diferente de um encontro presencial de comunidades ou subculturas virtuais (em convenções por exemplo). Os *Anonymous* romperam uma grande fronteira, como será melhor explicado mais adiante.

4.2 O surgimento do hacktivismo

Denning (2015) afirma que o hacktivismo surgiu no final da década de 1980 com vírus de computador e *worms*⁸² que espalham mensagens de protesto; "Um bom exemplo de hacktivismo precoce é o *Worms Against Nuclear Killers* (WANK), um *worm* de computador que ativistas anti-nuclear na Austrália lançaram nas redes da NASA e do Departamento de Energia dos Estados Unidos contra o lançamento de uma nave espacial que transportava plutônio radioativo". Ainda segundo Denning (2015) haviam diversos grupos de hackers que no início da década de 1990, praticavam o hacktivismo precoce como os "The Zippies" e "Strano Network".

Porém, o fenômeno do hacktivismo, ao qual o *Anonymous* é frequentemente associado, surgiu entre 1994 e 1996. O termo hacktivismo teria sido utilizado pela primeira vez em 1994⁸³ por Omega, um membro grupo cDc (*The Cult of the Dead Cow*) fundado em 1984, que desde sua origem defendia a criação de um *software* livre que deveria estar disponível para qualquer pessoa. Segundo o cDc:

“ele usou o hacktivismo para descrever o *hacking* para fins políticos. Originalmente era mais um trocadilho ou uma brincadeira. Mas desde o primeiro momento em que ouvi Omega usá-lo eu sabia que teria um significado profundo, não apenas para o cDc, mas para milhões de pessoas em toda a Internet”.⁸⁴

Hearn (2009) afirma que a partir do cDc surgiram diversas pessoas e grupos associados ao *hacktivismo*: advogados e ativistas virtuais defendendo, principalmente, os direitos humanos. O *software* livre se tornou um de seus princípios éticos. No interior destes grupos, ocorrem muitos debates sobre quais comportamentos são considerados aceitáveis ou éticos, quando relacionado às atividades *hackers*.

Em 04 de junho de 1995, o cDc “declarou guerra” contra a Igreja de Cientologia como resposta a tentativas da Igreja de remover um grupo de notícias chamado *alt.religion.scientology*.

É importante destacar que, em 2008, o *Anonymous* promoveu o Chanology, descrito por autores como Fontanella (2010), como “a primeira demonstração de organização e motivação política do *Anonymous* fora da Internet”, novamente atacando a Igreja de Cientologia, como será melhor descrito mais adiante.

⁸² O *Worm* (verme) é diferente de um vírus de computador. O vírus depende do programa que ele infecta enquanto o worm é um programa completo que se alastra sozinho dentro de um sistema.

⁸³ Um relatório de 2012 do Mcfee afirma que o termo foi utilizado pela primeira vez em um artigo publicado na revista *InfoNation* por Jason Sack em referência ao cineata Shu Lea Cheang em 1995.

⁸⁴ http://www.cultdeadcow.com/cDc_files/cDc-0384.php

Segundo Gabriella Coleman in KNAPPENBERGER (2012), “A Cientologia é um alvo interessante porque, de certa forma, é a perfeita inversão dos valores dos *geeks* e *hackers*. Em vários níveis diferentes: ficção científica, propriedade intelectual, discurso de liberdade, ciência e tecnologia. (...) existe um certo prazer em atacar seu oposto perfeito”.

Outro detalhe, refere-se ao fato de que, apesar de frequentemente associado ao hacktivismo, a utilização do termo ciberguerra ou “guerra cibernética” é considerado ruim por alguns pesquisadores. Richard Clarke (2015) destaca que o espaço cibernético já vem sendo utilizado como um espaço de batalha, considerado uma fonte de instabilidade em uma crise, podendo ser uma ameaça à paz.

Bobbio (2010, p.571) afirma que guerra é a continuação da política por outros meios e depende da hostilidade em um dado tempo das relações entre Estados, mesmo que o conceito de guerra ganhe novas definições com o próprio progresso da civilização.

Comprendemos que a definição do termo, apesar de suas distorções, está relacionada ao Estado e consideramos que estas “declarações de guerra” podem ser melhor compreendidas ou definidas como confrontos ou conflitos entre indivíduos contra organizações e o próprio Estado, com o objetivo de trazer visibilidade, criticar e até mesmo em tentativas de mudar uma certa situação.



Ilustração 13 : cDc (1998)

Fonte: Revista Wired (01/10/1998)⁸⁵

⁸⁵ Matéria da revista Wired disponível em: <http://www.wired.com/1998/10/orifice-98/>

Uma longa matéria na revista de música SPIN, foi publicada em 1999 com o título “*The Politics of Hacking*” com diversos grupos e hackers falando sobre os eventos que estavam acontecendo naquele momento envolvendo a temática do hacktivismo, e entre eles, o exército Zapatista⁸⁶ considerado por autores como Castells (2008) “o primeiro exército de Guerrilha informacional”, que havia, em junho de 1998, derrubado o site do governo do presidente Ernesto Zedillo. Para Castells (2008, p.103) o sucesso dos zapatistas teria se dado pela estratégia de comunicação de conseguir chamar a atenção do mundo e da sociedade mexicana para sua causa.

A matéria da revista SPIN apresenta o esforço dos *hackers* para que o hacktivismo fosse legitimado, criando *softwares* que poderiam ser utilizados por grupos dentro e fora da Internet. Os moldes eram semelhantes aos da década de 1960, contra qualquer forma de vandalismo, seguindo o estilo dos *sit-in*⁸⁷. Surgia segundo a matéria, uma nova geração de hackers, com suas próprias mensagens e ideais.

O cDc negava a ameaça de uma “guerra virtual”, pois este tipo de ameaça, mesmo que pudesse ocasionalmente ocorrer, serviria para alienar os hackers e a sociedade em geral ajudando a difundir equívocos, como afirma Emmanuel Goldstein⁸⁸, um hacker veterano e editor da revista 2600. Goldstein, ainda concordando com o fato de que os “hackers sejam majoritariamente novos, politicamente ingênuos, mas que eles estavam aprendendo a usar seus talentos”. (SPIN,1999).

Os hackers defendem que o hacktivismo deve ser feito em relação a uma agenda política, na qual o *hacking* deveria ser relacionado de alguma forma. É recomendável que os jovens “escolham primeiros suas causas antes de escolher os sites que irão hackear”. Eles ainda reforçam que a ideia de “sequestro” de máquinas (prática geralmente realizada com a utilização de um *ransomware*, um tipo de *malware* ou *software* nocivo que atinge um computador de maneira ilícita) é considerada uma prática condenável entre *hackers* de elite, uma vez que não tem nada a ver com hacktivismo e não respeitam os princípios da ética *hacker*. (SPIN;1999)

Hacktivistas do ponto de vista de Samuel (2004), definem seu movimento não por seu objetivo, mas por seus métodos, que seria um novo tipo de ativismo estratégico.

⁸⁶ O nome do exército é uma homenagem a Emiliano Zapata (1879-1919) que conseguiu fazer uma reforma Agrária no México no início do século XX. Em janeiro de 1994 ocuparam diversas prefeituras na região sul do país. Mais informações em: “A outra face da Terra: movimentos sociais contra a nova ordem global” in O poder da Identidade de Manuel Castells (2008).

⁸⁷ Uma forma de protesto político da década de 1960, criada pelo Movimento Negro. Eles ficavam sentados em lugares reservados "apenas para brancos" "*Sit-in* ou *sit-down*" em livre tradução, seria um “protesto sentado” sendo caracterizado como uma forma de protesto não violenta, ao qual os manifestantes permanecem sentados em um determinado local.

⁸⁸ Pseudônimo. Nome em referência a obra 1984 de George Orwell.

Em 2001, com base no artigo 19 da Declaração Universal dos Direitos Humanos "todos têm o direito à liberdade, opinião e expressão; este direito inclui a liberdade para prender opiniões sem interferência e para procurar, receber e dar as informações e as ideias usando todos os meios e não obstante a fronteiras" e do artigo 19 da Convenção Internacional dos Direitos Cívicos e Políticos⁸⁹, os hacktivistas declararam que:

1. Todos têm o direito a prender opiniões sem interferência.
2. Todos terão o direito à liberdade de expressão; este direito incluirá a liberdade para procurar informações por vias de comunicações orais, também receber e dar a informações e ideias de todos os tipos, não obstante a fronteiras, na escrita ou na cópia, no formulário ou na arte, ou em todos os outros meios de sua escolha.
3. O exercício dos direitos fornece no parágrafo 2 deste artigo que carrega com ele deveres especiais e responsabilidades. Pode conseqüentemente ser sujeito a determinadas limitações, mas estes estarão somente como são fornecidos pela lei e são necessários:
 - a. Por respeito aos direitos ou a reputação de outros
 - b. Para a proteção da segurança nacional ou da ordem pública, ou da saúde pública ou das morais.

Estes hackers publicam a “Declaração do Hacktivism”, reforçado o direito de liberdade do acesso à informação por qualquer meio de comunicação disponível, a oposição ao uso do poder do Estado para controlar o acesso ao trabalho de pensadores e intelectuais e de censurar a Internet, o que afeta o pleno exercício da democracia.

Alexandra Samuel (2004) relaciona em sua tese⁹⁰ que o hacktivism pode ser visto como futuro da participação política e apolítica a partir de suas táticas culturais, que fez com que os *hackers* adquirissem estratégias mais diretas e transgressivas do que a dos ciberativistas.

Já Houghton (2010) afirma que:

O hacktivism está envolvido em lutas sobre o controle da Internet e tende a ser destinado a garantir uma Internet ideal, em que os hacktivistas enxergam o que serve melhor aos cidadãos, do contrário de elites governamentais ou empresariais. Como tal, visa preservar, promover e manter uma Internet ideal não só no presente, mas também para potenciais ou futuros dos internautas. E não há dúvida de que cidadãos de ambos os lados dos segmentos digitais (Selwyn 2004; van Dijk & Hacker, 2003) reconhecem a importância da Internet como um meio de comunicação. (HOUGHTON,2010,p.29)

Enquanto a influência exercida pela Internet nos conflitos de Kosovo (1998/1999) foi considerada irrelevante, como aponta Himanen (2001,p.92) mesmo sendo considerada “a primeira Guerra da Internet” com atuação de crackers de diversos países, incluindo os Sérvios interferindo nos servidores da OTAN (Organização do Atlânticos Norte), e de americanos nos do governo Iugoslavo. A rede não tinha necessariamente “um canal receptivo de influência sobre o grande público”, ainda destinado aos meios de comunicação tradicionais.

⁸⁹ International Covenant on Civil and Political Rights (ICCPR)

⁹⁰ *Hacktivism and the Future of Political Participation* (2004)

Segundo Castells (2011) o número de usuários da Internet em 1995, era de 40 milhões. Dados demográficos referentes a quantidade de hackers eram particularmente difíceis de serem coletados. Sterling (1992) estimou que no início da década de 1990 havia cerca de 5.000 hackers, sendo 100 considerados de elite, enquanto Mungo (1992) afirma que haveriam 2.000 hackers realmente dedicados e outros 10.000 aspirantes.

Até o início dos anos 2000, o hacktivismo ainda não tinha atingido toda a sua potencialidade. Uma vez que nos anos 2000 a Internet tinha 400 milhões de usuários. Em 2015 o número ultrapassou 3,2 bilhões de pessoas que se conectam⁹¹ não apenas por meio de computadores, mas com Tablets, notebooks, smartphones e outros dispositivos com tecnologias cada vez mais avançadas.

Ao contrário do que aconteceu em Kosovo, hoje, a Internet (com grande participação dos jovens) foi decisiva em grandes eventos do Século XXI, a exemplo da Primavera Árabe, que segundo Vargas (2012) do *The New York Times* na matéria “*Spring Awakening*”, o Oriente Médio teria uma média de 100 milhões de pessoas com idades entre os 15 e os 29 anos com boa educação, mas sem emprego. Ainda segundo o jornal, mesmo que apenas uma fração da população tenha acesso à Internet este número teria saltado de 1,5 milhões em 2004 para 13,6 milhões em 2008.

A autora Tessa Jade Houghton (2010, p.202) em sua tese neohabermasiana que compreende o hacktivismo como forma pós-moderna de ampliação da Esfera Pública, tendo como base a ação direta *online*, uma vez que o hacktivismo permite:

Formas contestatórias de comunicação não-coercitiva para a esfera pública, em vez de exigir toda a participação em cumprir critérios racionais críticos, indo de alguma forma para neutralizar ou, pelo menos, desafiar os diferenciais de poder comunicativo e político presentes em sociedades tremendamente estratificadas dentro das quais estes existem, sendo, portanto, um objetivo importante.

As transmissões ao vivo (via *streaming*) tornaram cada indivíduo uma testemunha de grandes eventos em tempo real, tornando “a comunicação sem fio não mídias em seu sentido tradicional, mas meios de uma comunicação mais interativa” (CASTELLS,2011)

A Internet atualmente promove o que Castells (2013) define como “redes de indignação e esperança”, reflexo de uma mudança fundamental no mundo das comunicações, em função do surgimento da autocomunicação em massa – caracterizada como o uso da Internet e das redes sem fio como plataforma de comunicação digital, uma vez que processa as mensagens de

⁹¹ Segundo a ONU 3,7 bilhões de pessoas ainda não tem acesso a Internet no mundo. A “Penetração da Internet nos países desenvolvidos é de 81%, enquanto nos países em desenvolvimento fica em 40% e, nas nações mais pobres, em 15%.” <https://goo.gl/Lq3EVG>

muitos para muitos e, potencialmente, chega a receptores que conectam-se em incontáveis redes que transmitem informações digitalizadas em um bairro ou no mundo. (CASTELLS;2013)

Em uma pesquisa da GlobeScan realizada para a BBC em 2010⁹² que entrevistou 27.973 adultos em 26 países, sendo 14.306 usuários da Internet, apontou que 4 em cada 5 pessoas usuárias ou não da rede a consideram um direito fundamental e 53% dos entrevistados, considera que não deveria ser controlada pelo governo.

Em 2011 a Organização das Nações Unidas (ONU)⁹³ considerou a Internet um direito humano, compreendida como parte do Artigo 19 da Declaração Universal dos Direitos Humanos⁹⁴, e segundo La Rue (2011) todos os indivíduos devem ter o “direito de buscar, receber e difundir informações e ideias de todos os tipos através da Internet” reforçando “a natureza única e transformadora da Internet não só para capacitar os indivíduos a exercerem o seu direito à liberdade de opinião e de expressão, mas também por proporcionar uma série de outros direitos humanos, além de promover o progresso da sociedade como um todo.” (ONU, 2011)

Os limites do hacktivismo seriam atualmente mais indefinidos, uma vez que muitos hackers vão hoje também para as ruas protestar, em especial, o *Anonymous*.

4.3 ANONYMOUS

Entre 2003 e 2006, usuários do *imageboard* 4Chan passaram a formar pequenos grupos a partir da utilização de frases, memes e imagens (como *It's over 9000*, *mudkips*, *longcat is looong*), de forma que eles conseguissem identificar que, em meio a inúmeras postagens anônimas e aleatórias do canal /b/, havia um integrante desse pequeno grupo de usuários conhecidos.

Aos poucos, esses usuários começaram a se autointitular Anonymous e são frequentemente associados a práticas hacktivistas, cercados por uma série de códigos e regras que foram construídos ao longo dos anos.

4.3.1 Dos BBS ao 4Chan

⁹² Pesquisa disponível em: <https://goo.gl/jbE1nY>

⁹³ Relatório disponível em: <https://goo.gl/0iRvwp>

⁹⁴ Todo ser humano tem direito à liberdade de opinião e expressão; esse direito inclui a liberdade de, sem interferência, ter opiniões e de procurar, receber e transmitir informações e ideias por quaisquer meios e independentemente de fronteiras. <https://goo.gl/i7hzts>

Sébastien Wesolowski (2016) afirma que para entender os *Chans*⁹⁵ é preciso voltar na história e compreender o BBS. Segundo Scott Gilbertson (2010) o BBS⁹⁶ é um sistema de computador, conectado via telefone, semelhantes a um “quadro de avisos” (WESOLOWSKI;2016) com foco no compartilhamento de *softwares* ou troca de mensagens com usuários *online*, de maneira simples e barata virando uma verdadeira comunidade na década de 1980.

Gilbertson (2010) aponta que o primeiro BBS foi desenvolvido em 1978, por Ward Christensen e Randy Suess, com o nome de *Computerized Bulletin Board System* (CBBS), sendo inicialmente limitada às instituições financiadas pelo Departamento de Defesa para aperfeiçoar a ARPANET.

Posteriormente, os autores publicaram detalhes do desenvolvimento do sistema, que possibilitou a criação de diversas outras BBS, gerando a primeira comunidade baseada em computadores não-militares. (GIBERTSON;2010)

Wesolowski (2016) relata que em 1994, em seu auge, tinha cerca de 17 milhões de usuários só nos Estados Unidos, mas cerca de um ano depois começou a se tornar obsoleto, em função dos navegadores habilitados para acessar a Internet, que abriram a possibilidade de criação de uma “rede mais rica, expansiva e de mais fácil acesso do que o BBS” (WESOLOWSKI;2016). Ainda hoje, os BBS são utilizados por alguns *hackers* para promover o senso de comunidade.

Em 1996 um japonês chamado Masayuki Shiba criou uma BBS chamada *Ayashii Warudo*⁹⁷ (Mundo estranho/ suspeito), na qual os usuários são anônimos, desenvolvendo uma cultura baseada em memes⁹⁸. Criando posteriormente diversos sites embasados nesta estrutura (WESOLOWSKI;2016, TANASINN;20--).

Christopher “Moot” Poole, estava na Internet e se deparou com um *imageboard* dedicado a animes, chamado *2Chan*.⁹⁹ Segundo Fontanella (2010), *imageboards* tem origem nos fóruns japoneses, que originalmente iniciam uma discussão de forma anônima.

⁹⁵ Uma vez que as informações das comunidades dos *chans* não ficam indexadas em seus sites, dificultando estudos aprofundados desta temática, um tópico no site <https://goo.gl/4klcVw> oferece uma detalhada cronologia da criação dos chans, em especial do *4chan*, um importante registro, atualizado com frequência. Boa parte do artigo de Wesolowski (2016) <https://goo.gl/P4Opny> foi claramente baseado nele.

⁹⁶ O BBS foi muito utilizado no Brasil até na metade da década de 1990

⁹⁷ Em japonês: あやしいわーど

⁹⁸ Segundo Petrella (2006,p.54) “O conceito de meme vem de Richard Dawkins, biólogo evolucionista da universidade de Oxford, em seu livro “O Gene egoísta” (1976). O meme é como um vírus. Pode, portanto nos infectar. Assim como genes se propagam de um corpo para o outro por intermédio de espermatozoides ou ovos, memes pulam de um cérebro para o outro. Nós hospedamos e reproduzimos esses “parasitas informacionais” mediante a toda a nossa produção cultural: artes, religiões, artefatos, tecnologias, tudo.”

⁹⁹ <http://www.2chan.net/>

Os *imageboards* permitem que, por meio de sua interface simples e semelhante aos sites do início da década de 1990, que tópicos sejam abertos e organizados cronologicamente após a postagem de uma imagem (FONTANELLA;2014). Estes tópicos por sua vez, são geralmente divididos em uma série de canais com temas variados (origami, animes, moda, etc).

O que teria chamado a atenção de Poole foi o fato de que o site dava a possibilidade de, em poucos segundos, criar centenas de *posts* (postagens) de forma anônima, sem a necessidade do registro do usuário.

Em 2003, Poole desenvolve, aos 15 anos, o *4chan*¹⁰⁰, considerado o maior e mais influente *chan* fora do Japão. Em 01 de outubro de 2003, ele cria o canal /b/ (b/board) com seus temas aleatórios. Tal canal é definido por diversos pesquisadores como “anarquista” por englobar qualquer tipo de imagem, assunto ou piada. O Jornal *The Guardian* define o /b/ como “A Identidade da Internet” (DIBBELL;2010) pois o mantém o anonimato e a completa liberdade de expressão, típica de sites do início da década de 1990. A ideia do canal, segundo Jon Kelly e Jude Sheerin para a BBC, parecia ser “essencialmente colocar todos os trolls¹⁰¹ em um único lugar e ver o que acontecia”.

Porém, em 30 de janeiro de 2006, ocorreu uma grande mudança no *4chan*: “Moot” configurou seu site, forçando todos seus usuários a ficarem sem identificação, isto é, “anônimos” (Anonymous).

Teria sido o momento que efetivamente a ideia do *Anonymous* começou a ganhar força, uma vez que foi justamente durante este período que aumentaram as atividades entre os membros do canal /b/. Neste momento, não envolviam atividades “hacktivistas”; no geral, eram invasões, *floods*¹⁰² e desconfigurações aleatórias de outros sites e fóruns. Segundo Vendetta in *Knappenberger* (2012)

“A ideia do Anonymous começou como uma piada. Alguém sugeriu que o site todo, se o 4chan, se o /b/, fosse uma só pessoa, essa pessoa chamada Anonymous, que estaria sentada em algum lugar e você está lendo coisas deles. Era uma perspectiva de que se quem estivesse de fora, não conseguisse ver a diferença, como se fosse só uma pessoa”

Os usuários passaram a formar pequenos grupos, identificando membros do canal com frases, memes e imagens que os identificava de forma que conseguissem criar um certo padrão e se comunicar.

¹⁰⁰ <http://www.4chan.org/>

¹⁰¹ Troll segundo o dicionário Oxford é definido como alguém que faz um post ou comentário deliberadamente ofensivo ou provocativo com o objetivo de perturbar alguém ou provocar uma resposta irritada.

¹⁰² De “enchente”, uma das atitudes mais “irritantes” da Internet. É o ato de postar muitas mensagens seguidamente em fóruns ou bate-papos de forma que atrapalhem a comunicação entre os usuários.

File : 1130798121.jpg (22 KB, 128x150, mud.jpg)

 **SOON TO BE A XENON MOTION PICTURE** Anonymous 10/31/05(Mon)17:35 No.3212044

Today being Halloween, I decided to fuck with the major retard at school when I came out of science for break. He was dressed as Ash. Knowing this was going to happen, I brought a Mudkips doll. Thus I started the conversation, making sure no one saw me.

"So I heard you like Mudkips..."
 "MUDKIPS? I LUUUUUUUUUUUUVE MUDKIPS."

"O RLY? So, would you ever fuck a Mudkips, that is..." (he cuts me off before I could said 'if you were a mudkips')
 "OF COURSE"
 "Well I just happen to have a Mudkips here, and..."

Before I finished the sentence, which would have resulted in me hitting him across the face with the doll, he grabbed it. In one swift motion his pants were down and he was violently humping it. Not to get between a man and his Mudkips I started to walk away, because there is no way I'd be caught wrestling a half-naked crazy guy humping a Mudkips.

Needless to say, within 5 to 10 seconds, some girls saw him and started screaming. I coolly walked into a restroom, pretending nothing had ever happened; not that I had intended that outcome, but now that it was in play I didn't want to be involved.

>> Anonymous 10/31/05(Mon)17:35 No.3212045

I came back out two minutes later, and like any wanton act on school grounds there was now a huge crowd around him. He was still fucking it and baying this real fucked up 'EEEEEEEEEEINNNNF EEEEEEEEEINNNF' sound. Suddenly a scuffle broke out in the middle, meaning he probably did something stupid.

I asked someone what had happened. A girlfriend of one of the football players tried to get him to stop, but he bit her for trying to take it away. Someone called in a few football players (all dressed up like Road Warrior) who proceeded to pummel the shit out of the guy. Meanwhile the school police were freaking out and having trouble getting in to the situation.

A few minutes later the intruder alarm went off and we were all shuffled into classrooms. Over the intercom the principal announced that someone had thrown a flaming push toy into the library. Uh... what the hell.

So we were kept there and about 30 minutes later the principal came on again. This time he was saying that whoever was behind the beating should turn themselves in. All of a sudden this woman began yelling, "I WILL SUE YOU FOR DAMAGES. YOU LITTLE PUNKS, I'M GONNA SUE..." and it was cut off.

I asked an office later what had happened. Apparently his mother had come to pick him up and threatened to sue for the beating and 'whatever else happened.' The school threatened to counter-sue because of lewd conduct, inciting a riot, and starting a fight.

So I ask you: do you like Mudkips?

Ilustração 14: *Mudkips* (meme de identificação)¹⁰³

Fonte: <http://www.4chan.org/>

Fontanella (2010) define o Anonymous como substantivo próprio, uma incorporação dessa identidade social nas comunidades dos chans, possuindo uma voz e uma narrativa própria, uma memória em que os feitos da comunidade ganham um ator:

O Anonymous pode ser generoso e justo ou imaturo e cruel, refletindo as contradições e vicissitudes do agregado social que representa. Longe de ser uma identidade fechada, é uma referência flexível o suficiente para permitir que os diversos membros da comunidade reconheçam a si mesmos no que têm em comum. (FONTANELLA;2010)

Sobre as condições que possibilitam as percepções de formação de grupos e redes, Simmel (1995) afirma que há uma diferença entre os motivos primitivos e aqueles considerados avançados, pois em "uma mente primitiva, qualquer coexistência de objetos no tempo espaço são psicologicamente suficientes para criar uma conexão de ideias" (SIMMEL,1995,p.127).

Tais ideias, cada vez mais complexas, se relacionam por similaridade de atributos. As associações ocorrem naturalmente pelo próprio desenvolvimento da sociedade, tanto pelo

¹⁰³ Pode-se notar na figura 11, datada de outubro de 2005 (com número 3212044), o texto, aparentemente sem nexos, possui a imagem e a passagem '*Mudkips? I luuuuuuuuve Mudkips*'. Na resposta posterior, outro Anonymous responde e a frase final é justamente "*So I ask do you like Mudkips?*". *Mudkips* é um exemplo de código que indicaria a quem fizesse parte dessa comunidade que havia alguém pertencente ao /b/.

contato com um grupo original (família, por exemplo) quanto o que acontece por um processo de identificação de talentos e atividades semelhantes. (SIMMEL;1995)

A internet, quando se trata do 4chan, deve ser analisada com extrema cautela, pois muitos dos usuários que participam destes canais são considerados, em sua maioria, *Geeks*¹⁰⁴, *nerds* com uma média de idade de 16 anos, homens (CHEN,2012) e encontraram neste canal, uma oportunidade de conhecer pessoas que eles consideram semelhantes a eles mesmos de alguma forma.

4.3.2 Dando forma ao personagem: Epic Fail Guy

Antes de utilizarem a máscara de V/Guy Fawkes, os Anonymous se identificavam como um homem verde sem face, e a mensagem “*No Picture Available*”. Segundo a página *Know Your Meme*¹⁰⁵ alguns interpretam que os primeiros “Anon(ymous)” tenham se inspirado em “*The Son of Man*”, a famosa pintura de René Magritte para criar essa personificação dos chans anteriores a 2006, mas sem comprovação.



Ilustração 15: The Son of Man vs. Anonymous
Fontes: Internet/ 4Chan

A verdadeira inspiração da imagem dos Anonymous é desconhecida, porém existem muitas referências prováveis¹⁰⁶, tomando como o fato que, se tratando de *hackers*, muitos

¹⁰⁴ As origens da palavra Geek, segundo o dicionário Oxford é que teria origem no século 19, relacionando a um dialeto que se refere a “geck” tolo, teria origem germânica. Em holandês “gek” se refere a doido, bobo.

¹⁰⁵ <http://knowyourmeme.com/> é uma página de referência virtual focada na história de memes conhecidos, especificando suas origens e alcance.

¹⁰⁶ A exemplo dos “Saticons”, personagens do seriado “*Lost in Space*” (Perdidos no Espaço), da década de 1960, descritos como humanoides de origem desconhecida e sem rosto, que geralmente viajam em grupos de três utilizando roupas pretas e chapéu coco, com alto conhecimento tecnológico capazes de viajar de planeta em

costumam fazer referências a personagens de seriados antigos, HQ's, ficção científica, como o caso da LulzSec¹⁰⁷ (que possuíam membros oriundos dos chans) em relação ao seriado “*The Love Boat*”.

Porém, a mais provável é que seja simplesmente uma variação de um perfil que quando não é adicionada uma foto aparece a mensagem “*No Picture available*”.



Ilustração 16 : No Picture Available Vs. Anonymous
Fonte: 4Chan

Os Anonymous (também referenciado por Anons), até esse momento, eram um personagem, um meme do 4Chan ao lado de muitos outros¹⁰⁸.

A brincadeira com a máscara de V/ Fawkes no 4Chan, neste primeiro momento não carregava um sentido de resistência e insatisfação. Em 2006, é lançado o filme *V de Vingança*, e um meme, datado de 15 de setembro do mesmo ano, chamado “*Epic Fail Guy*”¹⁰⁹ surge nos

planeta. Nos dois episódios em que apareceram (*Wreck of the Robot*, *The Galaxy Gift*) na segunda temporada, estão sempre atrás de algum objeto de poder para fazer algo terrível.

¹⁰⁷ A LulzSecurity ou LulzSec ficou conhecida em 2011, quando o grupo de hackers/ hacktivistas fez uma série de ataques por um mês em alvos completamente aleatórios e sem propósito (como a Fox, HBGary FBI e a SONY), apenas por “diversão” ou Lulz (para rir). Um destes ataques (a firma de cibersegurança HBGary) é descrita no livro “Nós Somos Anonymous - por Dentro do Mundo dos Hackers” de Parmy Olson (2014). Uma das referências utilizadas nos ataques da LulzSec era o tema da série de TV Americana de 1977 “*The Love Boat*” (“O Barco do Amor”); além de outras iconografias ligadas a barcos. Por conta disso, o grupo às vezes é chamado de “*The Lulz Boat*” ou “*A Jangada do Lulz*” no Brasil. Porém, fora do Brasil. A LulzSec possui uma das consequências mais desastrosas entre o Anonymous: um dos 6 membros do grupo original (além de outros 12 ou 24 colaboradores), Hector Xavier Monsegur, o Sabu, tornou-se informante do FBI e ajudou na identificação dos hackers envolvidos nos ataques, levando a prisão de alguns de seus membros. O evento é conhecido como “sabotagem” (Colleman;2014) e durante nossas entrevistas muitos integrantes do Anonymous diretamente ou não relacionados a LulzSec, ficam claramente exaltados quando mencionamos o Sabu, principalmente pelo fato dele ter ficado livre das acusações, enquanto outros membros como Anarchaos (nome real Jeremy Hammond), que também faz parte do Anonymous, cumpre 10 anos de prisão (2013-2023).

¹⁰⁸ Alguns vídeos, com esses primeiros Anons em interação com outros memes: <http://youtu.be/zMJPMJ8cR14> (Mootroll'd) , <https://www.4chan.org/flash?file=SageMan.swf&title=Sage+Man>

¹⁰⁹ De Guy Fawkes.

chans. Na sequência, o personagem estava comendo taco, e ele esconde a sujeira com uma lata de lixo. Ao olhar dentro da lata, encontra a máscara do V, coloca em seu rosto e diz olá.¹¹⁰



Ilustração 17 : Epic Fail Guy

Fonte: Internet

Em 15 de outubro de 2006, o usuário Chainsaw09 postou o vídeo “*Epic Fail Guy on HW lan.*”¹¹¹. E se torna um meme conhecido nessa comunidade, presente em diversas brincadeiras.

Contudo, no final de dezembro de 2006 e início de 2007, os Anonymous começam a apresentar fortes traços de intolerância com alguns perfis, principalmente pedófilos, nazistas, racistas e praticantes de *bullying*. Essa postura ficou clara quando atacam o radialista Hal Turner, neste mesmo ano acusado de nazismo e racismo pelos Anonymous (um dos membros relatou o ocorrido e outras pessoas vieram a sua defesa). Eles conseguem tirar seu programa do ar e, ao descobrirem o endereço de Turner, mandaram entregar pizzas, dentre outros produtos anonimamente. Além de utilizar DDos em seu site para que o valor pago no site aumentasse e, claro, invadiram suas contas de e-mail e disponibilizaram esse material.

O que fez com que ele não tivesse dinheiro para manter a rádio. Turner só foi preso em 2009 em Chicago depois de ameaçar juízes em sua rádio. Outro caso envolve Chris Forcand, suspeito de pedofilia, que os membros do Anonymous obtiveram o endereço por meio de *doxing*¹¹² recolhendo assim provas que culminaram em sua prisão em dezembro de 2007.

O 4Chan pode ser visto como um ambiente descrito por Simmel (2006) como um mundo sem atritos, totalmente artificial e que leva a uma redução do caráter pessoal à interação

¹¹⁰Disponível em: <http://i.imgur.com/wseLW.png>

¹¹¹ http://youtu.be/DKjVHLCB_H8

¹¹² Prática comum no meio hacktivista baseada em pesquisas e divulgações públicas de dados pessoais de uma pessoa

homogênea, levando o homem a um comportamento de sociabilidade e cortesia¹¹³, ao qual o forte, o extraordinário não somente se iguala em valor, mas age como se o fraco fosse valoroso e superior (SIMMEL,2006, p.71).

Assim, é gerada uma associação entre iguais em simetria e equilíbrio, já que negam o que os diferencia assumindo uma única voz, no que Simmel (2006) chama de um jogo de faz de conta, no qual todos são iguais e cada um é especialmente honrado.

4.3.3 *Pool's closed. The Internet Hate Machine.*

Em 2006 usuários do canal /b/ promoveram uma invasão no jogo online “*Habbo Hotel*”, o que pode ser considerado uma de suas primeiras grandes operações: a *Pool's Closed* (a Piscina está Fechada).

Membros do *4chan* criaram avatares, semelhantes ao personagem Jules Winnfield interpretado pelo ator Samuel L. Jackson no filme *Pulp Fiction* (1994), trajando ternos, seguindo o estilo do movimento *Black Power*. Estes usuários se denominaram como */b/lockers* (pois a invasão foi estruturada no canal /b/), criando bloqueios em entradas de salas e principalmente na piscina, com objetivo de impedir que usuários do jogo fossem capazes de entrar em tais ambientes. Foi o momento em que percebem que quantidade de pessoas envolvidas no /b/ era maior do que até eles mesmos imaginavam.

No entanto, toda história tem dois lados, neste caso, muitos lados. Se alguns invadiram o *Habbo Hotel* por diversão, alguns membros apontam que invadiram por uma razão: em julho de 2006 houve o boato no *4chan* que moderadores do jogo tinham tendência a banir usuários de acordo com a cor da pele dos avatares, e por isso criaram bloqueios e entradas de salas e piscinas. Outra explicação, é que para esses primeiros Anonymous, a Internet não deve ser levada tão a sério, como muitos usuários do jogo levavam.

Por outro lado, isso fez com que esse substantivo coletivo do *Anonymous* se tornasse um meme popular, caracterizando em seu início um grupo descentralizado que passa a invadir e atacar uma variedade ainda maior de alvos (KNUTILLA,2011).

Ainda em 2006, segundo Olson (2014), são estabelecidas “As regras da Internet”¹¹⁴ em uma conversa do IRC¹¹⁵.

¹¹³ No caso de *chan*, de brincadeiras.

¹¹⁴ Regras disponíveis em ><https://archive.org/stream/RulesOfTheInternet/RulesOfTheInternet.txt>

¹¹⁵ *Internet Relay Chat* (Bate papo interativo da Internet), segundo Olson (2014) existem desde o final da década de 1980, permitindo que usuários possam conversar uns com os outros. Olson (2014) aponta que redes como a

Originalmente com 47 regras, dentre as quais as primeiras são: “*Regra 1*: Não fale sobre o canal /b/. *Regra 2*: Não fale sobre o canal /b/¹¹⁶ *Regra 3*: Nós somos Anonymous. *Regra 4*: Anonymous é uma Legião. *Regra 5*: Anonymous nunca perdoam. *Regra 6*: Anonymous podem ser horríveis, insensíveis, monstros indiferentes. *Regra 7*: Anonymous continuam disponíveis para entregas” e obviamente a *Regra 47* é “A piscina está sempre fechada”. Tais regras abrangem a etiqueta cultural dos painéis ou canais dos *chans*.

A popularidade do Anonymous aumentou quando o canal FOX11 (FOXNews) exibiu uma reportagem que os tornou “públicos”¹¹⁷ em 26 de julho de 2007, os chamando publicamente de Anonymous. O canal utilizou de termos pejorativos para descrevê-los, tais como “Hackers com esteroides” (*sic*), “Terroristas domésticos” (*sic*), que “invadem jogos infantis” (*sic*), afirmando que seus atos são sarcásticos e sádicos somente por “*lulz*” (uma variação de *LOL* : *laughing out loud* “rindo alto”), isto é, por pura diversão ou trollagem (brincadeiras, chacotas e provocações), gerando uma verdadeira “Máquina de ódio da Internet” (*sic*) (*Internet Hate Machine*). O “Anonymous” respondeu a reportagem pouco tempo depois¹¹⁸.

Obviamente, a definição de “*The Internet Hate Machine*” é motivo de risadas para muitos usuários até hoje. “Moot”, em declaração a BBC¹¹⁹, reforça que mesmo que os trolls de sua comunidade fossem acusados de fazer da internet uma ‘*Internet Hate Machine*’, “na maioria das vezes é muito mais latido do que mordida”.

4.3.4 Chanology

Em 14 de janeiro de 2008, um vídeo de ator Tom Cruise postado no Youtube ¹²⁰ falando de ideologias da Igreja de Cientologia acabou se tornando um meme. No dia 16 de janeiro, a Igreja entra na justiça para que o vídeo fosse retirado do ar se utilizando da Lei de Direitos Autorais.

IRC AnonOps, atraem diversas pessoas interessadas no Anonymous, e seus operadores (moderadores) são encarados “como um indicador de alto status social”.

¹¹⁶ As duas primeiras regras teriam sido inspiradas no filme “O Clube da Luta” (1999) em que A primeira regra do Clube da Luta é: você não fala sobre o Clube da Luta. A segunda regra do Clube da Luta é: você não fala sobre o Clube da Luta.

¹¹⁷ Disponível em: <http://www.youtube.com/watch?v=DNO6G4ApJQY>

¹¹⁸ Disponível em: <https://www.youtube.com/watch?v=RFjU8bZR19A>

¹¹⁹ <http://www.bbc.co.uk/news/magazine-10520487>

¹²⁰ https://www.youtube.com/watch?v=UFBZ_uAbxS0

Em resposta, algumas pessoas tomaram o ato ofensivo, contra a liberdade da Internet e resolveram agir postando, assim, uma das primeiras mensagens declaradamente como Anonymous:

“Olá Cientologia. Nós somos Anonymous. Ao longo dos anos temos assistido vocês. Suas campanhas de desinformação, repressão da dissidência, sua natureza litigiosa e isso nos chamou atenção. Com o vazamento do vídeo mais recente em circulação e a confiança daqueles que confiam em vocês, que você chama de líder, ficou claro para nós. O Anonymous decidiu que sua organização deve ser destruída. Para o bem de seus seguidores, para o bem da humanidade e para os risos vamos expulsa-los da Internet e sistematicamente dismantelar a Igreja de Cientologia de sua forma atual. (...) Seus métodos, hipocrisia e a ingenuidade da sua organização soa como sua sentença de morte. Você não pode se esconder, estamos em todos os lugares. Não podemos morrer, somos para sempre. Estamos ficando maiores a cada dia pela força de nossas ideias (...). Se quiser outro nome para o seu adversário nos chame de Legião, porque somos muitos. (...) O conhecimento é Livre. Nós somos Anonymous. Nós somos uma Legião. Nós não perdoamos. Nós não esquecemos. Espere por nós”¹²¹ (ANONYMOUS, 2008)

A palavra “Legião”, segundo o dicionário Michaelis (2016), refere-se a um grande número de pessoas, animais ou coisas; uma multidão. Tal termo, frequentemente utilizado pelo Anonymous, tem pelo menos três possíveis origens: a primeira, uma analogia aos *Borg*, vilões da série Jornada nas Estrelas. Borg é uma raça que tem como característica e arma o coletivismo e a capacidade de dividir a mesma consciência, de forma que a individualidade é eliminada.

A segunda hipótese segue o sentido bíblico em referência a um exército de anjos ou demônios (MICHAELIS, 2016) e teria sido extraído de trechos como do evangelho de Marcos (5:9): “E perguntou-lhe: Qual o teu nome? Respondeu ele: Legião é meu nome, porque somos muitos” (OLSON; 2014). Uma legião faria ainda ligação com a maior divisão do exército romano, que teria começado a crescer no final do século II a.C e chegou a atingir 6.000 homens.

Em declaração justificando o Chanology, o Anonymous afirma:

“Você não pode esconder; estamos em todos os lugares. Nós não podemos morrer; Nós somos estamos aqui para sempre. Estamos ficando maiores a cada dia - unicamente pela força das nossas ideias, maliciosas e hostis como frequentemente são. Se você quiser um outro nome para o seu adversário, então pode nos chamar de Legião, porque somos muitos.”¹²² (ANONYMOUS; 2008)

É interessante ressaltar que o Anonymous é cercado de uma série de termos militares, como por exemplo, como *Tango Down* (refere-se a um site que foi derrubado). Originalmente, é um termo militar que quer dizer que o alvo foi abatido. Para alguns membros pesquisados, não há diferença entre derrubar um site do governo ou fazer um protesto em frente de uma

¹²¹ Texto na íntegra e vídeo original <https://www.youtube.com/watch?v=JCbKv9yiLiQ>

¹²² *You cannot hide; we are everywhere. We cannot die; we are forever. We're getting bigger every day--and solely by the force of our ideas, malicious and hostile as they often are. If you want another name for your opponent, then call us Legion, for we are many.*

empresa: o efeito para eles é o mesmo. O Anonymous se autodenomina como “O Primeiro Exército da Internet”.

Outro detalhe que chamou a atenção durante as entrevistas, foi em referência a uma chamada “Unidade Tática Móvel” a Anonomobile, localizada em Washington D.C. Em entrevista via Skype¹²³ com a operadora da unidade, a ativista Sheriff Sands afirmou que a Anonomobile também é conhecida como *Anon Goliath* (Anon Golias), para ajudar na divulgação da operação MMM (*Million Mask March*), que acontece anualmente todo 05 de novembro ao redor do mundo; e em defesa das causas de Chelsea Bradley Manning, Edward Snowden e Julian Assange.

Durante a entrevista, questionamos que não faria sentido a unidade ser chamada de “Golias”, afinal, segundo passagens bíblicas, teria sido Davi que derrotou o gigante, não o contrário e ela afirmou que o nome faz referência a posturas tomadas pelo seu próprio Governo, não ao Anonymous. Sands afirma que recebe ataques frequentes em seu site, pois não omite sua identidade. A não omissão, segundo ela, é em função da localização da Anonomobile (geralmente estacionada próxima a NSA) e do receio de que, caso algo aconteça a ela, ninguém saiba sua identidade.



Ilustração 18: Anonomobile

Fonte: anomobile.com

A terceira hipótese pelo frequente uso do termo “Legião” pelos Anonymous refere-se a um traço relacionado à história da própria cultura hacker, oriunda da matéria “*Fanatic Life and Symbolic Death Among the Computer Bums*”, publicada em 7 de dezembro de 1972 na revista

¹²³ Não é um meio de comunicação frequentemente utilizado pelo Anonymous

Rolling Stone¹²⁴, podendo também ser relacionada a origem do gênero cyberpunk (STERLING;1992)

Retomando ao Chanology, em 1º de fevereiro de 2008 é lançado um Código de Conduta com 22 regras¹²⁵ dos Anonymous para protestos nas ruas. Conhecer esse código permite identificar a própria postura nas ruas que diferenciam um Anonymous de um “mascarado”.

É realmente um exercício de relativização de suas regras, quem os vê sem conhecimento tende a criar rótulos e até mesmo classifica-los como “desviantes” (Becker,1963). Mas de fato, cria-se um perfil muito peculiar dentro de quem segue tais regras:

“ Regra nº 0: Regras #1 e #2 da Internet ainda se aplicam. Os seus memes não são, neste momento, algo que o mundo real pode apreciar. Embora falar de um meme com um colega Anonymous é aceitável, o foco é manter esse conhecimento mínimo. Regra nº 1: Fique Tranquilo. Regra nº 2: Fique tranquilo, especialmente se for provocado. Você é um embaixador do Anonymous. Embora indivíduos presentes tentem atrapalhar a sua demonstração e isso vai dar nos nervos, você não deve perder a calma. Se o fizer, irá prejudicar o protesto e manchar a reputação do Anonymous. Regra nº 3: Deve-se cumprir as ordens de oficiais da lei acima de tudo. Fazer o contrário é prejudicial para a manifestação como um todo e poderá comprometer o seu desempenho como um ser humano. Não solicite números (identificação) do crachá de oficiais, a menos que você seja tratado de uma forma abusiva, pois isso pode enfurecer os oficiais. Regra nº4: Informe aos oficiais de sua cidade, pois em muitas jurisdições possuem regras sobre protestos públicos e pedem que sejam notificadas sua ocorrência. Conheça essas regras e as siga. Regra 5: Fique do outro lado da rua em frente ao alvo do protesto. Regra6: na ausência de uma rua, procure barreiras naturais que possam protegê-lo caso haja hostilidade de sua presença. Regra 7: Fique em propriedade pública, para que não seja acusado de invasão. Regra 8: Sem violência. Regra 9: Sem armas. O protesto é um evento pacífico você não precisa delas. Regra 10: Sem álcool. Evite ir alcoolizado, pois isso pode causar a violação das regras 1 e 2. Regra 11: Sem pichação, destruição ou vandalismo. (...) (ANONYMOUS, 2008)

As regras feitas para protegê-los ainda os adverte que não devem fazer nada “estúpido” (*Sic*) que prejudique o protesto, manche o nome da organização e de que fato sejam presos. Informam que eles são uma legião e não devem ficar sozinhos. E ainda orientam que deveriam ter apenas um megafone para que não cause confusão de informações, seguindo um código da vestimenta que fizesse com que as pessoas os levasse a sério (é comum ver Anonymous de ternos em protestos).

Ainda segundo as regras, eles devem cobrir o rosto para evitar identificação por vídeos, usando máscaras somente se a jurisdição local permitir; desenvolver e distribuir panfletos explicativos além da exibição de faixas; documentar toda manifestação, para posteriores divulgações dos vídeos do evento para que outros sigam o exemplo. (ANONYMOUS;2008)

Justamente em relação a este código conduta, que os Anonymous estavam prestes a romper a barreira do real-virtual. Não se tratava de um encontro presencial (fechado) entre

¹²⁴ Ver detalhes em: 3.4 “Eles são uma legião”: os hackers de hardware

¹²⁵ <https://www.youtube.com/watch?v=-063clxiB8I>

membros de uma comunidade virtual. Não era a sociedade civil organizada se utilizando da Internet para tomar decisões. Se tratava de uma comunidade virtual, com códigos próprios, de um personagem coletivo inserido no ciberespaço, que reconhecia o fato de que “mundo real” não é o deles, então eles deveriam respeitar suas regras.

A série de protestos contra as práticas da Igreja de Cientologia, articuladas no canal /b/ do 4chan, se espalhou em diversos países e iniciou uma mobilização segundo Fontanella (2010) que mesclava a defesa da liberdade, com “boas risadas”. Nesse momento, eles escolhem uma máscara que representaria o anonimato da Internet, na vida real:

Qual a única máscara que conhecemos ou que já fizemos piada dela? A máscara de Guy Fawkes. Sabe a última cena onde todos estão usando a máscara dele? Isso lembra muito que o Anonymous pensa que ele é. Queríamos representar o anonimato de algum jeito, quando passasse para a vida real. Acho que a máscara de Guy Fawkes, era uma das coisas mais naturais a acontecer. Era a ideia de que nenhum de nós era tão cruel quanto todos nós. Você tem essa multidão de pessoas do Anonymous, que vão lutar contra algo maior e vencer”. (VITALE in KNAPPENBERGER; 2012)

Em 10 de fevereiro de 2008, os usuários vão enfim para as ruas contando com cerca de 6.000-7.000 pessoas em 100 cidades ao redor do mundo (COLLEMAN,2014) que compareceram para a “Operação Chanology” para o espanto dos organizadores.



Ilustração 19: Anonymous durante o Chanology¹²⁶
Fonte: *Jeremy Azevedo*

Não ocorreram apenas manifestações nas ruas, muitos Anonymous também atacaram a Igreja de cientologia *online*, com *black fax* (comando para que o fax imprima inúmeras páginas pretas), entregas de pizza, DDoS nos sites, etc. A Igreja declarou que considerava o Anonymous um grupo de ciberterroristas que propagam intolerância e preconceito contra cientologistas.

Mas a ideia segundo alguns usuários era bem diferente de uma motivação ou manifestação política. Primeiramente, era para conseguir identificar outros integrantes dos chans, mas a ideia central era basicamente a seguinte: Eles queriam ir para frente da Igreja de

¹²⁶ É importante ressaltar na imagem 3, a presença do meme “*long cat is loong*” caracterizando uma identificação de um usuário do 4Chan a esquerda, e claro, a direita uma caracterização do 4chan

Cientologia, com a máscara do V, para mostrar que a Igreja era um “*Epic Fail*”. Afinal, “nada é para ser levado tão a sério.” (Regra número 20).

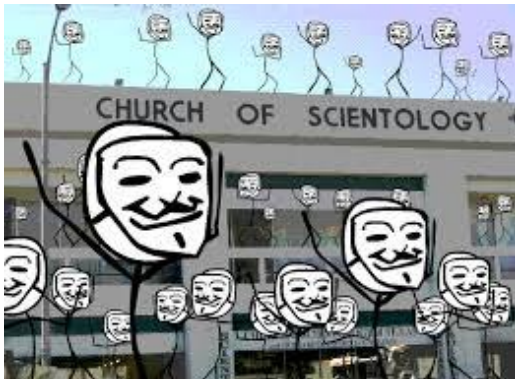


Ilustração 20: Epic Fail Guy
Fonte: Internet

Definitivamente, muitas pessoas levaram o ato realmente a sério e o *Anonymous* passou a utilizar “*We are Anonymous, We are Legion. We do not forgive. We do not forget. Expect us*” como seu lema. E a máscara, que era inicialmente uma proteção, se tornou gradativamente um dos símbolos do *Anonymous*, juntamente com o terno e a imagem de um indivíduo com uma “interrogação” que representa o anonimato.

Segundo Barret Brown *in* Knappenberger (2012), os atos contra a Igreja de Cientologia geraram confusão entre os membros; enquanto uma parte dos integrantes dos *chans* desejava manter um grupo pequeno, outra parcela desejava ampliar seu ativismo, se autoproclamando “O primeiro Exército da Internet”. Esta segunda parcela, segundo Coleman (2014), formou subgrupos, seguindo os caminhos do ativismo enquanto outros, seguiram o lado da transgressão¹²⁷.

Em 21 de janeiro de 2015, em comunicado oficial do 4Chan, Moot - o único administrador do site até então - anunciou sua aposentadoria, segundo ele por motivos pessoais, não financeiros, apresentando a comunidade em números: 42 bilhões de visualizações, 1,7 bilhões de *posts*, 1 bilhão de visitantes, somando 2,838 *terabytes* de dados mensais. Segundo o fundador, o site permanece na administração de 105 voluntários. Em 7 de março de 2015 Poole começou a trabalhar no Google com objetivo de reestruturar a rede social Google+.

O *Anonymous* perde dia após dia as características do *4Chan*, algo que um dos operadores de um perfil virtual *Anon18* lamenta em entrevista:

¹²⁷ Gabriela Coleman (2014) afirma que produzir vídeos e publicidade são processos legais, enquanto outros, como praticar DDos (Distributed Denial of Service, isto é, Ataque de Negação de Serviço) são considerados ilegais.

Os *Anonymous* do 4chan não são os meus favoritos, mas é aonde estão nossas raízes. O *Anonymous* para mim é uma ferramenta que pode ser usada para o bem ou para mal, depende do usuário (...) *Anonymous* no 4chan é o mesmo que dar uma arma a um gato, aqueles caras são doidos, mas engraçados. *Anonymous* tem mudado e deixado de ser engraçado, e isso é lamentável (...) costumamos tentar ser engraçados, nos divertir, mas tudo tem se tornado cada vez mais sério. Eu sei que em alguns lugares ainda é possível ser divertido mas torna tudo mais difícil para se conseguir respeito. Precisamos ser engraçados novamente.

Ainda segundo o *Anon18* enxergar o *Anonymous* como um tipo de “ferramenta” que pode ser utilizada por qualquer indivíduo, seria uma possível explicação para que as pessoas de uma forma geral, compreendessem algumas das atividades feitas em nome do *Anonymous* e que são completamente aleatórias, sem nenhuma relação com o ciberativismo ou com o hacktivismo.

Ao longo do tempo, o *Anonymous* ganhou experiência em manifestações e protestos de rua e também intensificou suas atividades hacktivistas online. Nem todo *Anonymous* é um hacker e a recíproca também é verdadeira. Da mesma forma que nem todo mundo que utiliza a máscara é necessariamente um *Anonymous*.

4.3.5 O homem e seu passado: Por que da máscara de Guy Fawkes?

Com a proporção tomada pelo *Anonymous* após 2008, percebemos que suas definições se modificam muito rapidamente, algo que os torna um desafio se tratando de pesquisas acadêmicas que tentam acompanhar o ritmo de mudança de eventos ou comunidades *online*. No entanto, quanto mais se distanciam da origem dos chans, mais os valores apresentados ou moldados em sua origem se dispersam ou desaparecem.

Nosso objetivo não “é construir o *Anonymous*”, mas analisar as fundamentações históricas de um mesmo personagem em diferentes formas, que obscurecem transformam o objeto de difícil interpretação, compreender suas origens nos faz ver que existe algo diferente, ou como afirma Foucault:

“(…) se o genealogista tem o cuidado de escutar a história em vez de acreditar na metafísica, o que é que ele aprende? Que atrás das coisas há ‘algo inteiramente diferente’; não seu segredo essencial e sem data, mas o segredo que elas são sem essência, ou que sua essência foi construída peça por peça a partir de figuras que lhes eram estranhas. (...) O que se encontra no começo histórico das coisas não é a identidade ainda preservada da origem – é a discórdia entre as coisas, é o disparate. (FOUCAULT, 2010, p.17).

Nos últimos 400 anos, a imagem de Guido Fawkes apareceu em diversos momentos de formas diferentes:

Em um primeiro momento, foi em sua origem; sua história original, ocorre em um período conturbado da história da Inglaterra, narrando a trajetória de um católico extremista,

um dos membros da Conspiração da Pólvora, que ao lado de outros 12 conspiradores¹²⁸, com intuito de matar o Rei James I (Protestante)¹²⁹ e restaurar um monarca católico ao trono. O plano era explodir o Palácio de Westminster durante a reunião da Câmara dos Lordes na data em que o Rei James I estaria presente no local. (SPINK;1901)

Porém, em 26 de outubro de 1605, Lorde Monteagle cunhado de Francis Tresham, um dos 12 conspiradores, recebeu uma carta anônima¹³⁰ pedindo que Monteagle não fosse ao Parlamento no dia 05 de novembro, levando a uma varredura minuciosa nas galerias subterrâneas do Palácio de Westminster.

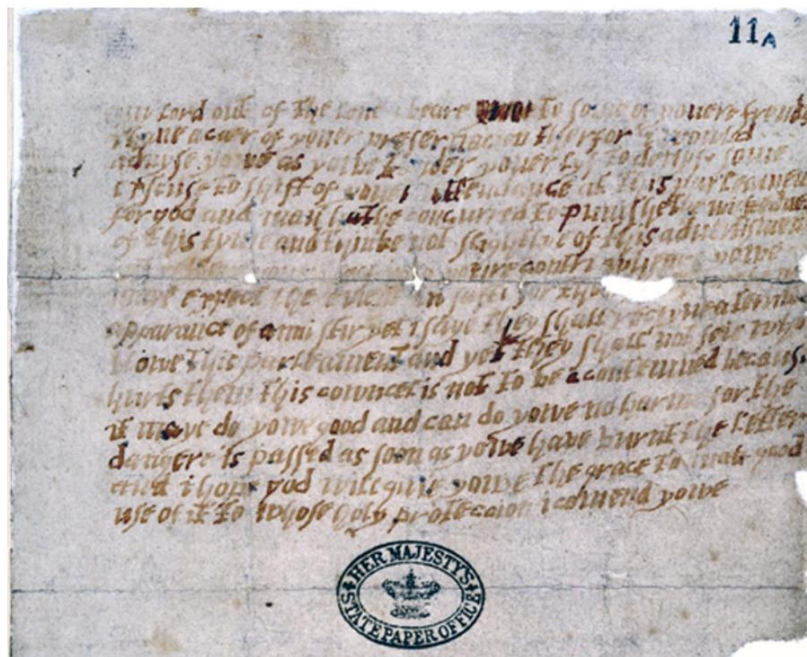


Ilustração 21: Carta para o Lorde Monteagle (26 de outubro de 1605)
Fonte: BBC

Em 05 de novembro de 1605, Guido Fawkes foi preso após ser pego escondendo cerca de 36 barris de pólvora na parte subterrânea do Parlamento. A data de sua prisão, 5 de novembro foi instituída como uma festa de comemoração da sobrevivência do rei, mas ficou conhecida como a “Noite das Fogueiras” (*Bonfire Night*) ou *Guy Fawkes Night*. Ainda hoje a data é

¹²⁸ Além de Guy Fawkes, faziam parte da conspiração: Robert Catesby, John Wright, Thomas Wintour, Thomas Percy, Robert Keyes, Thomas Bates, Robert Wintour, Christopher Wright, John Grant, Ambrose Rookwood, Sir Everard Digby e Francis Tresham

¹²⁹ James I foi pai de Carlos I, conhecido historicamente por ser um monarca tirano, que travou uma disputa pelo poder contra o parlamento Inglês, levando a Guerra Civil Inglesa (1642 – 1651) e a condenação à morte do rei. Como consequência a Inglaterra se estabeleceu como um governo republicano entre 1649 e 1660. Em 1651, Thomas Hobbes publica seu *Leviatã*.

¹³⁰ Transcrição da carta : *My Lord, devise some excuse to shift your attendance at this Parliament, for God and Man hath concurred to punish the wickedness of this time. Though there be no appearance of any stir, yet I say they will receive a terrible blow and yet they shall not see who hurts them. The danger is passed as soon as you have burnt this letter. I hope to God that you the Grace to use it.*

celebrada queimando bonecos em fogueiras, representando Fawkes, com o tradicional verso: "Lembraí, lembraí do cinco de novembro. A pólvora, a traição, a conspiração. Não sei de uma razão para que a traição da pólvora. Seja algum dia esquecida. ”¹³¹ (SPINK;1901; BBC;2001)



Ilustração 22 : Bonfire Nigh
Fonte: AFP

A imagem apareceu pela segunda vez na década de 1980 pelos traços de Alan Moore e David Lloyd no HQ *V for Vendetta*. Quando começou a ser escrita, os conservadores estavam a frente do Governo Inglês, representados pela figura de Margaret Thatcher, eleita em 1979. O autor, afirma que demorou cerca de 5 anos para completar a história e disse ter ficado intrigado com as feições de Fawkes e também por sua história, o que o levou a escolhê-lo para ser a imagem de seu anti-herói V.

A história do HQ começa em Londres em um cenário futurista, típico de contos e livros da década de 80, pós Terceira Guerra Mundial, em um cinco de novembro com uma população subjugada, vivendo em campos de concentração e regida por um governo fascista (que perseguia negros, homossexuais, muçulmanos, imigrantes). Nesse ambiente que V conhece a jovem Evey Hammond que o assiste explodir o Parlamento recitando os tradicionais versos da conspiração “Lembraí, lembraí do cinco de novembro(...)”.

¹³¹ *Remember, remember the fifth of November, Gunpowder treason and plot. We see no reason. Why gunpowder treason. Should ever be forgot*

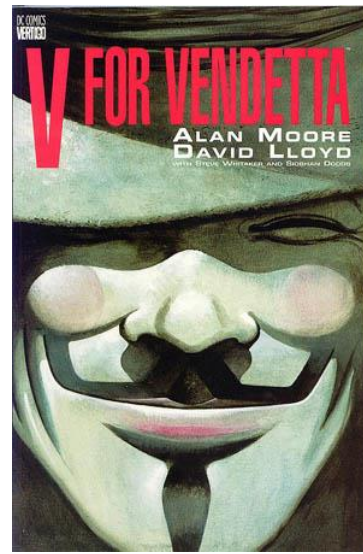


Ilustração 23: Fawkes/ V

Fonte: DC Comics Vertigo (Ilustrações de David Lloyd, roteiro de Alan Moore)

Posteriormente, toda a história se desenvolve em derrubar o governo por meio de uma ascensão popular, iniciada pela vingança pessoal do personagem V contra as pessoas diretamente ou não envolvidas nos experimentos e testes químicos aos quais ele fora submetido no passado¹³² e na construção da personalidade de Evey.

O terceiro momento em que a imagem aparece é na adaptação para os cinemas em 2005 do HQ *V for Vendetta*, com direção de James McTeigue e roteiro adaptado por Andy e Lana Wachowski, com Natalie Portman no papel de Evey e Hugo Weaving no papel de V.

Na adaptação foi recriada boa parte dos cenários e parte das frases muito difundidas entre muitos Anonymous e manifestantes: “Nenhum de nós é tão cruel quanto todos nós” ou a passagem do HQ que diz: “Você pretendia me matar? Não há carne ou sangue dentro deste manto para morrerem. Há apenas uma ideia. E ideias são a prova de bala.”¹³³ (V DE VINGANÇA, 1983, p.238). Além da clássica “O povo não deve temer seu governo. O governo deve temer seu povo.” (*sic*)

¹³² É interessante ressaltar que todos os capítulos do HQ comecem com a letra V (Voz, Vítimas, Vaudeville, Versões, Vox Populi e assim por diante). Na verdade, V não representa “Vingança” ou a letra, mas sim “5” em números romanos, que era o número do quarto que V ficava instalado. A ideia de que ele luta contra um sistema opressor é mais evidente no filme adaptado para os cinemas em 2005.

¹³³ Passagem adaptada na famosa cena hollywoodiana na qual a personagem Creedy atira em V repetidas vezes dizendo “-Morra! Morra! Porque você não morre? Porque não morre? E V responde “Embaixo dessa máscara há mais do que carne. Atrás dessa máscara há uma ideia, e Sr. Creedy .Ideias são à prova de bala.” (*sic*)



Ilustração 24: Cartazes do filme V de Vingança
Fonte: Reprodução

Os outros momentos aos quais a imagem aparece são como uma brincadeira dos *chans* com o meme “*Epic Fail Guy*”, posteriormente como forma de identificação dos membros dos *chans* e omissão de suas identidades quando vão para as ruas durante o Chanology, como forma de alguns Anonymous representarem seu ciberativismo e hacktivismo, juntamente com outras iconografias (COLLEMAN;2014).

E, por fim, a utilização da máscara em protestos e manifestações de rua como forma de demonstrar sua indignação contra seus governantes (fazendo mais alusão ao filme do que ao Anonymous em si).

Atualmente, as manifestações do dia 05 de novembro coincidem duas datas: a *Bonfire Night* e a MMM (*Million Mask March*), uma manifestação dos Anonymous que ocorre anualmente, com uma média de 670 cidades em todo mundo.



Ilustração 25 :Mapa da MMM (2015)
Fonte: Anonymous

Como supostamente ocorre esse processo de transição de um católico extremista, para um anarquista e posteriormente como um símbolo controverso de democracia, liberdade e resistência para tantos? Historicamente, diversos autores que apontam essa característica da sociedade é oriunda de sua estreita relação dos homens com seu passado. Thomas Hobbes em seu *Leviatã* (1642) aponta a importância desse processo, descrevendo que quanto mais tempo se passa, menores são as lembranças que certo objeto representou:

E quando qualquer objeto é afastado dos nossos olhos, muito embora permaneça a impressão que fez em nós, outros objetos mais presentes sucedem-se e atuam em nós, e a imaginação do passado fica obscurecida e enfraquecida, tal como a voz de um homem no ruído diário. Daqui se segue que quanto mais tempo decorrer desde a visão ou sensação de qualquer objeto, tanto mais fraca é a imaginação. Pois a contínua mudança do corpo do homem destrói com o tempo as partes que foram agitadas na sensação, de tal modo que a distância no tempo e no espaço têm ambas o mesmo efeito em nós. Pois tal como à distância no espaço os objetos para que olhamos nos aparecem minúsculos e indistintos em seus pormenores e as vozes se tornam fracas e inarticuladas, assim também, depois de uma grande distância de tempo, a nossa imaginação do passado é fraca e perdemos, por exemplo, muitos pormenores das cidades que vimos, das ruas, e muitas circunstâncias das ações. Esta sensação diminuída, quando queremos exprimir a própria coisa (isto é, a própria ilusão), denomina-se imaginação, como já disse anteriormente; mas, quando queremos exprimir a diminuição e significar que a sensação é evanescente, antiga e passada, denomina-se memória. Assim a imaginação e a memória são uma e a mesma coisa, que, por razões várias, tem nomes diferentes (HOBBS;2001, p. 12)

Karl Marx, outro autor que descreve em seu clássico *18 de Brumário*, de 1852, que Hegel comenta que grandes fatos e histórias se repetem duas vezes, a primeira vez como tragédia e a segunda como farsa (Marx, 2011, p.25). E prossegue afirmando que:

Os homens fazem sua própria história, mas não por livre e espontânea vontade, pois não são eles que escolhem as circunstâncias sob as quais ela é feita, mas estas lhes foram transmitidas assim como se encontram. A tradição de todas as gerações passadas é como um pesadelo que comprime o cérebro dos vivos. E justamente quando parecem estar empenhados em transformar a si mesmos e as coisas, em criar

algo nunca antes visto, exatamente nestas épocas de crise revolucionária, eles conjuram temerosamente a ajuda dos espíritos do passado, tomam emprestados os seus nomes, as suas palavras de ordem, seu figurino, a fim de representar com essa venerável roupagem tradicional e essa linguagem tomada de empréstimo, as novas cenas da história mundial. (MARX, 2011, p.25)

Marx faz uma analogia de como essa relação poderia ser rompida dando um exemplo de uma pessoa que aprende um novo idioma e o traduz com palavras de seu idioma original (isto, é, está ligada ao seu passado), mas quando consegue esquecer sua própria língua e utilizar apenas a nova, ele terá de fato assimilado o espírito dessa última e poderá produzir livremente. (Marx, 2011, p.26).

Analisando e elevando esse processo de construção de significado da máscara, ou do próprio personagem (Guy Fawkes) ao nível das multidões, autores como Lebon (1895, p. 30-31) compreendem que cada civilização possui uma limitação de suas ideias fundamentais que são raramente renovadas, e que as grandes mudanças costumam ocorrer quando acontece um processo de modificação dessas ideias, podendo perturbar sua ordem por duas categorias: a primeira como uma característica de estar sob o entusiasmo do momento (por um indivíduo ou doutrina) e a segunda por um processo de ideias fundamentais que geram estabilidade, como ideias religiosas, democráticas e sociais (LEBON, 1895, p.30).

A importância de uma ideia não está em seu valor hierárquico, mas sim nos efeitos que essa ideia irá produzir, o que irá caracterizar fatores essenciais de conduta (como o que ocorre com o próprio Estado). Para Lebon: “Mesmo que a ideia sofra as modificações que a tornam acessível às multidões, só atuará quando, por processos capazes de penetrar no inconsciente e passar a ser um sentimento. Esta transformação é geralmente muito demorada.” (LEBON, 1895, p.31)

Segundo o autor, nem é preciso que séculos passem sobre os heróis para que a imaginação das multidões lhes transforme em lendas (ou não), como foi o caso de Napoleão:

No tempo dos Bourbons, Napoleão tornou-se um filantropo, um liberal, um ser quase idílico, amigo dos pobres, que, no dizer dos poetas, nas suas choupanas o recordariam por muitos anos. Trinta anos depois, o herói bom e terno torna-se um déspota sanguinário, usurpador do poder e da liberdade, que sacrificara três milhões de homens à sua ambição. Atualmente a lenda continua a transformar-se. E quando alguns séculos tiverem passado sobre ela, os sábios do futuro, perante essas narrativas contraditórias, porão talvez em dúvida a existência do herói, como nós pomos em dúvida a de Buda, e verão nele apenas um mito solar ou um desenvolvimento da lenda de Hércules. (LEBON, 1980,p.24)

Berman (1982) complementa que a relação do homem com seu passado é um processo típico de uma mentalidade moderna, em que a busca dessas imagens no passado funcionam como uma paródia:

Outro tipo de mentalidade moderna se dedica à paródia do passado: esse “precisa da história porque a vê como uma espécie de guarda-roupa onde todas as fantasias estão guardadas. Ele repara que nenhuma realmente lhe serve” — nem primitiva, nem

clássica, nem medieval, nem oriental — “e então continua tentando”, incapaz de aceitar o fato de que o homem moderno “jamais se mostrará bem trajado”, porque nenhum papel social nos tempos modernos é para ele um figurino perfeito (BERMAN, 1982, p.22)

Segundo Giddens (1990)

Sociedades tradicionais, o passado é venerado e os símbolos são valorizados porque contêm e perpetuam a experiência de gerações. A tradição é um meio de lidar com o tempo e o espaço, inserindo qualquer atividade ou experiência particular na continuidade do passado, presente e futuro, os quais, por sua vez, são estruturados por práticas sociais recorrentes (Giddens, 1990, pp. 37-8).

Compreendemos assim que o processo de construção histórica do sentido com o qual a máscara é utilizada pelo Anonymous e da forma que imagem de Fawkes é vista pelas massas, funcionam como um elo que liga o presente ao passado, dando um sentido único que propiciou força em relação a sua imagem.

O objeto se debruça conscientemente ou não em uma profunda ligação com o passado, com a imagem de Guy Fawkes vista no âmbito das multidões, que buscam de maneira frequente dar um sentido para suas próprias ações, ou neste caso da utilização da máscara, assimilando e criando um novo sentido condizente com o espírito da época, produzindo um sentido livremente.

Alguns indivíduos que compartilham a história dos chans ou do próprio ciberespaço, afirmaram durante as pesquisas, que para muitos Anonymous que utilizam a máscara, esta não tinha significado algum a não ser de uma forma de “identificar” membros do próprio Anonymous que partilham os mesmos pontos de vista em suas próprias comunidades ou manifestações dentro e fora da Internet ou simplesmente para ocultar suas identidades durante os protestos.

Foi possível acompanhar a partir de 2008, um processo de construção de sentido em torno da própria máscara, ao qual, pessoas pouco (ou nada) relacionadas com os chans, passaram a buscar um significado mais profundo a respeito da máscara e do que ela viria a representar historicamente.

Certamente, apresentar, mesmo que de maneira superficial, os diferentes sentidos que a máscara carrega, não é um foco relacionado ao meio hacker, mas um traço do Anonymous em si. Acima de tudo, é a personificação do anonimato no mundo real. O que observamos é que pessoas mais inseridas dentro das lógicas do ciberespaço enxergam a máscara¹³⁴ de uma forma diferente daquelas mais inseridas nos valores do mundo (real) e sua incansável busca por sentidos.

¹³⁴ É possível ainda acompanhar situações do uso da máscara como uma forma de expressão de arte.

4.3.6 Critérios utilizados para seleção de amostras

Realizar entrevistas com hackers, em especial do *Anonymous*, exigiu boas escolhas, se tratando de estratégias e metodologias dentro das Ciências Sociais. Nossa primeira preocupação foi compreender e respeitar valores culturais que foram construídos ao longo do tempo, aos quais tanto a comunidade hacker quanto os *Anonymous* estão de fato inseridos. Os resultados de tais pesquisas foram apresentados ao longo dos primeiros capítulos dessa dissertação, oferecendo uma base para trabalhos que podem ser eventualmente desenvolvidos.

Se tratando de estratégias metodológicas, buscamos uma bibliografia que oferecesse algum tipo de estratégia ao qual poderíamos eventualmente aplicar em nossa pesquisa, para um levantamento de hipóteses e direcionamento das perguntas.

Existem poucos trabalhos quantitativos se tratando do meio hacker e os trabalhos referentes ao *Anonymous* são escassos. Um dos mais recentes e importantes vem sendo desenvolvido por Yevgeniy Golovchenko na Universidade de Copenhague, que inicialmente mapeou cerca de 2.770 páginas do *Anonymous* somente no Facebook, gerando um resultado de 22.2 milhões de “curtidas”, reconhecendo que é um tamanho mínimo, se tratando de toda a rede que o *Anonymous* desenvolveu também em outras redes sociais dentro e fora da Internet.

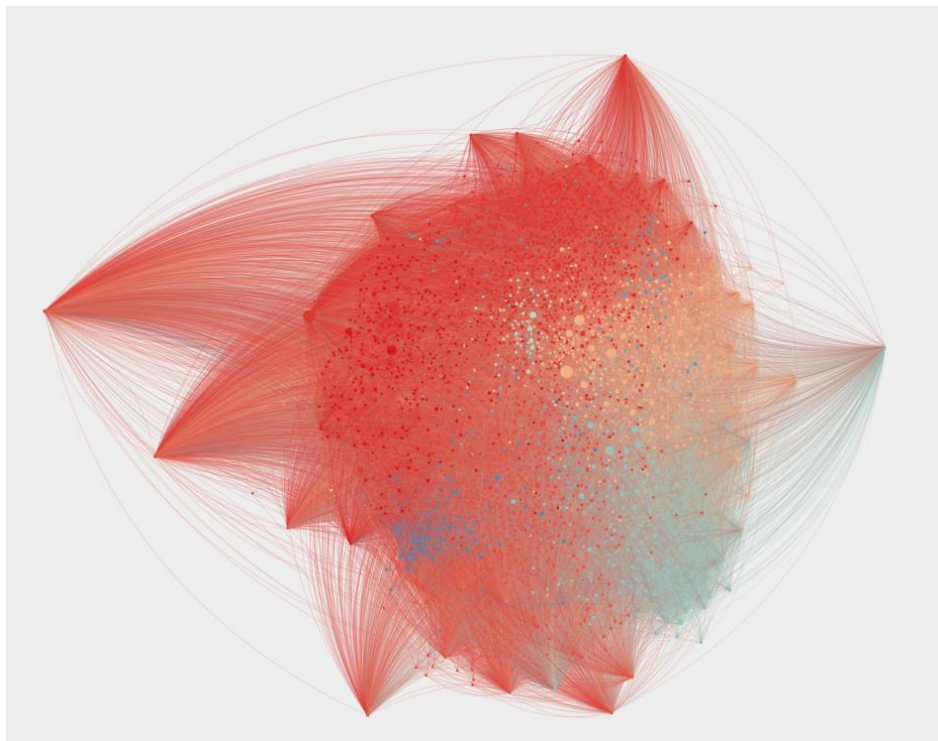


Ilustração 26 : A Rede do Anonymous no Facebook mapeada por Golovchenko
Fonte: <http://anonymous.hol.es/>

Uma vez que a principal rede utilizada por Anonymous no Brasil seja o Facebook, o trabalho de Golovchenko oferece a oportunidade de análises posteriores referentes, por exemplo, ao grau de conectividade entre páginas do Anonymous.

Um exemplo é o resultado obtido por uma rápida pesquisa referente às conexões diretas ou indiretas com a Anonymous Rio. A pesquisa de Golovchenko nos ofereceu uma ferramenta capaz de avaliar, mesmo que minimamente, o grau de importância e relevância da seleção de uma amostra que geraram nossos resultados, analisando o nível de conectividade do Anonymous por meio da ampliação do conceito de cidades idealizada por Luc Boltanski e Eve Chiapello (2009).

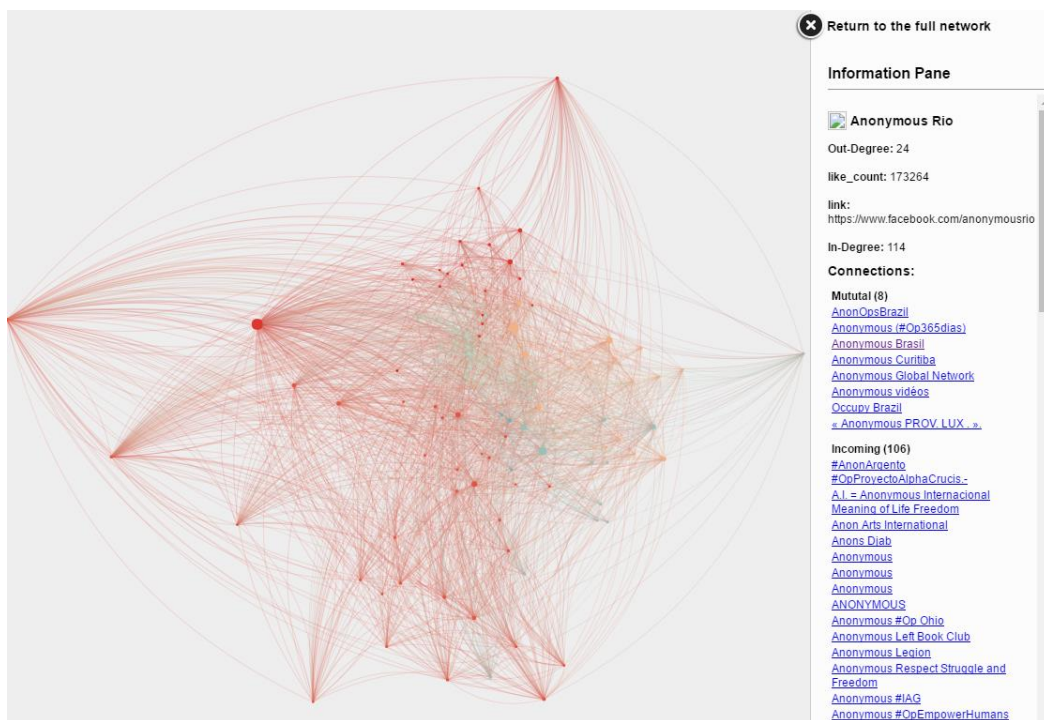


Ilustração 27: Conexões da Anonymous Rio no Facebook
Fonte: <http://anonymous.hol.es/>

Pesquisas quantitativas referentes à cena hacker são igualmente desafiadoras. Se tratando de trabalhos recentes, identificamos o trabalho de Michael Bachmann (2011) que realizou uma pesquisa quantitativa na *ShmooCon*, uma convenção de hackers que acontece anualmente na Costa Leste dos Estados Unidos em Washington, Distrito de Columbia. A parte inicial de seu trabalho foi baseada em três perguntas básicas: O que provoca o interesse inicial pelo hacking? O que levou os hackers a praticar o primeiro ataque? Qual a idade que este

primeiro ataque aconteceu? Um dos entrevistados relatou que seu interesse começou aos 9 anos de idade¹³⁵, outros 20% dos entrevistados aos 12 anos, mas a média é entre 15-16 anos.

Bachmann (2011) destaca que os hackers estudados nesta convenção, se tornaram mais profissionais, e muitos começaram a ver o hacking não como um desafio intelectual, mas também como uma fonte potencial de renda, os definindo como pessoas inteligentes, criativas e determinadas.

Apesar de seu estudo revelar que é um meio (pelo menos nesta convenção) com predominância masculina, revela que a atividade hacker está hoje relacionada a diversas faixas etárias, não exclusivamente entre adolescentes. Suas atividades iniciais são motivadas pela curiosidade (95% dos entrevistados), experimentação (85% dos entrevistados), empolgação e diversão (66%), sentimento de poder (21%), reconhecimento (19%), estímulo pessoal (18%), status e prestígio (15%), vingança pessoal (10%), ideologia política (5%), protesto contra corporações (3%), ganho financeiro (2%) e atenção da mídia (2%).

O tempo de experiência no meio hacker segundo Bachmann (2011) é de 6,5% com mais de um ano, 24,2% entre 2-5 anos, 37,9% entre 6-10 anos, 16% entre 10-15 anos, 8,1% entre 16-20 anos e 7,3% entre 20-28 anos, apontando que quanto mais o hacking se torna um hábito, mais profissional e ambicioso o hacker se torna. (BACHMANN;2011).

Bachmann (2011) reconhece as limitações de seu estudo, uma vez que foram dados levantados entre 130 participantes dentre 800 de uma convenção com um público bastante diversificado, propondo que outros estudos devem ser feitos em outras convenções e reuniões para uma análise de dados mais consistente.

Até o momento, não identificamos resultados de trabalhos quantitativos relacionados ao Anonymous, de forma que pudéssemos compará-los com outros referentes à cena hacker. No entanto, percebemos que os resultados de trabalhos qualitativos dedicados ao Anonymous de pesquisadores como Murilo Machado (2013), que se dedicou a amostras da Anonymous Brasil¹³⁶, Gabriella Coleman¹³⁷ ou Parny Olson¹³⁸ podem ser altamente variáveis em função dos recortes e seleção de fontes.

¹³⁵ Alexandra Samuel (2016) afirma que a habilidade para o hacking se manifesta na infância e destaca o fato de que as crianças de hoje têm uma variedade espantosa de opções tecnológicas. Eles têm os seus próprios smartphones e tablets e todo acesso a estas comunidades está em suas mãos. Samuel reforça a importância de que os pais saibam identificar tal habilidade ainda no início, para incentivar a prática do hacking ético, rompendo a lógica da transgressão, garantindo a utilização da Internet de forma responsável, os tornando a se tornar contribuidores construtivos da segurança e da cultura on-line de privacidade. (SAMUEL;2016)

¹³⁶ Dissertação “Por dentro dos Anonymous Brasil: poder e resistência na sociedade de controle” disponível em: <https://goo.gl/upJDdg>

¹³⁷ Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous

¹³⁸ Nós Somos Anonymous - Por Dentro do Mundo Dos Hackers

Como aponta Inkeles (1964, p.11), “não se pode esperar que um estudante ou pesquisador ingresse em um campo de estudos completamente indefinido e ilimitado (...) pode-se verificar, com o tempo, que a definição dos limites de um campo de estudos é apenas um artifício; no entanto, de início é necessária certa delimitação”

A mesma preocupação em relação a pesquisas referentes ao ciberespaço deve ser aplicada em relação aos hackers e principalmente em relação ao Anonymous, como anteriormente citamos (SCOTT, 1991, p.3): “só se o pesquisador tiver um claro entendimento da lógica de uma determinada medida, ele poderá fazer um julgamento sociológico, informando sua relevância para uma determinada peça de investigação”.

Se tratando de fatores culturais dos hackers, Houghton (2010) apresenta seis, estabelecidos a partir de entrevistas qualitativas que por hipótese “estabelecem uma coesão interna da comunidade através da negociação da identidade coletiva” (HOUGHTON,2010,p.65). Os fatores são:

- 1) Tecnologia: Hackers compartilham um relacionamento fácil, inovador, com toda a tecnologia, não apenas com computadores. Os verdadeiros hackers, hackeiam tudo e qualquer coisa.
- 2) Sigilo: Hackers têm uma relação ambivalente com o sigilo. Eles mantêm suas ações secretas das autoridades, mas visíveis para os seus semelhantes, a fim de compartilhar informações e ganhar reconhecimento ou elogios por seus feitos.
- 3) Anonimato: Este fator está ligado ao sigilo, em que as identidades off-line são mantidos em segredo enquanto uma persona on-line é construído de forma ativa.
- 4) Associação fluida: comunidades de hackers são redes informais com alta rotatividade de membros. Isto é devido a razões orgânicas de crescer fora do hacking e o compromisso maciço necessário para permanecer "até certa data" em tal ambiente que muda dinamicamente, mas também porque ele torna a detecção e repressão muito mais difícil.
- 5) Dominação masculina: pouca evidência de hackers do sexo feminino foram encontradas. Isso está ligado ao fato de que a informática é geralmente dominada pelos homens, através de fatores de socialização da infância e um ambiente de aprendizagem masculinos. A competitividade masculina na pirataria e a possibilidade de misoginia on-line alimentadas pelo anonimato também são criticados, mas nenhuma evidência fornecida suficientemente explica esta anomalia de gênero.¹³⁹
- 6) Motivações: As motivações descobertas por Jordan e Taylor¹⁴⁰ através de suas entrevistas eram de sentimentos de dependência e compulsão; a curiosidade; estar on-line como um ato de escapismo de uma existência off-line chata; sentimentos de poder; o desejo de reconhecimento e aceitação

Himanen (2001) demonstra que os hackers sempre respeitam o indivíduo e sempre foram contra o autoritarismo. Segundo o autor eles gostam de “experimentar a sensação de

¹³⁹ Muitas vezes os hackers ignoram marcadores como gênero, idade e nacionalidade. Entre os 30 entrevistados, 12 pessoas se declararam do gênero masculino, 2 do feminino: entre as quais uma foi presa aos 19 anos e a outra é ativista de rua investigada pelo FBI e opera a Anonobile. Dos 2 grupos (ou células) de manifestantes que acompanhamos e atuam dentro e fora da Internet do Brasil e dos Estados Unidos, possuem uma média de 20 membros principais, entre 5 e 8 membros eram mulheres. Muitos Anonymous declararam que preferem mulheres na orientação dos protestos e manifestações de rua.

¹⁴⁰ Tim Jordan e Paul Taylor realizaram diversas análises sociológicas das comunidades hackers, com obras como o artigo “Sociology of Hackers” (1998) e o livro “Hackers: Crime in the Digital Sublime” (1999)

pertencer a um determinado grupo, de existir como ser independente respeitado perante a comunidade e ser especial para outra pessoa” (HIMANEN,2001, p.55). Do ponto de vista de Himanen, eles “abominam qualquer tipo de violação dos limites individuais, não importa se tais violações ocorrem durante o expediente ou fora dele” (HIMANEN,2001, p.96).

No início de nossas tentativas de interação, um grande desafio esteve no fato de que muitos destes indivíduos desconfiaram da minha presença ou do simples fato de serem abordados, levantando questionamentos internos sobre o motivo de termos escolhido aquele perfil ou página em específico, indagando se estávamos realizando algum tipo de investigação para a polícia.

Com o tempo, percebemos que deveríamos ser mais claros com o tipo de trabalho que estávamos desenvolvendo, nos identificando de maneira clara, demonstrando que tal dissertação poderia ser de fato positiva para que outros pesquisadores pudessem compreender melhor suas ações.

O próprio esforço para entender melhor o Anonymous e o que justificava suas ações (dar exemplos, discutir com sua linguagem) foram fatores que melhoraram o contato com o objeto de maneira significativa.

Um dos critérios adotados para as entrevistas foi de entrar em contato com perfis conhecidos dentro do Anonymous ou com elevado grau de conexões e contatos ativos, não apenas com o trabalho de Golovchenko, mas do meu próprio conhecimento e contato com comunidades virtuais há mais de 15 anos ¹⁴¹e com diversos Anonymous no epicentro de grandes operações e ativos desde 2012.

Nossas amostras, mesmo que aparentemente poucas, envolvem Anonymous com um grande de número de seguidores¹⁴² e conexões, ativos há mais de 5 anos e envolvidos em variadas operações (não apenas divulgando, mas as idealizando e praticando o hacktivism), que foram/são investigados/ condenados por suas ações como hackers. Estes foram alguns dos nossos critérios.

Além de acompanharmos suas atividades essencialmente *online* (em fóruns, por meio comunicados em diversas redes sociais), foram também realizadas aproximadamente 50 tentativas de contato e cerca de 30 entrevistas foram feitas com páginas e perfis ativos do *Anonymous* de diversas nacionalidades¹⁴³, principalmente dentro de redes sociais como

¹⁴¹ Um dos maiores desafios desse trabalho esteve em me isentar de valores socialmente construídos em minhas experiências em comunidades virtuais, obedecendo às regras rígidas da pesquisa científica para que o trabalho tivesse validade.

¹⁴² Mais de 100.000 seguidores no Twitter ou no Facebook.

¹⁴³ Brasil, Canadá, Reino Unido, Alemanha, Estados Unidos, Holanda, Croácia, França, Turquia, entre outros.

Facebook (que predominam os perfis brasileiros) e o Twitter (que muitos afirmaram que seja a melhor forma de articular suas operações).

Algumas destas páginas ou perfis são operadas por uma pessoa, outras, até por vinte, por esse motivo é difícil falarmos com exatidão quantos indivíduos efetivamente participaram do processo de elaboração das respostas. Muitos decidiram em conjunto se deveriam ou não responder nossas perguntas. Destes entrevistados, boa parte está sob investigação, dois já foram presos e tiveram suas identidades amplamente expostas por seus Governos na imprensa¹⁴⁴, contra sua vontade, de maneira bem semelhante ao que acontecia com os *phreakers* que acompanhamos no capítulo 01.

Os contatos foram feitos expondo claramente os objetivos desta dissertação, primeiramente como observadora dentro da organização de uma operação (de rua), o que me permitiu compreender como as decisões são tomadas e como acontece as trocas de conhecimento e informações. Posteriormente, fui desligada do grupo, “pois eu não participava”. Mas essa foi uma estratégia adotada: tentava não opinar ou participar, para não comprometer meu posicionamento como pesquisadora.

Em uma segunda fase, desenvolvemos questionários (ver Anexo 01) que direcionassem melhor nossas questões, para que conseguíssemos compreender seus argumentos antes de entrarmos em contato com perfis que possuíam uma rede maior de contatos.

Buscamos com estas entrevistas compreender o que os leva a desencadear suas ações. Algumas destas conversas foram ao longo de seis meses¹⁴⁵. Iremos apresentar alguns fragmentos destas entrevistas no tópico a seguir.

4.3.7 *Desencadeando operações*

A partir das entrevistas (essencialmente qualitativas) e analisando o material recolhido, reunimos em sete pontos/motivos¹⁴⁶ mais citados que desencadeiam operações e/ou levam um processo de identificação com o Anonymous¹⁴⁷:

- 1- Não se sentem representados. Destacam a falta de confiança em seus governantes, nos políticos e partidos (em especial em relação a transparência e abusos de poder);

¹⁴⁴ Levantamento feito com entrevistas e notícias desde 2011-12.

¹⁴⁵ Utilizamos diversas formas e plataformas para realizar as entrevistas, como Jabber, IRC, twitter, facebook, Skype, e-mail e até mesmo o pastebin.com. As escolhas foram feitas pelos entrevistados, por meios aos quais eles se sentissem mais seguros para responder as questões.

¹⁴⁶ Os pontos não incluem atividades aleatórias/ sem causa aparente

¹⁴⁷ Considerando atividades hacktivistas, ativistas e ciberativistas.

- 2- Censura e ameaça à liberdade (do indivíduo, da população, da Internet ou da liberdade de expressão)
- 3- Perseguição/ Prisão¹⁴⁸ (Étnica, Política- principalmente de *whistleblowers*¹⁴⁹)
- 4- Violência (pedofilia, *bullying*, *cyberbullying*, violência sexual, violência animal, violência policial)
- 5- Situações de injustiça; (como violação dos direitos humanos)
- 6- Desigualdade; (social, de renda, de gênero, de oportunidades)
- 7- Discriminação e racismo

Podemos acompanhar que muitas das atividades (ou operações), realizadas pelos Anonymous, envolvem formas de ações diretas não violentas dentro e fora da Internet, com objetivo de obter resultados concretos excluindo possíveis intermediários e representantes.

Muitas de suas operações conseguiram realizar mudanças políticas ou sociais dentro e fora do ciberespaço, em outras abriram profundos debates na sociedade, buscando dar visibilidade para pessoas ou situações cuja divulgação na mídia não é ampla. Como o caso da “Operação mais Pão Menos Opressão” (2013) que buscava trazer visibilidade para cidadãos em situação de rua no Brasil, a #OpSafeWinter (2013- Atualmente) na América do Norte, Europa e Ásia que busca ajudar estes moradores principalmente durante os meses de inverno ou a #OpGabon que apoia protestantes gaboneses, denunciando massacres e violações dos direitos humanos na região.

*Anon01*¹⁵⁰ envolvido em mais de 10 operações, afirma que “do contrário do governo, não há censura (no Anonymous) e não existe uma autoridade que os comanda”.

O hacktivista britânico *Anon07* começou a atuar em 2008 ainda no 4chan. Ele acredita que boa parte dos sistemas políticos são corruptíveis, mas que acha modelos semelhantes ao da Islândia interessantes.

Segundo Castells (2013) a constituição islandesa preserva os princípios filosóficos de liberdade, valores sociais e demandas de movimentos sociais de 2011, como formas de representação política tais como os princípios de igualdade, livre acesso a documentos públicos. O maior destaque foi o uso da internet e de plataformas como Facebook e Twitter para ouvir

¹⁴⁸ Incluem campanhas de apoio a hacktivistas/ativistas presos como a Free Jeremy Hammond, Free Barrett Brown, Free Lauri Love , todos Anonymous que foram presos /sentenciados e tiveram suas identidades reveladas ou a “Apoio os 23” no Brasil. E ainda retaliações como as ocorridas após o suicídio do hacker/ativista Aaron Swartz, processado pelo sistema legal dos EUA por violação de direitos de artigos acadêmicos protegidos por copyright da JSTOR dentro do MIT. Para maiores detalhes sobre o caso de Swartz assistir o documentário: *The Internet's Own Boy: The Story of Aaron Swartz* (2014) disponível em: <https://youtu.be/84qdLAnhX5U> e os ataques do Anonymous ao departamento de Justiça dos Estados Unidos em 2013: <http://reut.rs/WZWmCJ> e <https://goo.gl/PJ0DUj>

¹⁴⁹ Segundo o dicionário Cambridge: *Whistleblower* é uma pessoa que diz a alguém com autoridade sobre algo ilegal está que acontecendo, especialmente em um departamento do governo ou uma empresa.

¹⁵⁰ Alguns Anonymous pediram confidencialidade em seus perfis, pois não desejam ser vistos como porta-voz ou falar em nome de outras pessoas.

demandas e propostas de mudanças da Constituição entre todos os cidadãos do país, uma vez que 94% dos islandeses estão conectados à Internet (CASTELLS;2013)¹⁵¹.

A maior preocupação do *Anon07* se trata da liberdade e dos direitos humanos, declarando que sempre foi um ativista, mas afirma que foi atuando como Anonymous que conseguiu perceber mudanças reais acontecendo, a partir de suas ações.

Diversos entrevistados relatam ver resultados rápidos em suas ações, algo que deu um novo direcionamento de seus objetivos pessoais. Os entrevistados afirmam que passaram a ser mais atuantes dentro de sua própria comunidade, passaram a questionar decisões e estratégias de seus governantes, se tornando, em alguns casos, ativistas.

O brasileiro *Anon017* afirma ter começado a ler mais livros dentro da área de política e direito, para compreender e questionar situações ao quais ele tinha um conhecimento superficial. Apesar de ter se afastado do Anonymous por falta de organização e preocupado com a possibilidade de ser indiciado, se tornou mais ativo dentro de sua comunidade, reunindo pais e exigindo, por exemplo, melhoras na escola de seus filhos.

O *Anon013* acredita que “todos os políticos são desonestos” e que o “Anonymous oferece a possibilidade para ajudar outras pessoas”. Questiono como o Anonymous o/a teria mudado e ele/a afirma que: “a experiência me deu a oportunidade de ter mais coragem e usar minha própria voz. (...) agora dou voz a minha opinião”.

Alguns Anonymous utilizam ainda a arte como forma de protesto e se dedicam em suas páginas na divulgação de trabalhos de artistas. Muitos utilizam suas máscaras como uma forma de expressão.

O *Anon18* atua desde 2010-2011, período que começou a conhecer e entender melhor o que poderia fazer como Anonymous. Atualmente, com mais de 100.000 seguidores, afirma que começou bem jovem e que nunca havia se sentido um ativista, “me sentia condicionado a não questionar meu governo”, algo que mudou durante os Occupy (2011).

Inicialmente, esteve engajado em diversas operações de cunho hacktivistas, e destaca que buscou formas que pudesse atuar dentro da legalidade (tende mais ao ciberativismo e ajuda humanitária). Enxerga que o “Anonymous seja muito mais do que DDoS, hacking e ‘suporte

¹⁵¹ No Brasil, a Lei nº 12.965, de 23 de abril de 2014, conhecida como o Marco Civil da Internet, contou a participação democrática da população para construção da proposta. Detalhes em: <https://goo.gl/KnmuQ6>

técnico’ de protestos”, para ele, “O Anonymous é como uma ferramenta, que pode ser usada para o bem ou para o mal”.



Ilustração 28: Anonymous

Fonte: Ferguson, 22 de outubro de 2014. Foto de Steven Sweetleaf/Flickr

Do ponto de vista do *Anon029*, do Brasil, ativos desde 2011, boa parte das pessoas que se identificam com o Anonymous, em especial no Brasil, não tem conhecimento algum sobre programação, o que faz com que o Anonymous não se limite apenas ao hacking. Muitas de suas atividades são voltadas a denúncias de repressão policial, corrupção, copa do mundo e mais recentemente contra a Anatel e operadoras de telefonia em relação a limitação da Internet.

O *Anon023*, também do Brasil, afirma que é difícil especificar um padrão, uma vez que seu próprio perfil é composto por diversas pessoas, em variadas localidades com gostos e opiniões muito diferentes. Que a ideia de criar uma página/ site surgiu por eles acreditarem que haja, em alguma medida, uma ideologia que represente seus princípios, assegurada pela segurança do anonimato, pela ausência de um líder, e que permita que eles possam agir sem que saibam quantos ou quem eles são. Apesar de usar meios mais convencionais para se comunicar (IRCs, Telegram, Twitter, Facebook¹⁵²), para realizar a organização de algum protesto, eles procuram locais mais reservados.

O *Anon021*, que possui mais de 90 mil seguidores, critica pessoas dentro e fora do setor de tecnologia que reclamam do anonimato de suas ações, afirmando que “críticas são bem-

¹⁵² A utilização do Facebook, foi questionada pela maioria dos hackers fora do Brasil, que possuem uma preocupação maior em relação a segurança e a interceptação de conversas. Geralmente eles utilizam meios considerados mais seguros de comunicação, como o Jabber, fóruns na DeepWeb e e-mails criptografados. O meio conhecido que eles utilizam é o Twitter, justamente para organizar operações e estabelecer contatos de uma forma mais generalizada. Muitos *Anonymous*, fora do país, afirmam que o idioma é uma limitação e que muitas vezes eles não recebem informações sobre as atividades dos Anonymous do Brasil, o que de certa forma restringe o apoio as suas atividades e causas.

vindas, mas a maioria das pessoas que as fazem, estão sentadas ‘comendo pipoca’ e apenas assistindo a tudo. Não fazem nada a não ser viverem suas vidas” (*sic*). O hacktivismo é visto de uma forma diferente pelo *Anon021* “o hacktivismo não se trata de quebrar um sistema, mas sair dele”, ser independente e ter a habilidade de “mudar as regras do jogo”, “ter a capacidade de conseguir ajudar a derrubar um regime autoritário, inclusive o do seu próprio país. É algo que une a todos”.

Também questiono *Anon021* se ele atuaria de alguma forma para ajudar o governo. Ele afirma que não ajudaria nenhum governo direta ou indiretamente: “Porque eu ajudaria? Acredito que a NSA tem ferramentas muito mais eficientes de identificação”

Seria uma forma do próprio Anonymous agir de forma mais direcionada, com objetivos mais concretos. Ele afirma que ouviu falar do Anonymous pela televisão, e nos últimos cinco anos se envolve com hacktivismo, e que somente uma pessoa sabe quem ele é e o que ele faz, afirmando: “preciso de uma testemunha para minha defesa, para quando for preso”.

Mesmo sabendo que suas ações podem levá-lo à prisão, alega: “Este é o mínimo que podemos fazer depois do que Snowden¹⁵³ fez. Não me importo com as noites sem dormir. Me importo com as pessoas que ajudo do outro lado do mundo.” Quando pergunto se ele tem medo de ser preso responde: “ Não sendo preso nos Estados Unidos, em Israel ou no Oriente Médio, por mim tudo bem”.

A partir do momento que suas operações conseguem alterar ou atingir resultados positivos na sociedade percebemos o hacktivismo como forma de ação direta que amplia os limites de atuação dos hackers.

4.4 Conceito de “Cidade por projetos” de Luc Boltanski

Para compreender o conceito de cidade por projetos que utilizamos para analisar as atividades praticadas pelo Anonymous, é importante apresentar em linhas gerais, como Luc Boltanski, desenvolveu a teoria da justificação.

Apesar de o autor ter trabalhado como assistente de pesquisa de Pierre Bourdieu entre 1969-1976, Vandenbergue (2006) aponta que sua obra é uma ruptura da sociologia crítica de Bourdieu, partindo de uma análise construtivista dos grupos sociais.

¹⁵³ Edward Joseph Snowden é um analista de sistemas, ex-administrador de sistemas da CIA e ex-contratado da NSA que tornou públicos detalhes de vários programas que constituem o sistema de vigilância global da NSA (Wikipédia)

Boltanski (2004) explica que a teoria do *habitus*, que visava pôr fim à antítese da sociedade/indivíduo – que, na sociologia estruturalista correlaciona a capacidade de incorporação de uma estrutura social por agentes (BOURDIEU;2002) –, foi construída a partir de leituras de Bourdieu de autores culturalistas estadunidenses como resultado do encontro da etnologia com a psicanálise, levando a um certo nível de interiorização da ação.

Segundo Vandenbergue (2006),

Se a construção do campo constitui o momento objetivista e determinista da análise, a explicação pelo *habitus* constitui seu momento subjetivista e genético, reintegrando o senso comum e as pré-noções, assim como as ações e as interações situadas na análise do campo. Compreendendo as ações e as interações situadas como produto das estruturas sociais interiorizadas, que regem a produção dos atos que, em certas circunstâncias bem específicas, reproduzem as estruturas das quais elas são o produto, Bourdieu integra dialeticamente a ação e a estrutura, o *habitus* e o campo, em um mesmo sistema de reprodução, superando, assim, a oposição entre o subjetivismo e o objetivismo, mas dando-lhe um deslocamento claramente objetivista. Forçando conscientemente a relação e minimizando o livre arbítrio dos atores, reduzidos a agentes, Bourdieu busca desvelar a exterioridade no coração da interioridade e a desfeticizar as determinações sociais que levam os atores a agir como o fazem.

Conforme Boltanski (2004, p.220), Bourdieu aplicou tal modelo para analisar as classes sociais e a “originalidade da sociologia crítica feita pelo autor e sua equipe foi sua retirada predominantemente filosófica e sua ancoragem na prática da sociologia como uma profissão, combinando os conceitos de criação e campo empírico, os tornando o mais próximos que fosse possível”. (BOLTANSKI, 2011, p. 18).

Por outro lado, o autor aponta que a sociologia bourdiesiana engessou a teoria de Bourdieu, produzindo uma “representação mecanicista da ação” (BOLTANSKI,2004), que em muitos casos negligenciam os atores sociais.

A sociologia da crítica de Boltanski surge observando situações às quais os atores estão engajados em disputas na esfera pública (Boltanski;1982). Vandenbergue (2006) destaca o ponto de ruptura do trabalho de Boltanski com a sociologia crítica de Pierre Bourdieu:

Os teóricos da justificação renunciam à história de longa duração, incorporada nos corpos ou objetivada nos sistemas sociais, para se ligarem, resolutamente, ao presente imediato, recusando projetar as características estruturais na situação observada e ligá-las aos atores dos atributos e das qualificações fixas herdadas do passado. Atentos ao cerne da situação, eles se situam resolutamente na tradição do pragmatismo americano e apresentam uma análise relacionada às sequências de ação e de disputa relativamente curtas, a fim de apreender as pressões situacionais, materiais e ideais, as operações de justificação (Dodier, 1991, 1993). Contrariamente ao teórico do *habitus*, eles não estão tão interessados pelo passado ou pelo futuro quanto pelo presente. O que lhes interessa não é o sistema, nem a estrutura, mas as ações e as práticas; não os atores nem os agentes, mas a situação; não os homens e as mulheres, mas seus momentos – *moments and their men* –, para retomar uma fórmula célebre de Goffman (1967, p. 3). Os momentos críticos (Boltanski; Thévenot, 1991, p. 31) retêm mais particularmente sua atenção. Nesses momentos não habituais de crítica e de questionamento, os atores exprimem, publicamente, suas censuras e se voltam para a justiça.

A continuidade do trabalho de Boltanski (*et al.*) construiu um modelo que nos permite compreender como os atores manifestam suas ações sem recorrer à violência, justificando suas pretensões à justiça (BOLTANSKI,2004; VANDENBERGUE,2006).

Segundo Boltanski (2004), não devemos considerar somente intenções escondidas e inconscientes dos atores, mas devemos levar em conta o que eles dizem. Vandenbergue (2006) aponta que denunciar uma injustiça, provocar transformação na sociedade ou até mesmo solicitar uma mudança deixou de ser um monopólio da sociologia crítica, mesmo que seus resultados sejam desiguais ou diferentes do proposto, a sociologia da crítica permite um nível de incerteza nas consequências de um ato.

Por essas razões, os autores da justificação e da sociologia da crítica se dedicam ao presente imediato, sem criticar ou explicar as ações dos atores, mas buscam suas percepções a partir de suas próprias observações na esfera pública.

O conceito de cidades que substituem as estruturas foi utilizado pela primeira vez por Boltanski e Thévenot na obra *On Justification: Economies of Worth* “como mediações simbólicas e axiológicas, que permitem constituir a situação como um conjunto bem ordenado de interações vividas entre as pessoas e os objetos que os atores encontram em seu ambiente imediato” (Vandenbergue, 2006, p. 331).

Em “*De la justification*”, Boltanski (2004,p.221) afirma que não buscava uma sociologia geral, nem tenta excluir relações de força. Na verdade:

Trata-se de pensar em situações nas quais as relações de força estão mais ou menos neutralizadas, uma situação pública, ou seja, uma situação que a justificação responde a crítica e a crítica a justificação. Em situações desse tipo, não podemos considerar somente as intenções escondidas e inconscientes dos atores, mas também o que eles dizem. Isso é o mínimo que podemos fazer para reconhecê-los, para reconhecer sua posição normativa, seu ponto de apoio normativo – aquilo que nomeávamos tradicionalmente como “valores”. A ideia presente em *De la justification* é a de que esses pontos de apoio normativos existem em número limitado em cada momento do tempo, em uma certa sociedade, o que não exclui, absolutamente, as relações de força.

Da “teoria social, segundo esses autores, não caberia estabelecer princípios que tornem possíveis relações justas, mas cabe-lhe analisar os reclamos de quem se sente injustiçado, para sistematizar os princípios ou as justificativas ali pressupostos.” (Sobottka, 2012, p.141).

Segundo Alcantara (2005), o próprio conceito de justiça está ligado nas disputas entre agentes, que buscam realizar o que eles entendem como justo, em situações ou períodos históricos diferentes. A teoria da justificação só faria sentido se pensada levando em consideração a existência de uma moralidade arraigada nos indivíduos e suas ações partem deste contexto moral. (ALCANTARA; 2005)

Assim, foram apresentados seis tipos de cidades e cada uma delas com sua própria justificativa: A cidade inspirada (Santo Agostinho – *A cidade de Deus*) baseada na grandeza da

inspiração, citando a vida de artistas e santos, em que “todo aquele que a alcança ou a vive é grande”; a cidade doméstica (Bossuet – *La politique tirée des propres paroles de l’écriture sainte*) baseada na hierarquia e ordenamento familiar; na cidade de renome (Hobbes – *Leviatã*), a grandeza está na busca do reconhecimento dos outros indivíduos; a cidade cívica (Rousseau – *Do contrato social*) baseada na vontade geral; na cidade comercial ou mercantil (Adam Smith – *A riqueza das nações*) grandeza está na capacidade de um indivíduo enriquecer em um mercado competitivo; e a cidade industrial (Saint Simon – *Du système industriel*) baseada na capacidade dos profissionais e a eficácia de um processo. (ALCANTARA,2005; BOLTANSKI,1981; SOBOTTKA, 2012)

Todas as seis cidades foram articuladas para justificar o “novo espírito do capitalismo”, que deu nome à obra lançada em 1995 juntamente com Eve Chiapello, em um momento em que o capitalismo precisou criar novas formas para manter a adesão das pessoas, diferentemente do final da década de 1960, ao qual a crítica social em relação à chamada sociedade do consumo estava em seu auge. Neste trabalho, foi introduzido um novo tipo de cidade: a cidade em rede, mais conhecida como “cidade por projetos”.

Alcantara (2005) afirma que, segundo Boltanski e Chiapello, este espírito do capitalismo teria sido concretizado ou materializado em textos de gestão empresarial, que foram objeto de pesquisa e disseminados pela gestão empresarial.

“Cidade por projetos” é um termo oriundo da gestão empresarial, ligada a uma empresa que possuiu inúmeros projetos associando pessoas variadas, que costumam participar de inúmeros projetos que se referem a oportunidades e possibilitam conexões de um segmento de rede, ao qual a multiplicidade de encontros passa a gerar conexões temporárias que são reativáveis por grupos diversos em distancias sociais muito grandes. Segundo Boltanski (2009):

Os projetos possibilitam a produção e a acumulação num mundo que, se fosse puramente conexonista, conheceria apenas fluxos, sem que coisa alguma pudesse estabilizar-se, acumular-se ou ganhar forma: tudo seria carregado pela corrente incessante dos contatos estabelecidos, que, em vista de sua capacidade de comunicar tudo com tudo, distribuem e dissolvem incessantemente aquilo que cai em suas malhas. O projeto é precisamente um amontoado de conexões ativas capazes de dar origem a formas, ou seja, dar existência a objetos e sujeitos, estabilizando e tomando irreversíveis os laços. Portanto, é um *bolsão de acumulação* temporário que, sendo criador de valor, dá fundamento à exigência de ampliar a rede, favorecendo conexões. (BOLTANSKI,2009, p. 135)

Boltanski (2009) afirma o sucesso constituído por um novo sistema de valores, no qual as pessoas podem se apoiar para fazer julgamentos, em que se é capaz de diferenciar os comportamentos que são considerados aceitáveis ou não. Durante este processo, é possível, segundo o autor, avaliar qualidades e atitudes que não haviam sido anteriormente

identificadas, legitimando assim, novas formas de poder e determinam quem será o beneficiado do projeto. (BOLTANSKI;2009).

Do ponto de vista de Boltanski (2009), em um mundo no qual a justiça deve se adaptar a um mundo reticular (não ligado à rede), são estabelecidos critérios de relação entre seus membros, marcado pelo fim de um projeto e a busca por novos. Porém estes projetos podem ser eventualmente retomados e muitas redes podem ser reativadas, uma vez que estas permanecem disponíveis.

A cidade por projetos, segundo Boltanski (2009, p.138), é vista como um sistema de injunções que pesam sobre um mundo em rede, incitando sua formação e crescimento (ramificações), respeitando os princípios da ação justificável, próprias dos projetos.

4.4.1 Escolha da Operação

Compreendendo a dificuldade metodológica que o próprio objeto apresenta, procuramos identificar e selecionar em meio a diversas operações declaradamente realizadas por Anonymous, um exemplo de uma atividade essencialmente hacktivista, ao qual pudéssemos aplicar a teoria de Boltanski.

Machado (2013,p.97) destaca que:

(...) à luz dos exemplos práticos no Brasil, os Anonymous não são uma ideia homogênea nem tampouco cegamente unida, mas sim um emaranhado de grupos e coletivos que possuem diferentes pensamentos e metodologias de trabalho, de modo que estes frequentemente são conflitantes uns com os outros. Para atestá-lo, basta ver as inúmeras reações que se sucederam às operações WikiLeaks e Globo. Uma vez propostas, enquanto alguns Anons se engajam em ações de apoio a elas, outros discordaram de seu ideal ou de seu modus operandi, passando a criticá-la abertamente e fomentando um debate que, em muitos momentos, parece não ter fim. Além do mais, nada impede que os que se mostram contrários criem seus próprios nichos, suas próprias ações e seus próprios métodos de trabalho. Nesse sentido, os Anons adotam a cultura do individualismo colaborativo, também muito própria à cultura hacker(...)

Principalmente após o Chanology¹⁵⁴, não existe uma homogeneidade para estabelecer um “perfil” do Anonymous, o mesmo se aplica para o hacktivismo; no caso deste trabalho, delimitamos a prática para a defesa dos direitos humanos.

Oxblood Ruffin critica algumas posturas e práticas do Anonymous, como uso de DDoS, invasões e roubo de dados, mas pondera que, quando tais atividades podem salvar uma vida, elas passam a ser práticas mais aceitáveis ou justificáveis no meio hacker. (MILLS;2012)

A dificuldade para a seleção de uma operação se deu em função da extensão das atividades e da própria característica de boa parte das operações hacktivistas do Anonymous:

¹⁵⁴ Anteriormente a 2008, traçar este perfil seria possível, uma vez que boa parte dos membros do Anonymous eram membros essencialmente dos chans (especialmente do /b/).

elas são curtas (duram entre 3-15 dias)¹⁵⁵ e buscam atingir resultados concretos de forma rápida. Cada nova operação abre novas redes de contatos¹⁵⁶ de pessoas engajadas em uma causa, que são agregadas de forma coletiva como atividades do Anonymous.

Não é incomum em muitos casos que Anonymous adotem uma estratégia semelhante à feita pelos *yippies* ainda em 1968, quando Abbie Hoffman passou a utilizar os meios de comunicação ao seu favor (conforme apresentado na p.23 desta dissertação), a diferença é que o Anonymous usa a internet e passou a utilizar portais de notícias *online* ao seu favor¹⁵⁷.

Em alguns países, os Anonymous pararam de “atacar” a imprensa, eles até questionam algumas publicações, mas muitos se mostram mais abertos para conversar com jornalistas e pesquisadores. Esta mudança ocorreu em algumas redes, quando, segundo o *Anon28* e o *Anon29*, eles passaram a argumentar que atos contra meios de comunicação, vão contra o princípio da liberdade de expressão ao qual eles defendem.

Oxblood Ruffin, um dos fundadores do hacktivism, afirma para Mills (2012)

que apoia fortemente o uso de mídias sociais como Twitter e YouTube para promover os direitos humanos, uma técnica ao qual o Anonymous certamente tem dominado e conseguido um efeito positivo. ‘Esse é um exemplo clássico de hacktivism’, disse ele sobre a atuação do Anonymous ajudando manifestantes a organizar e dar a volta tentativas de censura do governo”

A escolha pela análise da #OpDarkNet, que durou cerca de 3 semanas, ocorreu em função da complexidade técnica e pela disponibilidade dos relatos ao decorrer de sua atividade, por meio de “comunicados de imprensa” feitos pelos Anonymous nela envolvida, que acreditamos que sejam capazes de expor valores incorporados da prática do hacktivism, com base na teoria de Boltanski.

4.4.2 Análise da #OpDarkNet

¹⁵⁵ É possível identificar outros 2 grupos de operações: as que ocorrem de maneira contínua (como a #OpDeathEaters) e as que acontecem uma vez por ano (como a #MMM).

¹⁵⁶ Durante as entrevistas, dois fatos nos chamaram a atenção: Alguns hackers após as entrevistas, indicaram novos contatos aos quais poderiam colaborar com nossa pesquisa. O segundo fato foram hackers ou coletivos que atuam anonimamente dentro do Anonymous. Muitas atividades são praticadas pelos próprios perfis/ páginas, enquanto outros não querem ter suas atividades abertamente associadas ao Anonymous. São contatos que por exemplo, desenvolvem e garantem segurança nas comunicações.

¹⁵⁷ Durante uma onda de ataques ao decorrer de algumas operações que ganham repercussão e recebe ampla cobertura da imprensa, não é incomum práticas como DDoS e Defacement em websites completamente aleatórios e vulneráveis a ataques. Essa postura de quantidade (ao invés de qualidade) é questionada entre hacktivistas dentro e fora do Anonymous. Outro fato que presenciei como observadora, dentro de um grupo *online* de pessoas que idealizavam e organizavam *online* uma operação de rua, foi o compartilhamento de manuais com técnicas de discurso; mas como foi uma experiência dentro de apenas uma operação, não podemos determinar que esta seja uma prática corriqueira.

A Operação DarkNet ocorreu em outubro de 2011, em meio a diversas operações como a #Occupywallstreet.

Segundo o “Comunicado de Imprensa” do Anonymous, divulgado no Pastebin no dia 20 de outubro de 2011, em 06 de outubro alguns “anons” estavam pesquisando sobre criptografia e segurança na DarkWeb (TOR, I2P) quando identificaram uma quantidade crescente de pedófilos em uma seção da “*Hidden Wiki*”, chamada “*Hard Candy*”, com grupos de discussão que incluíam imagens de crianças e adolescentes.

Em 20 de outubro, identificaram que o total de visualizações da seção era de 2.055.701, enquanto a Hidden atingia 2.677.430 visualizações. Segundo o comunicado, alguns membros do Anonymous foram desafiados por usuários *da Silk Road*¹⁵⁸ a tirar um dos maiores sites desta seção do ar: o Lolita City.

Ao acessar a comunidade e receberem respostas perturbadoras de membros de um fórum, resolveram iniciar a #OpDarkNet, visando revelar o abuso e a “perversão” dos membros desta comunidade para a população em geral. Outro agravante apontado pelo comunicado é que um dos integrantes deste grupo de Anonymous foi vítima de abuso infantil.

Segundo o Anonymous (2011), eles começaram a desenvolver ferramentas¹⁵⁹ para identificar e recolher maiores informações sobre hospedagem e os integrantes desta comunidade.

Esta operação ocorreu dentro da chamada *DarkWeb*, associada a *Deep Web*, e um dos alvos foi um site (incluso em uma *DarkNet*) de pornografia infantil chamado “*Lolita City*”. A operação expôs o nome e dados pessoais de 1589 usuários no *Pastebin*¹⁶⁰ com informações do volume de imagens baixadas por cada um. Além de disponibilizar detalhes da ação publicamente, enviaram as informações para INTERPOL e ao FBI para investigação.

Existe uma relativa confusão sobre a diferença entre a *Deep Web* e a *Darkweb*. O primeiro termo teria sido utilizado pela primeira vez em 2001 por Michael K. Bergman em seu artigo “*The Deep Web: Surfacing Hidden Value*”, em que a Deep Web, basicamente, é uma série de redes não detectáveis por motores de busca convencionais.

A DarkWeb é a rede de sites que tem como características a omissão de seus IP’s (número do computador) dos servidores que as executam, dificultando a identificação de quem

¹⁵⁸ Para compreender melhor a Silk Road, assistir o documentário “Deep Web” (2015) Disponível em: <https://youtu.be/62P2PzNI04Q>

¹⁵⁹ O software recebeu os nomes “The Legion”, “Thor” e posteriormente “Chris Hansen” (em referencia ao autor do programa de TV “*To Catch a predator*” (2004)

¹⁶⁰ <http://pastebin.com/qWHDWCre>

está por trás destes sites, ligadas a redes fechadas de um grupo privado de pessoas, as chamadas DarkNet.

Weisskopf (2015) afirma que as partes anônimas e criptografadas acessadas por softwares - como o TOR (*The Onion Router*), que faz a conversão da rede e dá segurança aos usuários (omitindo seus IP's) - são áreas que estão intencionalmente inacessíveis por navegadores padrão. Originalmente, o TOR foi desenvolvido pelo governo estadunidense para fins militares. Posteriormente, o software foi disponibilizado gratuitamente (Software Livre) com *Open Source* (código aberto), para a utilização da população em geral.

O TOR, acrônimo de "*The Onion Router*" (algo como "Roteador Cebola"), faz uma analogia para demonstrar que o usuário precisa "descascar muitas camadas", como se faz com uma cebola, para conseguir algumas informações ou encontrar a identidade real do usuário.

Esta analogia das "camadas" criou uma visão errônea para a população em geral de que a "*Deep Web*" é separada por camadas ou domínios, estruturada por um tipo de hierarquia de dados, informações e acesso na Internet.

Além dos usuários "comuns, as redes da DarkWeb/ DarkNet são frequentemente utilizadas por Governos, informantes, jornalistas, ativistas de países como o Irã e a China. Além do TOR, outros programas acessam diferentes DarkWebs, como o I2P, FAI, FreeNet, entre outros. Alguns destes sites, são "fechados".

Segundo Silva (2015):

A utilização da Dark Web pelos seus usuários tem dois objetivos principais, o primeiro é hospedar ou transmitir conteúdo de maneira que não seja visível a qualquer pessoa ou entidade na Internet que esteja realizando monitoramento. O segundo objetivo tem por finalidade permitir o acesso e a publicação de conteúdo de maneira anônima, impedindo a identificação da origem de determinado acesso e sua rastreabilidade. O uso da Dark Web pode ter fins lícitos ou ilícitos por parte de seus usuários.

Segundo Egan (2015), Deep Web é um termo genérico que representa 90% do conteúdo total da *Internet* e inclui DarkWebs (representando 0,01% deste total).

Inicialmente, a operação tinha como principais estratégias a Engenharia Social, o DDoS (para derrubar os servidores) e foi incluída como parte do #OccupyWallStreet, ganhando uma forte adesão de hackers que se disponibilizaram para ajudar a chegar na raiz do problema, isto é: identificar quem hospeda o site, quem o mantém, e quem são os usuários.

No mesmo mês, os *Anonymous* declararam que "a Operação *Darknet* nunca foi destinada a derrubar o TOR ou os "*darknets*":

"O único objetivo da Operação era revelar que um serviço como o "Projeto TOR" poderia ser arruinado pelo 1% que o utiliza para pornografia infantil. Os outros 99% são compostos por jornalistas chineses/ iranianos, Inteligência do Governo que lutam

uma guerra secreta com a *Al-Qaeda*, e nós *Anons*, que acreditamos no direito de livre expressão.” (ANONYMOUS,2011)

A operação foi detalhadamente explicada por meio de outro “Comunicado de imprensa”.

Por volta das 8:30, enquanto navegávamos na “*Hidden Wiki*”, notamos uma seção chamada “*Hard Candy*”, que foi dedicada a links de pornografia infantil. Nós, então, removemos todos os links do site e em menos de 5 minutos os links foram editados de volta por um administrador. Por esta razão, vamos manter a “*Hidden Wiki*” indisponível. Aproximadamente às 08:45 notamos que 95% da pornografia infantil listada na “*Hidden Wiki*” compartilham uma impressão digital com o servidor de hospedagem “*Freedom Hosting*”. Por volta das 21:00 de 14 de outubro de 2011, foi identificado que o “*Freedom Hosting*” é o anfitrião da maior coleção de pornografia infantil na Internet. Nós, então, emitimos um aviso para remover o conteúdo ilegal do seu servidor, o que eles se recusaram a fazer. Às 23:30 de 14 de outubro de 2011, nós infiltramos no servidor de hospedagem compartilhada da “*Freedom Hosting*” e desligamos os serviços para todos os seus clientes, devido à sua falta de ação para remover a pornografia infantil a partir de seu servidor. Aproximadamente às 17:00 do dia 15 de outubro de 2011, o “*Freedom Hosting*” instalou seus *backups* e seus serviços restaurados para seus clientes de pornografia infantil. Nós emitimos vários avisos para remover toda a pornografia infantil de seus servidores, algo que a “*Freedom Hosting*” se recusou a fazer. Por volta das 20:00 do dia 15 de outubro, apesar das novas configurações de segurança, mais uma vez infiltramos no servidor de hospedagem compartilhada da “*Freedom Hosting*” e paramos o serviço de todos os clientes. Os proprietários e operadores da “*Freedom Hosting*” estão apoiando abertamente a pornografia infantil e permitindo que pedófilos possam ver crianças inocentes, alimentando seus problemas e colocando crianças em risco de rapto, abuso sexual, estupro e morte. Por isso a #OpDarknet se declara inimigo número 1 da “*Freedom Hosting*”. (...) Nossas demandas são simples. Remova todo o conteúdo de pornografia infantil de seus servidores. Recusem-se a fornecer serviços de hospedagem para qualquer site que lide com a pornografia infantil. Esta afirmação não é apenas destinada a “*Freedom Hosting*”, mas todo mundo na internet. Não importa quem você é, se percebermos que é um anfitrião, que promove ou que apoia a pornografia infantil, você vai se tornar um alvo. (...) Nós somos *Anonymous*. Nós somos uma legião. Nós não perdamos. Nós não nos esquecemos. Esperem de nós.¹⁶¹ (ANONYMOUS; #OpDarkNet Press Release 2011)

Segundo o último comunicado divulgado no dia 02 de novembro de 2011, entre os dias 26 e 27 de outubro, eles iniciaram uma nova operação chamada #OpSec (*Operation Security*) contra os desenvolvedores do TOR, que lançariam uma nova versão do software no dia 27 de outubro.

É interessante ressaltar que, novamente, o Anonymous utilizou um termo militar. De forma resumida, as *Operations security* (OPSEC) foram reforçadas durante a Guerra do Vietnã e se referem a uma metodologia ou a um processo capaz de identificar se suas próprias ações podem ser observadas pela inteligência do país adversário, buscando determinar se a informação recolhida pode ser útil para o inimigo e determinando medidas capazes de reduzir os impactos e a exploração desta informação (falha).

Membros do Anonymous teriam entrado em contato com amigos da *The Mozilla Foundation*TM e do *Developers of Firefox*TM para conseguir uma autorização para configurar um certificado (que segundo o site do Mozilla/ Firefox são o equivalente digital de cartões de

¹⁶¹ <http://pastebin.com/T1LHnzEW>

identidade. Eles são usados para criptografar e descriptografar as informações transferidas entre os sites), conseguindo adicionar um “TorButton”¹⁶² para o Firefox chamado “*The Honey Pawt*”, um tipo de extensão para o TOR, desenvolvido para canalizar todo o tráfego proveniente da seção “*Hard Candy*” e do “*Lolita City*” para realizar o que eles chamaram de “registro forense”, para recolher provas como tráfego online e identificação dos números reais dos IP’s destes indivíduos.¹⁶³

Segundo o Anonymous (2011), o programa não era um *malware* ou um vírus, uma vez que tinham autorização para utilizá-lo e estavam dentro das normas do Mozilla/Firefox. Eles pararam o DDoS (considerado por alguns membros um tipo de “Occupy”) que impedia o acesso à Hidden Wiki e inseriram uma mensagem falsa de atualização de segurança do TOR na seção Hard Candy com o *The Honey Pawt*

Assim, eles monitoraram a atividade destes usuários por 24 horas recolhendo provas para apreciação da justiça e identificando 190 supostos pedófilos, que tiveram a localização de seus endereços IP divulgadas.



Ilustração 29: Localização dos IP's identificados pelo Anonymous durante a #OpDarkNet
Fonte: Anonymous (2011)

¹⁶² Pacote de software que permite o acesso ao Tor

¹⁶³ Mesmo que segundo o Anonymous (2011) a extensão tenha sido utilizada apenas na seção “Hard Candy”, o programa em si abriu um precedente que demonstrava a possibilidade de explorar uma vulnerabilidade do TOR. Acreditamos, com base nos comunicados de imprensa que a prática tenha sido “White Hat” para o Firefox e “Gray Hat” para o TOR, permitindo o aumento de segurança para extensões deste tipo.

A operação foi finalizada em 02 de novembro de 2011. Em 2012, os Anonymous foram considerados uma das 100 pessoas mais influentes do mundo, segundo o *ranking* da revista TIME¹⁶⁴. Em agosto de 2013, Eric Eoin Marques, de 28 anos, operador da *Freedom Hosting*, foi detido em Dublin, na Irlanda, e, segundo o FBI, considerado "o maior facilitador de pornografia infantil do planeta", com quatro acusações que envolvem: publicidade, distribuição, conspiração para fazer propaganda e distribuição de pornografia infantil.

Marques (que possui dupla cidadania) foi extraditado para os Estados Unidos em 16 de dezembro de 2015 e poderá ser condenado a 30 anos de prisão.

Uma das táticas de neutralização¹⁶⁵ apresentada por Becker (2005, p.39) afirma que “ sua própria indignação moral ou dos outros pode ser neutralizada por uma insistência em que o dano não está errado à luz das circunstâncias. O dano, pode-se afirmar, não é realmente um dano, é antes uma forma legítima de retaliação ou punição”.

Notamos que do momento em que o Anonymous passou a se enxergar como objeto de ação, não como agente, a justificção de seus atos passaram a ser vistos por eles como válidos, mas muitas vezes não pelo sistema legal ou pela comunidade. Neste caso, o alvo de seus ataques foi um grupo que possui posturas moralmente inaceitáveis para a maioria da população; são pedófilos, mesmo que estes indivíduos busquem suas próprias justificções para seus atos a partir de suas próprias percepções de “certo e errado”, a Constituição¹⁶⁶ garante proteção integral à criança e ao adolescente, contra este tipo de conduta.

O Anonymous não encontrou muita resistência para esta operação, em parte, graças a uma estratégia inteligente, de lançá-la em meio ao auge dos protestos do *Occupy Wall Street* em 2011, gerando empatia do público apoiando-se em valores morais, éticos e principalmente juridicamente legais para a recolha de provas em um ambiente virtual, que era propício para a atuação dos hackers, uma vez que segundo Castells (2003, p.43), “hackers existem fundamentalmente online”. São detalhes que deram credibilidade para suas ações durante a #DarkNet.

Observamos que, o Anonymous procura atuar com pautas que criam pouca tensão na sociedade em períodos de sensibilização e manifestações coletivas. Durante as entrevistas, o *Anon021* destaca a importância de operações, que buscam identificar a raiz de um problema,

¹⁶⁴ <http://goo.gl/88ZcEU>

¹⁶⁵ Distinção de técnicas para neutralizar a força dos valores de aceitação de ordem

¹⁶⁶ No Brasil são os artigos os artigos 240 e 241, do Estatuto da Criança e do Adolescente(Lei nº 11.829, de 25 de novembro de 2008 que altera a Lei 8.069, de 13 de julho de 1990) que visam o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet com penas – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.

do contrário de atos que tenham um tipo de estratégia considerada superficial. O *Anon021* criticava as operações contra o Estado Islâmico (EI) #OpIsis ou #OpIceIsis:

(...) Não participei de nenhuma operação contra o EI (Estado Islâmico), por exemplo, primeiro, pois eu acredito que sejam ações superficiais. Identificar perfis não reduz o massacre que está acontecendo, mas se eles identificassem quem opera, financia e mantem estes sites, seria uma medida de fato eficiente”.

A estratégia de identificar perfis em redes sociais como o Twitter segundo o *Anon021*, poderia prejudicar a localização, pois muitos membros do EI, poderiam utilizar formas mais seguras de comunicação, utilizando por exemplo, a própria Dark Net. “ Tornaria tudo mais difícil, como um hacker, você precisa estar sempre um passo adiante”.

Percebemos que alguns dos traços do Anonymous refletem a história da própria comunidade hacker ao qual eles estão inseridos, enquanto outros traços são reflexos da cultura da juventude no tempo e lugar que estes indivíduos vivem. (CASTELLS;2003)

O que buscamos apresentar, com o detalhamento e as consequências desta operação, foi a aplicabilidade da teoria de Boltanski, que nos permitiu analisar as reclamações de quem se sentia injustiçado, de forma que os Anonymous nela envolvidos, fossem capazes de se apoiar e sistematizar justificativas e princípios para os seus atos, se tornando capazes de diferenciar comportamentos que eles consideravam aceitáveis ou não.

4.5 Considerações Finais

Podemos acompanhar ao longo do trabalho a construção da Cultura hacker na sociedade e os momentos nos quais eles passaram a ser vistos como um problema social. A partir da década de 1990, com o desenvolvimento da World Wide Web, a cena hacker teve a possibilidade de ampliar sua atuação, principalmente em relação ao hacktivismismo.

Segundo Tapias (2014, p.44) :

Se as novas tecnologias introduzem mudanças radicais na forma de conceber a informação e seu uso, é obrigatório reconhecer a partir daí que essas inovações e seu uso, é obrigatório reconhecer a partir daí que essas inovações, gravitando sobre o computador, afetaram, nas poucas décadas transcorridas a partir da sua invenção, quase todos os aspectos de nossas vidas, sendo determinantes as mudanças desencadeadas em nossas formas de pensar.

O campo de atuação da cena hacker foi ampliado com a evolução gradual de dispositivos móveis que deram a possibilidade da população estar conectada à internet, a qual a própria ONU reconheceu como um direito fundamental.

O Anonymous abre um novo campo de estudo aos cientistas sociais que concentram seus trabalhos em temas relacionados ao ciberespaço, por ser um objeto essencialmente híbrido entre duas realidades, que transita entre o real e o virtual.

Pode-se destacar ainda o fato de que, segundo Castells (2013), a maior dificuldade dos estudos voltados a uma sociedade em rede é em função da celeridade dos processos e a forma que as mudanças acontecem. Os *Anonymous* estão em atividade desde 2003 e podemos acompanhar ao longo de sua trajetória as mudanças que sofreram e as possibilidades que foram abertas em relação ao hacktivismo, o ciberativismo e até mesmo sobre conceitos de uma identidade coletiva.

Uma vez que a justificação possui relação direta com concepções de justiça e ações moralmente aceitáveis por meio de critérios estabelecidos entre estes indivíduos, buscamos identificar conceitos da teoria de Boltanski, os ampliando para ações do *Anonymous*, selecionando de forma inicial uma operação hacktivista (#OpDarkNet), buscando identificar em seus relatos valores socialmente construídos dentro e fora da Internet, ampliando a aplicabilidade do modelo de Boltanski em outros contextos da sociedade.

Jeremy Hammond, um hacktivista do *Anonymous*, condenado a 10 anos de prisão e considerado um terrorista pelo FBI, fundou um site chamado “Hack This Site”¹⁶⁷. Com uma forte referência, tanto com as demandas da comunidade hacker quanto com a ideia da obra de Hoffman “*Steal this Book*” (“Roube este livro” de 1971), uma das mais importantes obras do movimento de contracultura.

O site tem o objetivo de formar uma comunidade aberta, na qual qualquer pessoa pode contribuir e participar no desenvolvimento do site. O *Hack This Site* é gratuito e oferece desafios, treinamentos, recursos e a oportunidade de serem invadidos para que “*hackers underground*” testem suas habilidades incentivando a prática do hacking ético.

Do ponto de vista de Hammond (2014) o “hacktivismo existe dentro da história dos movimentos de justiça social. Hacktivismo ainda é o futuro, e é bom ver as pessoas ainda fazer algo sobre isso.”

Outros *Anonymous* criaram dentro da *Dark Web* uma rede para treinar uma nova geração de hacktivistas. Alguns *Anonymous* criticam o fato de que apesar do número de perfis e páginas terem crescido, seu nível técnico foi reduzido e que muitos não respeitam princípios da ética.

Segundo o hacker *Jacob*¹⁶⁸, um atual membro associado ao CCC na Alemanha, existe uma verdade que parece óbvia, mas raramente é abordada: os hackers também envelhecem, eles amadurecem suas posturas procuram novas formas de contribuir para a comunidade, reforçando um sistema próprio de valores.

¹⁶⁷ <https://www.hackthissite.org/>

¹⁶⁸ O nome real do *hacker* foi alterado para manter o sigilo das entrevistas.

Do ponto de vista de Dominguez (2012) o “Anonymous tem sido muito eficaz, tanto como uma rede e como o surgimento de um tipo de sociedade civil que é extremamente íntima com a cultura da Internet”

Fuchs compreende o Anonymous como um tipo de movimento¹⁶⁹, como afirma no texto “*The Anonymous movement in the context of liberalism and socialism*” baseado em uma rede informal de interações entre uma pluralidade de indivíduos, grupos e organizações engajados em conflitos políticos ou culturais, com baseada em compartilhar identidades coletivas.

Destacamos os trabalhos de Christian Fuchs professor e diretor do Instituto de Pesquisa de Mídia e Comunicação (*Communication and Media Research Institute*) do *Westminster Institute for Advanced Studies*, que afirma que o Anonymous é uma expressão das contradições do próprio liberalismo.

Para Fuchs (2013, p.347) :

o Anonymous é ao mesmo tempo movimento e antimovimento é a ação coletiva baseada no compartilhamento de identificação com alguns valores básicos (como liberdades individuais e liberdade da Internet) resultando em protestos práticos online e off-line contra seus adversários, e ao mesmo tempo para muitos engajados nas plataformas do Anonymous, como jogos individuais e divertimento. Na maioria das vezes, o Anonymous existe “*for the lulz*”, para diversão de seus usuários, mas de tempos em tempos- e com o passar dos anos, essa frequência aumenta- em ações individuais se convertendo em ações políticas coletivas. Muitas pessoas se engajam no Anonymous por suas ações políticas compartilhadas em alguns valores políticos básicos, expressados em seus manifestos.

Do ponto de vista de Fuchs (2014) acompanhamos entre os séculos XX e XXI a ascensão da ideologia neoliberal, que tensiona o individualismo radical, a responsabilidade individual, o empreendedorismo, o mercado e a competição como princípios do governo, entre outros. Para o autor, os Anonymous estão alinhados com a linguagem da liberdade individual que são características do liberalismo contemporâneo, assim como suas contradições. (FUCHS; p.99, 2014)

Ainda segundo Fuchs, a autora Jodi Dean destaca que a cultura computacional sempre esteve relacionada a relação entre publicidade e privacidade, segredo e transparência, argumentando que que entre 1950-1960 os primeiros programadores eram uma verdadeira elite que detinha um conhecimento praticamente secreto, posteriormente, nos anos 1970 os hackers desafiaram esta estrutura e passaram a defender que a informação deveria ser livre, com o computador a serviço da população.

Por fim, Dean (2012) afirma que a ascensão do neoliberalismo na década de 1980, fez com que este *ethos* contracultural da informação pública se tornasse uma ideologia do

¹⁶⁹ Autores como Gabriella Coleman e Parmy Olson compreendem o Anonymous como um tipo de “movimento fluído” ou “grupo fluído” em função de sua falta de estrutura ou regras para afiliação.

capitalismo comunicativo, em que a liberdade da rede é também a liberdade do mercado, das corporações, que estendem a força do mercado para o domínio social. (FUCHS;2014, DEAN; 2002)

Assim, Fuchs afirma que o Anonymous converte estas funções em uma organização, como um novo espírito do capitalismo, sem que signifique que o Anonymous suporte a ideologia capitalista, mas as “complexas relações do Anonymous com o capitalismo são cruciais para os valores políticos” (Fuchs, p.100; 2014), representando uma geração mais jovem, moldada pela Internet e toda sua relevância.

A ideia do Anonymous e de seu hacktivismismo ainda está ativa e em evolução.

5. REFERÊNCIAS

- #OPDARKNET Press Release. Anonymous.** 15 out. 2011. Disponível em: < <http://pastebin.com/T1LHnzEW> > Acesso em: 14 nov. 2013
- #OPDARKNET Official Press Release. Pedo hunt trophies, Bear Rugs for Mike Perry.** 30 out, 2011. Disponível: < <http://pastebin.com/qWHDWCRe> > Acesso em: 14 nov. 2013
- A HISTORY OF Anonymous.** Disponível em:< <https://goo.gl/Tk8mCv>> Acesso em : Dez.2013
- A PESQUISA CIENTÍFICA** na Universidade de São Paulo. O Globo,Rio de Janeiro, 09 Mar, 1961. Matutina, Geral, p. 9
- ALBERTS, Gerard, OLDENZIEL, Ruth (org). **Hacking Europe: from computer cultures to demoscenes.** Springer, 2014.
- ALCANTARA, Fernanda Henrique Cupertino. **Economia Solidária: o dilema da institucionalização.** Arte & Ciência, 2005.
- ALMEIDA, Clarissa Ribeiro Pereira de. **Entre e através: complexidade e processos de design em arquitetura-** Universidade de São Paulo. Dissertação (Mestrado em Arquitetura e Urbanismo). 2008. Disponível em: < goo.gl/C9DApb > Acesso em: 16 mar. 2016.
- ASSANGE, Julian. **Cypherpunks: liberdade e o futuro da internet.** Boitempo Editorial, 2015.
- BACHMANN, M. **Deciphering the hacker underground: First quantitative insights.** In T. Holt & B. Schell (Eds.) Corporate hacking and technology-driven crime: Social dynamics and implications (pp. 105-127). Hershey, PA: IGI Global, 2010.
- BAHIANA, Ana Maria. Cyberpunk. O Globo, Rio de Janeiro, 21 mai, 1989. Matutina, Segundo caderno, p. 12.
- BARAN, Paul. **On distributed communications networks.** IEEE transactions on Communications Systems, v. 12, n. 1, p. 1-9, 1964.
- BARLOW, John Perry. **Declaração de Independência do Ciberespaço.** Davos, Suíça.1996
- BARRETO, M.R.P. **As virtudes e os defeitos das publicações.** Folha de São Paulo, São Paulo, 7 out, 1987. Informática, p. B-6
- BECKER, Howard S. **Outsiders: estudos de sociologia do desvio.** Zahar, 2008.
- BERGER, Peter; LUCKMANN, Thomas. **A construção social da realidade.** Petrópolis: Vozes, 1998
- BERGMAN, M.K. **The Deep Web: surfacing hidden value.** 2001. Disponível em < <https://goo.gl/c9q4vj> > Acesso em: 16 nov. 2015.
- BERMAN, Marshall. **Tudo que é sólido desmancha no ar.** Editora Companhia das Letras, 2012.

BERNERS-LEE, T.J., R. CAILLIAU and J.-F. Groff. **The world-wide web, Computer Networks and ISDN Systems** 25 (1992) 454-459.

BEVARD, Charles W. **Five Students Psych Bell System, Place Free Long Distance Calls.** The Crimson. 31 May. 1966

BOBBIO, Norberto, et. al. **Dicionário de Política** - 2 Vols. 13ª Ed. Bolso, UNB, 2011.

BOLTANSKI, Luc; THÉVENOT, Laurent. **On justification: Economies of worth.** Princeton University Press, 2006.

BOLTANSKI, Luc, CHIAPELLO, Ève. **O novo espírito do capitalismo.** WMF Martins Fontes, 2009.

BONAS, Maurício. **Nos livros, todo o charme da tecnologia.** Folha de São Paulo, São Paulo, 1 ago, 1984. Informática, p.27

BRITO, Paulo. **Saiba como escolher uma boa introdução.** Folha de São Paulo, São Paulo, 1 ago, 1984. Informática, p.27

BRAND, Stewart. **Spacewar: Fanatic life and symbolic death among the computer bums.** Rolling Stone, n. 7, p.50-57, 1972

BRASIL. Lei 7.232/84, de 29 de outubro de 1984.

BREEN,C.,DAHLBOM, C. A. **Signaling systems for control of telephone switching.** Bell System Technical Journal ,v.39, n.6, p. 1381-1444, 1960

BRITO, João. **Jogos de ação, bom início para aprender linguagem de máquina.** Folha de São Paulo, São Paulo, 8 mai, 1985. Informática.

BRITO, João Carlos de. **Pais querem computador na vida dos filhos.** Folha de São Paulo, São Paulo, 05 ago, 1987.

BUSH, Vannevar. **Science: the endless frontier: a report to the president on a program for postwar scientific research.** 1945.

CARMO, João Clodomiro. **O impacto sobre a sociedade em poucas mas boas análises.** Folha de São Paulo, São Paulo, 1 ago, 1984. Informática, p.27

CARDOSO, Irene. **A geração dos anos de 1960: o peso de uma herança.** Tempo Social, v. 17,n. 2, p. 93-107, 2005

CARVALHO, Mário César. **Universidade reclama mais lançamentos.** Folha de São Paulo, São Paulo, 01 ago, 1984. Informática.

CARVALHO, M.S.R.M. **A trajetória da Internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança.** Dissertação (Mestrado em Engenharia de Sistemas e Computação)- Universidade Federal do Rio de Janeiro, Rio, RJ,2006. Disponível em: < goo.gl/nE7kk4> Acesso em: 05 set. 2015

CASOS DOS JOGOS de guerra obriga EUA a reverem segurança. Folha de São Paulo, São Paulo, 21 jul, 1985. Exterior, p.2

CASTELLS, Manuel. **A Sociedade em Rede - a era da informação: economia, sociedade e cultura; v.1.** Tradução para o português: Roneide Venancio Majer; atualização para a 6ª edição: Jussara Simões . São Paulo: Paz e Terra. 1999

_____. **O poder da Identidade- - a era da informação: economia, sociedade e cultura; v.2.** Tradução para o português: Klauss Brandini Gerhardt. São Paulo: Paz e Terra. 1999

_____. **A galáxia da Internet.** Rio de Janeiro: Jorge Zahar, 2003;

_____. **Redes de indignação e esperança: movimentos sociais na era da internet.** Jorge Zahar Editor Ltda, 2013.

CHAPUIS, Robert et al. **100 Years of telephone switching.** Part I, Manual and Electro, IOS Press, 2003.

CHEN, Carl. **The creation and meaning of internet memes in 4chan: Popular internet culture in the age of online digital reproduction.** Institutions Habitus Spring (2012): 6-19.

CLARKE, Richard A; **Guerra Cibernética - A próxima ameaça à segurança e o que fazer a respeito,** Rio de Janeiro: Brasport, 2015.

COE, Lewis (1995). **The Telephone and Its Several Inventors: A History,** McFarland, North Carolina, 1995.

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

_____. **. Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous.** Verso Books, 2014.

COLLINS, William Edward. **Queen Elizabeth's defence of her proceedings in church and state.** No. 77. SPCK, 1958.

COMPLETE HISTORY of 4chan. Tanasinn.info. Disponível em < <https://goo.gl/U30OhU>> Acesso em: 10 jan. 2016.

COMPUTADORES. Super Interessante. Nov, 1987 Disponível em: < <http://super.abril.com.br/tecnologia/computadores> > Acesso em: 21 fev 2015

CONFIRA OS IMPACTOS da ditadura militar no Brasil. EBC, 23 mar. 2014. Disponível em < <https://goo.gl/TUlvxD> > Acesso em 20 nov. 2014

COSTA, Pedro. **Hackers dominam sistemas.** O Estado de São Paulo, São Paulo, 21 mai,1988. Geral, p.15

_____. **A invasão dos piratas de computadores.** O Estado de São Paulo, São Paulo, 27 mar, 1988. Ciência, p.21

CLUBES DO COMPUTADOR se multiplicam e atraem nova geração. Folha de São Paulo, São Paulo, 4 nov, 1988. Especial Viva

CRANKS, PRANKS and supermen. Computer Fraud & Security Bulletin. v.4, n.1, p.9-11,1981.

CRESCEM OS CASOS no Brasil. O Estado de São Paulo, São Paulo, 29 ago, 1989. Economia, p.45

DA SILVA, Elisabeth Murillo. **É possível falar de tribos urbanas hoje? A moda e a cultura juvenil contemporânea.** Iara – Revista de Moda, Cultura e Arte, São Paulo: Senac, v. 4, n. 1, p. 47-64, abr. 2011.

DA SILVA, Marco Antonio Rodrigues, XAVIER, Fabio Correa. Deep Web e a Rede Tor: Qual a sua Relação? Instituto Brasileiro de Tecnologia Avançada (IBTA) Revista Phronesis – Ano I – vol. 2 – Nov/2015

DA SILVEIRA, Sérgio Amadeu. **Ciberativismo, cultura hacker e o individualismo colaborativo.** Revista USP 86 (2010): 28-39.

DAWKINS, R. **O gene egoísta.** Belo Horizonte: Editora Itatiaia. Companhia das Letras, 1976, 544 pp

DENNING, Doroth. **Information warfare and security.** 2015

DIBBEL, Julian. **Radical Opacity** .MIT Technological Review. 2010. Disponível em < <https://goo.gl/YzB7qU> > Acesso em: 13 dez. 2014.

DICTIONARIES, Oxford. "Oxford Dictionary of English." (2010).

DODIER, N. **Agir dans plusieurs mondes.** *Critique*, xlvii, 529-530, p. 427-458, 1991

_____. **Les appuis conventionnels de l'action: elements de pragmatique sociologique.** *Réseaux*, 62, p. 63-85, 1993.

EGAN, Matt. What is the Dark Web? How to access the Dark Web. What's the difference between the Dark Web and the Deep Web?. Pcadvisor, UK. 28 abr.2016 Disponível em: < <https://goo.gl/zSFQZV> > Acesso em: 30 abr. 2016

FLORY, David. **The great blue box phone frauds.** IEEE Spectrum, v. 27, n.11, p.117-119, nov. 1990

FONTANELLA, Fernando. **Nós somos Anonymous: anonimato, trolls e a subcultura dos imageboards.** Disponível em:< <https://goo.gl/lRtfMb>> . Acesso em: nov. 2013

FOUCAULT, Michel. **Microfísica do poder.** Rio de Janeiro, Edições Graal, 2010.

FOUR IN FIVE Regard Internet Access as a Fundamental Right: Global Poll, BBC. 2010. Disponível em <<https://goo.gl/jbE1nY> > Acesso em: 10 mar. 2014

GANG DO COMPUTADOR é formada por mais de 600 adolescentes. O Globo, Rio de Janeiro, 19 jul. 1985. Matutina, o Mundo, p.14

GIBSON, William. **Neuromancer.** São Paulo: Aleph, 2008.

GIDDENS, Anthony. "As Consequências da Modernidade .1990.

GIDDENS, Anthony. Sociologia. Porto Alegre: Artmed, 2005.

GILBERTSON, Scott. **Feb. 16, 1978: Bulletin board goes electronic.** Wired.com, 2010.

GOLOVCHENKO, Yevgeny. **Anonymous Facebook page network.** Disponível em: <http://anonymous.hol.es/> Acesso em: Ago.2015.

HALL, Stuart, and Tony Jefferson, eds. **Resistance through rituals: Youth subcultures in post-war Britain**. Psychology Press, 1993.

HAUTSCH, Oliver. **O que é um transistor e porque ele é importante para o computador?** 2010. Disponível em: < <http://goo.gl/iLo6QO> > Acesso em: 19 set. 2015

HEARN, Kay, Rachel J. Mahncke, and Patricia A. Williams. **Culture jamming: from activism to hactivism**. Australian Information Warfare and Security Conference. 2009.

HEARN, Kay, et al. **Culture jamming: From activism to hactivism**. In: Australian Information Warfare and Security Conference. 2009.

HIMANEN, Pekka. **A ética dos hackers e o espírito da era da informação: a diferença entre o bom e o mau hacker**. Campus, 2001.

HISTORY OF Hacking. Disponível em: < <https://goo.gl/2Czict> > Acesso em: Fev.2015

HOBBS, Thomas. **Leviatã**. Editora Abril. Coleção Pensadores (2000).

HOFFMAN, Abbie, et al. **Steal this book**. New York: Pirate editions, 1971.

HOUGHTON, Tessa J. **Hactivism and Habermas: Online protest as neo-Habermasian counterpublicity**. Tese (Doctor of Philosophy)- University of Canterbury, Kent, UK, 2010. Disponível em: < <https://goo.gl/QPz6dE> > Acesso em: 20 dez. 2015

HUGHES, Eric. **The cypherpunk manifesto**, 1993. Disponível em < www.activism.net > Acesso em: 10 dez. 2014.

INTERNET, Rules of. Disponível em:< <https://goo.gl/Oo8jkk> >Acesso em: out.2013

JAMESON, Fredric. **Pós-Modernismo: a lógica cultural do capitalismo tardio**. Tradução para o português : Maria Elisa Cevalco. São Paulo: Ática, 2004

JOBS, Steve. Stanford commencement address. **Speech, Stanford University, Stanford, CA**, v. 14, 2005.

JOHNSON, Allan G. **Dicionário de sociologia**. Rio de Janeiro: Jorge Zahar Editor. 1997

JORDAN, Tim, TAYLOR, Paul. **A sociology of hackers**. The Sociological Review, v.46, n.4, p.757-780, nov.1998. Disponível em: < <http://www.yorku.ca/kitzmann/hackers.pdf> > Acesso em: 20 jan. 2015

_____. **Hackers: crime in the digital sublime**. Psychology press, 1999.

LAPSLEY, Phil. **Exploding the phone: The untold story of the teenagers and outlaws who hacked Ma Bell**. Grove Press, 2013.

_____. **Phreaking out ma bell**. IEEE Spectrum, v.50, n.2, p. 30-35, 2013. Disponível em: < goo.gl/LKZBrK > Acesso em: 11 nov.2015

KELLY, Jon. Jude Sheerin .The strange virtual world of 4chan. Disponível em: <<https://goo.gl/gNGS8Q>> Acesso em: jan.2014.

KIM, Joon Ho. (2004). **Cibernética, ciborgues e ciberespaço: notas sobre as origens da cibernética e sua reinvenção cultural**. Horizontes Antropológicos, 10(21), 199-219

KNAPPENBERGER., Brian. **We are Legion**. Luminant Media. 2012.

KNUTTILA, Lee. **User unknown: 4chan, anonymity and contingency**. First Monday 16.10 (2011). < <http://firstmonday.org/article/view/3665/3055> >

LA RUE, Frank. **Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression**. ONU. 2011. Disponível < <https://goo.gl/0iRvwp> > Acesso em: 16 nov. 2015

LEHMAN, Elvira Vigna. **Piratas da eletrônica julgados nos EUA**. Folha de São Paulo, São Paulo, 04 abr, 1984. Informática

LEBON, Gustave. **Psicologia das multidões**. São Paulo, WMF Martins Fontes 224 (2008).

LEMONS, André, et al. **Hackers no Brasil**. Contracampo. Niteroi, n.6, p. 41-42, 2002. Disponível em < goo.gl/uyAcBI > Acesso em: 16 jul. 2014

LICKLIDER, J.C.R; CLARK, W.E. **On-line man-computer communication**. Proceedings of the May 1-3, 1962, spring joint computer conference. ACM, 1962.

LICKLIDER, Joseph CR. **Man-computer symbiosis**. IRE transactions on human factors in electronics, n. 1, p. 4-11, 1960.

LÉVY, Pierre. **Cibercultura**. Tradução para o português: Carlos Irineu da Costa. São Paulo: Editora 34, 1999.

LÉVY, Steven. **Hackers: Heroes of the computer revolution**. Vol. 4. New York: Penguin Books, 2001.

LEVY, Steven. **Os heróis da revolução: como Steve Jobs, Steve Wozniak, Bill Gates, Mark Zuckerberg e outros mudaram para sempre as nossas vidas**. Tradução para o português: Maria Cristina Sant'Anna São Paulo: Évora (2012).

LICHSTEIN, Henry. **Telephone Hackers Active**. The Tech, v. 43, n. 20, p.20, 1963.

MACHADO, Murilo. **Por dentro do Anonymous Brasil: poder e resistência na sociedade de controle**. Dissertação (Mestrado pelo Curso de Ciências Humanas e Sociais)- Universidade Federal do ABC, Santo André, SP, 2013. Disponível em: < <https://goo.gl/uMX7z1> > Acesso em: 20 abr. 2015.

MADDOX, Brenda. **Women and the switchboard**. In The social impact of the telephone (1977): 262-80.

MALONE, Michael S. **Intel Trinity, The: How Robert Noyce, Gordon Moore, and Andy Grove Built the World's Most Important Company**. Harper Collins, 2014.

MCLUHAN, Marshall. **Os meios de comunicação: como extensões do homem**. Editora Cultrix, 1974.

MARTIN, Douglas. **Joybubbles, 58, Peter Pan of Phone Hackers, Dies**. The New York Times, New York, 20 Ago. 2007. Disponível em: < goo.gl/f1EJ9b > Acesso em: 22 fev. 2015

MARTINS, Ana Maria. **Ladrão eletrônico, um tipo que começa a preocupar**. O Globo, Rio de Janeiro, 14 out. 1985. Economia, p.21

MARX, Karl. **O 18 de Brumário de Luís Bonaparte**. São Paulo, Boitempo Editorial, 2011.

MAIS 623 MENINOS participaram dos “Jogos de Guerra”? . O Estado de São Paulo, São Paulo, 19 jul, 1985. Geral, p.7.

MÁSCARA DO ANONYMOUS remete a figura histórica do século 17. Disponível em: <http://www1.folha.uol.com.br/fsp/tec/tc2906201104.htm> Acesso em: jan.2014.

MATTELART, Armand, SCHMUCLER,Héctor. **América Latina en la encrucijada telemática**. México: Fólios, 1983.

MATTOS, Erica Azevedo da Costa et al. **Ethos hacker e hackerspaces: práticas e processos de aprendizagem, criação e intervenção**. Dissertação (Mestrado pelo Programa de Pós-Graduação em Urbanismo, História e Arquitetura da Cidade)- Universidade de Santa Catarina, Florianópolis, SC, 2014. Disponível em: < goo.gl/vOxFIN> Acesso em: 22 mar. 2015

MEDEIROS, Jota.B. **Yes, nós não temos cybeprpunk**. O Estado de São Paulo, São Paulo, 01 nov, 1987. Caderno 2, p.59.

MELO, Alice. **O Nascimento de uma nação**. Revista de história.com.br. 2012. Disponível em:< <https://goo.gl/kRd2um> > Acesso em: 27 fev. 2016

MENTOR, The. **The Hacker’s Manifesto: The Conscience of a Hacker**. 8 jan. 1986. Disponível em: < <http://phrack.org/issues/7/3.html#article>> Acesso em: 10 abr. 2014.

MENTOR, The. **The Conscience of a Hacker**. Disponível em: <http://phrack.org/issues/7/3.html>MARX, Karl. **O 18 Brumário de Luís Bonaparte**, Boitempo Editorial, São Paulo.

MILLS, Elinor. **Old-time hacktivists: Anonymous, you've crossed the line..** Cnet, 30 mar. 2012. Disponível < <https://goo.gl/8fDo4s> > Acesso em 25 abr. 2016

MOON, David. **Hacking Politics: how geeks, progressives, the Tea Party, gamers, anarchists and suits teamed up to defeat SOPA and save the internet**. New York/London: OR Books. 358p. 2013.

MOORE, Alan. **V de vingança** Panini books, 2012

MUNGO, Paul; CLOUGH, Bryan. **Approaching zero: the extraordinary underworld of hackers, phreakers, virus writers, and keyboard criminals**. Random House Inc., 1993.

OAD, CRANK AND CLODO on the warpath. Computer Fraud & Security Bulletin.v.2, n.7, p.10-12,1980.

OKLAHOMA, Ray. **Regulating The Phone Company In Your Home**. Ramparts Magazine, Jun. 1972 Disponível em: < <http://explodingthephone.com/docs/dbx0431.pdf> > Acesso em: 15 fev. 2015

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**, adotada em 10 de dezembro de 1948.

OKLAHOMA, Ray. **Regulating The Phone Company In Your Home**. Disponível em: <https://goo.gl/YM6Ubf> Acesso em: Jul.2015

OLSON, Parmy. **We Are Anonymous**. Random House, 2013.

O PENTÁGONO REVISA sistemas eletrônicos. O Estado de São Paulo, São Paulo, 21 jul, 1985. Geral, p.10.

OPPENHEIMER, Walter. **O Reino Unido se rebela contra os abusos de pedófilos com poder e fama**. El Pais, Londres, 20 jul. 2014. Disponível em < <https://goo.gl/LjjLQM> > Acesso em: 15 nov. 2015

ORTH, Maureen. **For Whom Ma Bell Tolls Not**. Los Angeles Times (1886-Current File); Oct 31, 1971; ProQuest Historical Newspapers Los Angeles Times (1881 - 1985) p. P28. Disponível em: < goo.gl/0PndEa> Acesso em: 15 dez. 2014

OS ROBIN HOODS da era eletrônica. Folha de São Paulo, São Paulo, 1 set, 1983. Antena, p. 24

PACIORNIK, Guilherme Flynn et al. **Movimentos sociais e as novas Tecnologias da Informação e Comunicação: um estudo de caso na zona sul da cidade de São Paulo, a Casa dos Meninos**. Dissertação (Mestrado em Sociologia)- UNICAMP, São Paulo, Sp, 2013. Disponível em: <<http://goo.gl/514k6y>> Acesso em: 30 jun. 2015

PAGET, François. **Hacktivismo: O ciberespaço tornou-se a nova mídia para vozes políticas**. McAfee Labs. 2012. Disponível em < <https://goo.gl/4t0PLU> > Acesso em: 05 out. 2015.

PAIS, José Machado; et al. **Tribos urbanas: produção artística e identidades**. Annablume, 2004.

PEIRCE, Charles Sanders. **Logical machines**. American Journal of Psychology, vol. 1, 1887, pp. 165-70. Tradução comentada de: CESTARI, Guilherme Henrique de Oliveira; GAZONI, Ricardo Maciel; NÖTH, Winfried. Teccogs: Revista Digital de Tecnologias Cognitivas, TIDD PUC-SP, São Paulo, n. 10, p. 20-47, jul-dez. 2014

PERRY, Barlow John. **A Declaration of the Independence of Cyberspace**. Electronic Frontier Foundation (EFF), Fev. 8, 1996. Disponível em: < goo.gl/PFIQxD > Acesso em: 11 nov. 2014.

PETERS, Benjamin. **How Not to Network a Nation: The Uneasy History of the Soviet Internet**. MIT Press, 2016.

PIAZZI, Pierluigi. **Dominando o MSX**. 1987. Disponível em: <<https://youtu.be/w28b6elAHho>> Acesso em: 03 jan. 2016

_____. **Video Aula de MSX Basic** . 1987. Disponível em: < <https://youtu.be/UeEEWKtrfPg> > Acesso em: 03 jan. 2016

PIRATAS DA INFORMÁTICA juntos na Holanda. O Globo, Rio de Janeiro, 04 ago. 1983. Matutina, o Mundo, p.14.

PIRATAS DA INFORMÁTICA atacam o monopólio. O Globo, Rio de Janeiro, 6 ago, 1989. Matutina, O mundo, p.37

POLÍCIA INVADE CASAS de piratas de computador. O Globo, Rio de Janeiro, 30 set. 1987. Matutina, o Mundo, p.17

POPPE, Ine. **Hippies from Hell.** 2001. Documentário.

POOLE, Hilary W. et al. (Ed.). **The Internet: a historical encyclopedia.** Abc-Clio Inc, 2005.

POWANSKI, Ronald (2000): **La Guerra Fría. Estados Unidos y la Unión Soviética, 1917-1991** Crítica, Barcelona.

PRISÃO DE JOVENS revela fragilidade do Pentágono. Folha de São Paulo, São Paulo, 24 jul, 1985. Informática, p.30

RAYMOND, Eric S. **A brief history of hackerdom."** DiBona, Ockman y Stone, Open Sources, Disponível em: [www.tuxedo.org/~ esr/writings/cathedral-bazaar/hacker-history/](http://www.tuxedo.org/~esr/writings/cathedral-bazaar/hacker-history/) (primera versión 1992) (1999). Acesso em 12 dez 2014.

REIS, Edgardo Costa. **Hackers, mais de mil piratas de computador preocupam os EUA.** O Globo, Rio de Janeiro, 28 jul. 1985. Matutina, O mundo, p.30

_____. **Quadrilhas do computador já ameaçam matar.** O Globo, Rio de Janeiro, 09 dez. 1984. Matutina, O mundo, p.30

ROSENBAUM, Ron. **Secrets of the little blue box.** Esquire Magazine, v. 76, p. 117-125. 1971.

ROMANO, Michael. **The politics of hacking.** Spin. p. 168. 1999.

RUFFIN, Oxblood. **Hacktivism, From Here to There.** 2004. Disponível em: < http://www.cultdeadcow.com/cDc_files/cDc-0384.php > Acesso em: 30 mar 2016

SAMUEL , Alexandra Whitney. **Hacktivism and the future of political participation.** 2004. Thesis (to the Department of Government in partial fulfillment of the requirements for the degree of Doctor of Philosophy in the subject of Political Science) - Harvard University Cambridge, Massachusetts, 2004. Disponível em: < goo.gl/WLCL5B > Acesso em: 01 out. 2015

SANTOS, José Rodrigues dos. **A propósito das noções de ‘problema social e problema sociológico.** Universidade de Évora, Departamento de Sociologia, CIDEHUS (1999). Disponível em: < goo.gl/fASaQp > Acesso em: 14 mar. 2016.

SHILOV, Valery V., SILANTIEV, Sergey A. **Reasoning vs. Orthodoxy, or, The Lesson from the Fate of Russian “Reasoning Machine.** In: **IFIP International Conference on Human Choice and Computers.** Springer Berlin Heidelberg, 2014.

SHUMAN, Phil (July 26, 2007). "FOX 11 Investigates: 'Anonymous'". MyFOX Los Angeles (KTTV (Fox)) Disponível em: <https://youtu.be/DNO6G4ApJQY> Acesso em: nov. 2012

SILVA, Elisabeth Murilho da. **É possível falar em tribos urbanas hoje? A moda e a cultura juvenil contemporânea.** Iara: Revista de Moda, Cultura e Arte, 2011

SIMMEL, Georg. **Questões fundamentais da sociologia.** Zahar, 2006.

_____. **Conflict and the web of group affiliations.**" Trans. K. Wolff and R. Bendix. New York: Free Press. 1995

SOBOTTKA, Emil, SAAVEDRA, Giovani. **Justificação, reconhecimento e justiça: Tecendo pontes entre Boltanski, Honneth e Walzer** . Civitas - Revista de Ciências Sociais. v. 12, n. 1, 2012.

SPINK, Henry Hawkes. **The Gunpowder Plot and Lord Mouteagle's Letter.** Goodale Press, 2010.

STERLING, Bruce. **Mirrorshades: The cyberpunk anthology.** New York, Ace Books, 1988.

_____. **The hacker crackdown: law and disorder on the electronic frontier.** New York, Bantam Books, 1994.

STREETER, Thomas. **The net effect: Romanticism, capitalism, and the Internet.** NYU Press, 2011.

TAPIAS, José Antonio Pérez. **Internautas e naufragos: a busca do sentido na cultura digital.** Edições Loyola, 2006.

TAYLOR, Paul A. **Hackers: crime in the digital sublime.** Psychology press, 1999.

TER-GHAZARYAN, Aram. **Computers in the USSR: A story of missed opportunities.** Russia Beyond The Headlines, 24 sep. 2010. Disponível em: < goo.gl/kDb2Dy > Acesso em: 15 ago. 2015

THE GUNPOWDER PLOT Disponível em: http://www.bbc.co.uk/history/the_gunpowder_plot Acesso em: jan.2013

THE JARGON File (version 4.4.7) Disponível em: < <http://www.catb.org/jargon/html> > Acesso em: 20 mar. 2015

THE POLITICS OF Hacking. SPIN, 1999

TOUSSAINT, F. y Esteinou Madrid, J. **Las perspectivas en America Latina.** Telos N° 15. Septiembre, Noviembre 1988.

TRIGGS, Teal. **Scissors and glue: Punk fanzines and the creation of a DIY aesthetic.** Journal of Design History. v. 19, n.1, p-69-83. 2006

TURING, Alan M. **Computing machinery and intelligence.** Mind, v. 59, n. 236, p. 433-460, 1950.

TURNER, Fred. **From counterculture to cyberculture: Stewart Brand, the Whole Earth Network, and the rise of digital utopianism.** University Of Chicago Press, 2010.

TURGEMAN-GOLDSCHMIDT, Orly. **Between Hackers and White-Collar Offenders.** In: HOLT, Tomas et al. **Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications.** IGI Global, 2010.

UIT: 3,7 bilhões de pessoas ainda não têm acesso à Internet no mundo. ONU, 22 jul. 2016. Disponível em: < <https://goo.gl/Lq3EVG> > Acesso em: 29 jul. 2016

VANDENBERGUE, Frédéric . **Construção e crítica na nova sociologia francesa**. *Soc. estado*. 2006, vol.21, n.2, pp.315-366. Disponível em: < <https://goo.gl/9jqV2f> > . Acesso em: mai. 2016.

VARGAS, J. A. **Spring Awakening. How an Egyptian Revolution Began on Facebook**. The New York Times , New York, 17 fev. 2012. Disponível em: < <https://goo.gl/1AkHPr> > Acesso em: 15 fev. 2014

VILBIG, Kevin. **Hack All The History! Hackers 1959-1991**. Bachelor of Science in University Honors and Social Science Richard Beyler Portland State University, 2013 Disponível em: < goo.gl/IGA9Wn > Acesso em: 03 dez. 2015

WAINBERG, Jacques A. **Revolucionários, mártires e terroristas: a utopia e suas consequências**. Paulus. 2015.

WARGAMES. Direção: John Badham. [S.l.]: MGM/UA Home Entertainment, 1983. 1 DVD (114 min).

WEAVER, A., NEWELL, N. A. **In-Band Single-Frequency Signaling**. Bell System Technical Journal, v. 33, n.6, p. 1309-1330,1954.

_____. **Signal-Frequency Signaling System for Supervision and Dialing over Long-Distance Telephone Trunks**. Transactions of the American Institute of Electrical Engineers, v.70, n.1, p. 489-495, 1951

WEISSKOPF, Carmen, et al. **Shopping on the dark net**. New Scientist, v. 228, n. 3052, p. 41, 2015.

WEIZENBAUM, Joseph. **O poder do computador e a razão humana**. Lisboa: Edições, v. 70, 1976.

WESOLOWSKI, Sébastien .**Une brève histoire des imageboards**. Motherboard. 8 ago. 2016. Disponível em: <<https://goo.gl/wtCkZR>> Acesso em: 20 ago. 2016

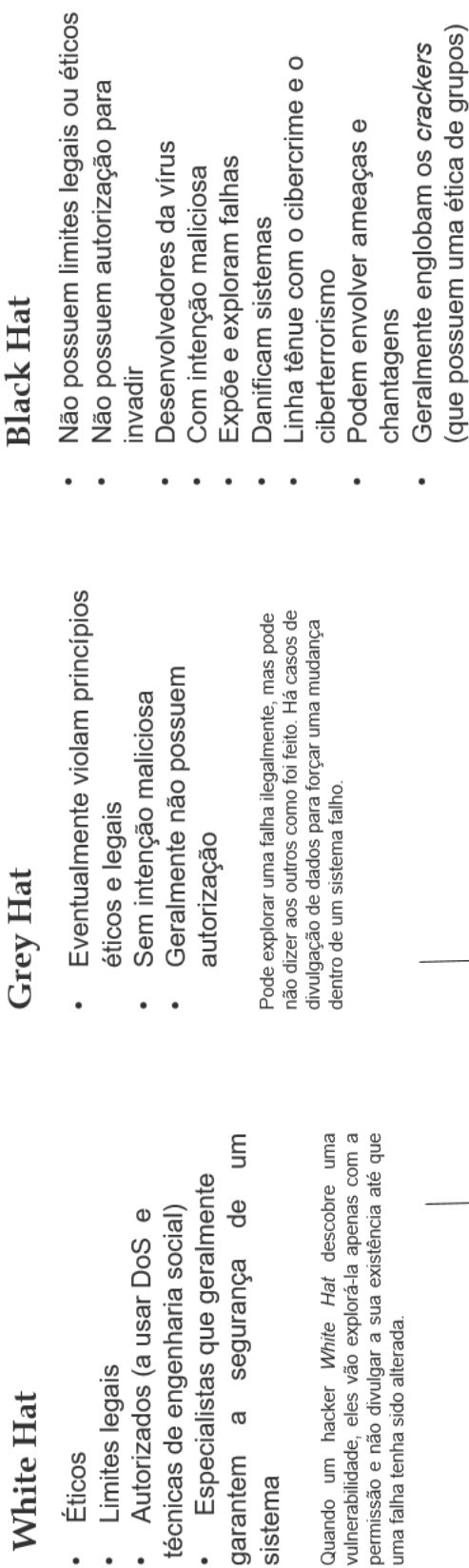
YIPL (TAP Magazine). **Youth International Party Line First Issue**. jun. 1971.Disponível em:

< <http://flag.blackened.net/daver/misc/yipl/yipl1.html> > Acesso em: 30 jun, 2015

ZAPPA, Regina, et al. **1968: Eles só queriam mudar o mundo**. Rio de Janeiro: Ed. Jorge Zahar. 2008.

ANEXO 01: Modelo Básico de Tipologia dos Hackers.

3 tipos de Hackers (além dos desenvolvedores, programadores e hackers em seu sentido ampliado)



ANEXO 02 : Modelo básico de Entrevista

Anonymous Research**Anonymous Name:****Country:****Gender:** Male Female No matter**Age:** No matter**You are:** Activist Hacktivist Ciber-activist Simpatizyng Other:**About your political direction:** Anarchist Democrat Republican Other**When you join in Anonymous and why?****Do you agree with your government? Why?****Do you think that Anonymous have a ideology?****Do you feel represented by your government?** Yes No**Do you feel safe with the police?** Yes No**What is the best political system in your opinion?****What is your biggest fear or concerns:** Heathcare Service Corruption Freedom Education War The politicians Police Violence Ecological Human Rights Economical System Democracy Political party Ciberviolence Religion

Others:

How many operations do you act? And which one?**How do you collaborate with Anonymous (with pages, sharing information, hacking?)****How do you think that your government and society see Anonymous? And how do you see yourself?****What is the most important to you:** Individual Motivation Collective**How Anonymous change you ?**