REVISTA ECO PÓS | ISNN 2175-8889 | CINEMA EXPERIMENTAL | V 19 | N.2 | 2016 | PERSPECTIVA

A trajetória cypherpunk e suas práticas discursivas

The cypherpunk way and their discursive practices

Sérgio Amadeu Silveira

Professor Adjunto 3 do Centro de Engenharia, Modelagem e Ciências Sociais Aplicadas, da Universidade Federal do ABC.
Email: samadeu@gmail.com

Submetido em: 18/08/2015
Aceito em: 23/03/2016

PERSPECTIVA

RESUMO

O texto tem por objetivo analisar a prática discursiva de um tipo específico de ciberativismo denominado cypherpunk. A partir da reunião de manifestos e listas de discussões de importantes coletivos cypherpunks, foram analisadas suas principais narrativas. A hipótese que dirigiu a investigação foi a de que a origem libertária e anarcocapitalista do ideário cypherpunk foi sendo alterada principalmente após o 11 de setembro. Os discursos e as propostas de ação de relevantes agrupamentos cypherpunks foram se aproximando dos movimentos globais de contestação mais próximos das forças de esquerda.

PALAVRAS-CHAVE: *Cypherpunk*; ciberativismo; criptografia; cultura hacker; privacidade.

ABSTRACT

The text aims to analyze the discursive practice of a specific type of cyber activism called cypherpunk. There were analyzed manifestos and lists of important collective discussions cypherpunks. The hypothesis that directed the research was that the libertarian and anarcho-capitalist origin of cypherpunk ideology was mainly being changed after 11 September. The speeches and proposals of relevant cypherpunks action groups were closer to the global movements of left-wing politics forces.

KEYWORDS: cypherpunk; cyber activism; encryption; hacker culture; privacy.

REVISTA ECO PÓS | ISNN 2175-8889 | CINEMA EXPERIMENTAL | V 19 | N.2 | 2016 | PERSPECTIVA

A participação política ganhou novas formas de ação com a expansão do uso das redes informacionais. Na última década do século XX, observa-se o surgimento de expressões como ativismo *online*, ciberativismo (Vegh, 2009, p.73), ativismo *hacker* ou hacktvismo (Von Busch, 2006, p. 16) para tratar de ações nas redes digitais vinculadas à tradição anarquista, autonomista e aos movimentos culturais tecnológicos envolvidos em ações diretas e de resistência, tais como o apoio ao movimento antiglobalização e à guerrilha zapatista no sul do México.

Um *hacker* é uma pessoa com conhecimentos avançados de sistemas informacionais, exímios desenvolvedores de códigos e de soluções para problemas lógicos complexos (Raymond, 2001, *online*). *Hackers* buscam se diferenciar daqueles que usam tais habilidades apenas em benefício pessoal ou para cometer crimes, chamando-os de *crackers*. Alguns *hackers* se envolvem em ações políticas e participam da luta em defesa de causas que consideram importantes e podem ser chamados de hacktvistas (Wray, 1998). Por dominarem tecnologias cibernéticas e utilizá-las para as ações políticas em rede também podemos compreender o hacktvismo como um tipo de ciberativismo, expressão muito utilizada por pesquisadores da área de cibercultura (Silveira, 2010, p. 33).

Este texto trata de um tipo específico de ciberativismo, denominado de *cypherpunk,* que ganhou destaque mundial principalmente a partir das denuncias realizadas pelo *Wikileaks*[1], obtendo ainda mais projeção após as revelações de Edward Snowden, o ex-agente da inteligência dos Estados Unidos que divulgou detalhes sobre o sistema de vigilância massiva praticado pela NSA, agência de espionagem digital norte-americana. A investigação aqui exposta pretende mostrar uma modalidade de ativismo e de engajamento político específica, bem como suas relações ambivalentes com o discurso de esquerda ao mesmo tempo em que os componentes fundamentais do pensamento *cypherpunk* recebem influência direta do ultraliberalismo ou anarcocapitalismo de matriz norte-americana.

1. O que caracteriza os *cypherpunks*

O *cypherpunk* é um ativista que defende o uso generalizado da criptografia[2] forte como caminho para a mudança social e política. Existe um movimento *cypherpunk* ativo desde os anos de 1990, influenciado pela cultura *hacker* e pelas ideias libertárias. Ganhou destaque o empenho de Philip Zimmermann, em 1991, ao desenvolver e distribuir o *software* PGP[3] com a intenção de dar acesso à criptografia para todos (Singh, 2002,

1 O *Wikileaks* é uma organização independente de mídia que busca expor as informações que os Estados e grandes corporações buscam esconder da opinião pública. Foi fundada por Julian Assange, em 2006. Informações podem ser obtidas no *site* do *Wikileaks* https://wikileaks.org.

2 Segundo a Cartilha de Segurança do Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil, cert.br, "a criptografia, considerada como a ciência e a arte de escrever mensagens em forma cifrada ou em código, é um dos principais mecanismos de segurança que você pode usar para se proteger dos riscos associados ao uso da Internet". Disponível em: http://cartilha.cert.br/criptografia/. Acesso em: 10/03/2016.

3 PGP é o acrônimo de *Pretty Good Privacy* que poderia ser traduzido como privacidade muito boa. O PGP popularizou a criptografia permitindo que textos e *e-mails* fossem cifrados e decifrados por pessoas comuns.

p. 321-329). Durante a maior parte da década de 1990, havia uma lista de discussão *cypherpunk* extremamente ativa. Grande parte dos *cypherpunks* estava envolvida em intensas controvérsias políticas e jurídicas relativas ao direito de uso da criptografia. Os coletivos *cypherpunks* estão crescendo em todo o mundo e sendo chamados a participar da luta política em defesa da privacidade, do anonimato e da liberdade nas redes digitais.

Timothy C. May, ou Tim May, foi engenheiro eletrônico e cientista da Intel desde os primórdios da empresa até 2003, quando se aposentou (Ludlow, 2001, p. 4-6). Escreveu sobre tecnologia e política, sendo um dos fundadores mais ativos da lista de correio eletrônico dos *cypherpunks*. A partir da década de 1990, Tim May redigiu textos importantes sobre proteção de informações e a questão da privacidade. Em 1994, May lançou, na lista de correio eletrônico que ajudou a criar, o FAQ[4] sobre os *cypherpunks* denominado *The Cyphernomicon: Cypherpunks FAQ and More, Version 0.666*. Nele, além da história dos *cypherpunks*, Tim May tratou de vários temas do universo do ativismo, da criptografia e dos fundamentos do que seria sua doutrina política. É autor do *Crypto Anarchist Manifesto* que analisaremos adiante.

Quais os pontos centrais da doutrina *cypherpunk*? Existem elementos unificadores daqueles que se autodenominam *cypherpunks*? May escreveu no *The Cyphernomicon* que sua observação dos comentários e dos debates na lista de discussão o levava a acreditar que os *cypherpunks* possuem uma série de convicções e crenças em torno de pontos importantes:

> — Que o governo não deve ser capaz de espionar as atividades das pessoas;
> — Que a proteção de conversas e negociações das pessoas é um direito básico;
> — Que esses direitos podem ser assegurados pela tecnologia e não somente pelas leis;
> — Que o poder da tecnologia muitas vezes cria novas realidades políticas (daí o mantra: *cypherpunks* escrevem códigos)[5] (May, 1994, *online*).

Uma análise dos recursos narrativos empregados por May evidencia claramente a desconfiança dos governos e a crítica ao poder estatal de vigilância sobre as pessoas. Como a lei do Estado não pode garantir o direito à privacidade, uma vez que o governo é o grande interessado na coleta de informações de seus cidadãos, os *cypherpunks* enaltecem o uso da tecnologia como forma política de assegurar esse direito. A tecnologia é então um recurso claramente político e pode alterar o jogo de poder.

A afirmação da tecnologia como portadora de um poder político positivo, ou seja, da capacidade de criar e alterar as realidades sociais e de mudar o jogo de forças, parece estar no terreno de um certo determinismo tecnológico. Todavia, uma leitura mais profunda dos textos de May, e de outros importantes *cypherpunks*, indica que a rotulação de determinismo deve ser atenuada, pois defendem o desenvolvimento de soluções de criptografia forte exatamente para vencer os defensores do controle. Assim, o que existe é um jogo entre grupos que desenvolvem tecnologia. Há aqueles que querem ampliar a capacidade dos Estados em controlar as pessoas e há os que escrevem códigos para permitir que os indivíduos fujam desses controles opressivos. A

4 FAQ na linguagem da Internet é uma lista de perguntas e respostas mais frequentes sobre um dado assunto.

5 Livre tradução para: 3.4.1. "Is there a set of beliefs that most Cypherpunks support?" + There is nothing official (not much is), but there is an emergent, coherent set of beliefs which most list members seem to hold: - that the government should not be able to snoop into our affairs; - that protection of conversations and exchanges is a basic right; - that these rights may need to be secured through technology rather than through law; - that the power of technology often creates new political realities (hence the list mantra: "Cypherpunks write code")". Link: http://cypherpunks.to/faq/cyphernomicron/chapter3.html#2. Acesso em: 10/03/2016.

REVISTA ECO PÓS | ISNN 2175-8889 | CINEMA EXPERIMENTAL | V 19 | N.2 | 2016 | PERSPECTIVA

tecnologia parece ser mais ambivalente e passível de disputa social.

Em oposição às ideias de May, Dorothy E. Denning, uma importante pesquisadora de segurança da informação norte-americana, considera os *cypherpunks* uma ameaça, principalmente a vertente cripto-anarquista, devido à sua capacidade tecnológica combinada com seus objetivos anti-estatais. Denning escreveu:

> Considerando o crescimento explosivo das telecomunicações e do mercado de criptografia, será necessário observar de perto o impacto da criptografia na aplicação da lei. Se a criptografia à prova de governo começar a minar a capacidade das agências para a aplicação da lei, para realizar as suas missões e combater o crime organizado e o terrorismo, então os controles legislativos sobre a tecnologia de criptografia podem ser desejáveis. Uma possibilidade seria licenciar produtos de criptografia, mas não a sua utilização. Certificados podem ser concedidos apenas para os produtos que satisfaçam razoavelmente aplicação da lei e exigências de segurança nacional para a descodificação de emergência e fornecer a proteção de privacidade para os usuários"[6] (Idem, 2001, p. 97).

O que está em questão aqui é o poder soberano. O Estado deve ter um poder ilimitado diante da sociedade? No seu território, o Estado reivindica um poder total sobre a vida dos indivíduos. Existem razões de Estado que clamam pelo controle das populações e de seus desviantes. Tais razões se justificam também diante das razões dos outros Estados, pois a lógica da força é, em última instância, o que pode decidir os contenciosos sem instituições de poderes superior. Aqui, o discurso *cypherpunk* que apela pela defesa da sociedade, só vê a possibilidade dessa defesa se realizar mediante a completa submissão dos seus indivíduos, em todas as esferas da vida, à estrutura estatal, fato notoriamente conhecido, debatido e tratado pela Ciência Política. O discurso *cypherpunk* nasce contestando o poder irrestrito do Estado.

O nascimento do ativismo e dos coletivos *cypherpunks* estão estreitamente vinculados à perspectiva anarcocapitalista ou libertária norte-americana. Em 1993, um breve texto chamado *A Cypherpunk's Manifesto* foi fundamental para a consolidação da primeira comunidade que a partir da perspectiva libertária via na criptografia um uso político. Foi escrito por Eric Hughes, matemático que no início de 1990 esteve na Universidade da Califórnia, em Berkeley. Hughes foi um dos articuladores do movimento *cypherpunk* junto a Timothy C. May e John Gilmore.

> ... A privacidade em uma sociedade aberta também exige criptografia. Se eu disser alguma coisa, quero ser ouvido apenas por aqueles a quem eu desejo que ouçam. Se o conteúdo do meu discurso está disponível para o mundo, não tenho privacidade. Criptografar é indicar o desejo de privacidade e cifrar com criptografia fraca é indicar um fraco desejo de privacidade.
> (...)
> Não podemos esperar que os governos, empresas ou outras grandes organizações sem

6 Livre tradução para: "Considering the explosive growth of telecommunications and the encryption market, it will be necessary to closely watch the impact of encryption on law enforcement. If government-proof encryption begins to undermine the ability of law-enforcement agencies to carry out their missions and fight organized crime and terrorism, then legislative controls over encryption technology may be desirable. One possibility would be to license encryption products but not their use. Licenses could be granted only for products that reasonably satisfy law-enforcement and national security requirements for emergency decryption and provide privacy protections for users".

REVISTA ECO PÓS | ISNN 2175-8889 | CINEMA EXPERIMENTAL | V 19 | N.2 | 2016 | PERSPECTIVA

rosto nos conceda a privacidade por sua caridade[7] (Hugues, 1993, online).

Hugues trouxe uma importante desconfiança não somente de governos, mas também de "empresas ou outras grandes organizações". Há um certo mal-estar em relação às instituições que ganham poder, seja político, econômico ou social, em geral. O indivíduo e sua privacidade parece ser alvo dos ataques das grandes instituições modernas, o Estado e as firmas. O anonimato e a defesa da privacidade aparecem como grandes direitos a se defender. Em nenhum momento o Manifesto chama a uma ação nos parlamentos ou à mobilização coletiva pela aprovação de leis ou pela pressão contra governos intrusos e que executam a vigilância. Para os *cypherpunks*, todos os governos são constituídos para controlar e vigiar os indivíduos. A política em defesa dos direitos individuais passa pelo uso da tecnologia. Os *cypherpunks* são coletivos que, de certo modo, pretendem dar aos indivíduos conscientes dos ataques às suas liberdades uma alternativa de enfrentamento do poder.

Umas das principais ideias dos *cypherpunks* é desenvolver tecnologias que tenham a capacidade de enfrentar o enorme poder das instituições e de dar às pessoas condições de resistir. O primeiro parágrafo do Manifesto escrito por Hugues define a primazia do indivíduo diante do Estado ao afirmar a importância do direito à privacidade. A privacidade concretiza a vontade do indivíduo de não ser visto, ouvido ou controlado por nenhuma instituição. Para Hugues, "a privacidade é o poder de se revelar seletivamente ao mundo"[8] (Hugues, 1993). O poder é visto como a capacidade de garantir uma vontade diante de ações opostas. Esse poder é exercido pela inteligência criptográfica, pelas possibilidades de encontrar soluções que anulem a força de estruturas gigantescas. Uma frase que consta no livro *Cypherpunks*, de Julian Assange, vinte anos após o lançamento do Manifesto de Hugues, dita por Jacob Appelbaum[9], esclarece as possibilidades da tecnologia diante do poder: "a força de praticamente todas as autoridades modernas provém da violência ou da ameaça de violência. É preciso reconhecer que, com a criptografia, nem toda a violência do mundo poderá resolver uma equação matemática" (Assange, 2013, p. 80).

> Nós os *cypherpunks* nos dedicamos à construção de sistemas anônimos. Estamos defendendo nossa privacidade com criptografia, com sistemas de encaminhamento de e-mail anônimos, com assinaturas digitais e com o dinheiro eletrônico. *Cypherpunks* escrevem códigos. (...) Nosso código é livre para todos usarem, em todo o mundo. Nós não nos importamos se você não aprova o software que escrevemos. Sabemos que o software não pode ser destruído e que um sistema amplamente disperso não pode ser desligado. A criptografia vai inevitavelmente se espalhar por todo o mundo e com ela os sistemas de transações anônimas que torna possível. (…) Para a privacidade ser generalizada deve ser parte de um contrato social. As pessoas devem buscar juntas implantar esses sistemas para o bem comum. Privacidade aplica-se apenas na medida em que existe a cooperação dos semelhantes na sociedade[10] (Hugues, 1993).

7 Livre tradução para: "Privacy in an open society also requires cryptography. If I say something, I want it heard only by those for whom I intend it. If the content of my speech is available to the world, I have no privacy. To encrypt is to indicate the desire for privacy, and to encrypt with weak cryptography is to indicate not too much desire for privacy. (...) We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence".

8 Livre tradução para: "Privacy is the power to selectively reveal oneself to the world".

9 Appelbaum é desenvolvedor do anonimizador de navegação na Internet chamado TOR.

10 Livre tradução para: "We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography,

REVISTA ECO PÓS | ISNN 2175-8889 | CINEMA EXPERIMENTAL | V 19 | N.2 | 2016 | PERSPECTIVA

Para os coletivos *cypherpunks*, desenvolver tecnologia é também um ato de libertação. Apesar da postura que enaltece o programador individual, o *cypherpunk* incentiva e pratica a distribuição das tecnologias que cria para uso livre, portanto, sua ação individual é voltada para a construção de "sistemas para o bem comum". Tal como na cultura *hacker*, os *cypherpunks* praticam o individualismo colaborativo (Silveira, 2010, p.38). Apesar desse espírito colaborativo, o compartilhamento do conhecimento e das técnicas de criptografia não retiram a primazia do indivíduo que é cultuada pelos *cypherpunks*.

A análise discursiva dos principais textos dos *cypherpunks* evidencia a sua intrínseca ligação com a doutrina anarcocapitalista, que, por sua vez, não pode ser resumida em um único autor ou em um conjunto único de proposições. O que parece ser típico das doutrinas anarcocapitalistas é o fato de todas elas defenderem a liberdade de contratos entre indivíduos, a liberdade irrestrita de mercado e as possibilidades de vida social sem Estado (Friedman, 1973; Tucker, 1926); Nozic, 1991). Lançado antes do *A Cypherpunk's Manifesto*, redigido por Eric Hugues, em 1993, o texto *The Crypto Anarchist Manifesto*, escrito por Tim May, em 1992, contém uma evidente adesão ao pensamento anarcocapitalista:

> Um espectro ronda o mundo moderno, o espectro da criptoanarquia. A tecnologia computacional está à beira de fornecer a capacidade para os indivíduos e grupos se comunicarem e interagirem uns com os outros de uma forma totalmente anônima. Duas pessoas podem trocar mensagens, conduzirem empreendimentos e negociar contratos eletrônicos sem saber o nome verdadeiro ou a identidade legal um do outro. Interações em redes serão irrastreáveis, via um extensivo reencaminhamento de pacotes criptografados e tecnologias à prova de violação com a implementação de protocolos de criptografia com garantia quase perfeita contra qualquer adulteração. Reputações terão importância central, muito mais do que as obtidas nos índices de classificação de crédito atuais. Esses desenvolvimentos irão alterar completamente a natureza da regulamentação do governo, a capacidade de taxar e controlar as interações econômicas, a capacidade de manter a informação em segredo, e até mesmo irão alterar a natureza da confiança e da reputação[11] (May, 1992, *online*).

The Crypto Anarchist Manifesto marca o seu início apostando na adesão dos indivíduos e grupos a um tipo específico de interação social, em que a confiança em perfis e *nicknames online* passa a substituir até os intermediários tradicionais das transações econômicas nos mercados. Para Tim May, as tecnologias da informação e a criptografia permitiriam superar a justificativa para a interferência das instituições controladoras e asseguraria a ultrapassagem da ideia liberal de um Estado regulador. A reputação e o anonimato poderiam não só conviver, mas assegurar as relações de troca e as demais sociabilidades que constituem a vida em sociedade. Ali, a reputação não está ligada a uma identidade civil, formalmente reconhecida pelo governo. A confiança se adquire pela prática de rede. A partir da disseminação da criptografia assimétrica, será a chave pública de

with anonymous mail forwarding systems, with digital signatures, and with electronic money. Cypherpunks write code. (...) Our code is free for all to use, worldwide. We don't much care if you don't approve of the software we write. We know that software can't be destroyed and that a widely dispersed system can't be shut down. (...) Cryptography will ineluctably spread over the whole globe, and with it the anonymous transactions systems that it makes possible.(...) For privacy to be widespread it must be part of a social contract. People must come and together deploy these systems for the common good. Privacy only extends so far as the cooperation of one's fellows in society".

11 Livre tradução para: "A specter is haunting the modern world, the specter of crypto anarchy. Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive re- routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any tampering. Reputations will be of central importance, far more important in dealings than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation".

alguém, até mesmo sem nome, que permitirá a construção de uma reputação, de um estilo, de uma verdade efetiva de como aquele indivíduo anônimo se comporta nas redes.

Existem várias modalidades de criptografia, as duas principais são a criptografia simétrica e a criptografia assimétrica. A simétrica permite cifrar uma mensagem com uma chave que será a mesma utilizada para decifrar o que foi escondido por ela. Já a criptografia assimétrica trabalha com algoritmos (rotinas logicamente encadeadas) que geram duas chaves com funções inversas. Todo o texto que for cifrado com uma chave somente poderá ser decifrado com a outra que compõe o par. Isso permite que uma pessoa distribua fartamente nas redes digitais a cópia de uma de suas chaves criptográficas que será chamada de chave pública. A outra chave será chamada de privada e deve ser guardada com o máximo de segurança possível. Desse modo, somente as mensagens escritas com a chave privada daquela pessoa poderão ser decodificadas com sua chave pública. Isso permite a todos saber se foi mesmo a pessoa em questão que enviou uma determinada mensagem. Quanto maior for o tamanho das chaves geradas maior será a sua segurança. Repare que a chave pública de alguém não exige sua identidade legal. As transações realizadas com essa chave podem gerar uma boa ou má reputação. Sem dúvida, para evitar que alguém emita um par de chaves em nome de outra pessoa, as comunidades que utilizam criptografia usam técnicas de certificação digital baseada em uma rede de confiança em que um assina a chave de outro, confirmando que uma determinada chave pública é de fato de quem diz ser.

> Assim como a tecnologia de impressão alterou e reduziu o poder das guildas medievais e da estrutura de poder social, os métodos criptológicos também alterarão a natureza das corporações e da interferência do governo nas transações econômicas. Combinado com a emergência dos mercados de informação, criptoanarquia vai criar um mercado líquido [com um grande número de compradores e investidores] para todo e qualquer material que possa ser colocado em palavras e imagens. Assim, como uma invenção aparentemente menor do arame farpado possibilitou o cercamento de grandes sítios e fazendas, alterando para sempre os conceitos de terra e direitos de propriedade na fronteira oeste, também será a descoberta aparentemente menor de um ramo da matemática que cortará e desmantelará as cercas de arame farpado em torno da propriedade intelectual[12] (May, 1992).

Esse penúltimo parágrafo de *The Crypto Anarchist Manifesto* revela novamente uma queda para um certo determinismo tecnológico. Para Andrew Feenberg, o determinismo tecnológico implica que o "destino da sociedade diante da tecnologia seja ficar dependente de uma dimensão não-social que age no meio social sem, entretanto, sofrer uma influência recíproca" (Feenberg, 2010, p. 108). É também curioso que o final do Manifesto contenha um ataque à ideia de propriedade intelectual. Os principais pensadores libertários norte-americanos não forjaram um consenso sobre a legitimidade da propriedade sobre ideias. Thomas Jefferson, Benjamin Tucker e Tom Palmer eram radicalmente contrários à propriedade intelectual, enquanto Herbert Spencer, Lysander Spooner e Ayn Rand foram seus ardorosos defensores (LONG, 1995). A criptoanarquia de-

12 Livre tradução para: "Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions. Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put into words and pictures. And just as a seemingly minor invention like barbed wire made possible the fencing-off of vast ranches and farms, thus altering forever the concepts of land and property rights in the frontier West, so too will the seemingly minor discovery out of an arcane branch of mathematics come to be the wire clippers which dismantle the barbed wire around intellectual property".

REVISTA ECO PÓS | ISNN 2175-8889 | CINEMA EXPERIMENTAL | V 19 | N.2 | 2016 | PERSPECTIVA

fendida por May, voltada à defesa do livre compartilhamento de códigos, textos e ideias nas redes informacionais, poderia ser vista como uma atitude anticapitalista, porém nada mais é do que a adesão a uma das mais tradicionais correntes anarcocapitalistas presentes na história dos Estados Unidos.

2. 11 de setembro e a espionagem massiva

O início do século XXI foi extremamente turbulento, em especial, para os coletivos *cypherpunks*. Em 13 de setembro de 2001, dois dias após o ataque terrorista às Torres Gêmeas, Lance Cottrell, desenvolvedor de sistemas de privacidade na Internet e criador do serviço de remetente anônimo para a troca de e-mails chamado *Anonymizer.com*[13] postou a seguinte mensagem na lista de discussão *Cypherpunks*:

> (...) além de mostrar que não vamos ser intimidados nem desistir de nossas liberdades diante dos terroristas, este é um momento em que o mundo precisa desses serviços [de remetente anônimo] mais do que nunca. Diante de crises, há uma tendência dos governos repressivos em suprimir a comunicação e o livre acesso à informação. É exatamente nesses momentos em que a comunidade que defende a privacidade deve brilhar de modo mais forte[14] (Cypherpunks Tonga[15]).

O atentado de 11 de setembro de 2001 marcou importantes mudanças no sistema de vigilância e de contra-espionagem dos Estados Unidos da América. A espionagem global de governos e populações civis, praticada nos tempos da Guerra Fria, foi remodelada e ampliada. Teóricos importantes como Joseph Nye, no livro *Cyberpower,* advogaram a maior relevância da cibersegurança contra as fragilidades criadas pela expansão da Internet e seus riscos para o poder nacional. Ativistas, ciberativistas e *hackers* foram considerados tão perigosos quanto terroristas e passaram a ser alvos de observação minuciosa do Estado norte-americano. Ao mesmo tempo, grandes corporações e fundações, vinculadas ao esquema de manutenção de poder de Washington, desenvolveram um discurso de incentivo às práticas de *hacking* contra governos autoritários e democráticos de orientação antiamericana.

Joseph Nye (2010) escreveu que o poder depende de contexto onde é exercido. Para ele, o rápido crescimento do ciberespaço alterou o cenário do poder e um novo contexto emergiu na política mundial. Isso ocorreu principalmente pela disseminação das tecnologias de informação e comunicação que geraram

13 Os serviços de remetentes anônimos (Anonymous Remailers) são servidores que recebem mensagens com instruções incorporadas para onde enviá-las sem revelar sua origem na rede. Asseguram o anônimato na comunicação em uma rede cibernética tal como a Internet. Logo após a postagem de Lance Cottrell está escrito: "Dois dias depois, em 15 de setembro de 2001, o Tonga Remailer foi aberto". Trata-se de um serviço de *Anonymous* Remailers. Disponível em : http://www.cypherpunks.to/remailers/. Acesso em: 15/02/2015.

14 . Livre tradução para: "In addition to showing that we will not be cowed into giving up our cherished freedoms by terrorists, this is a time when the world needs these services more than ever. In crises there is a tendency for repressive governments to crack down on communications and free access to information. It is at exactly those times that the privacy community must shine its brightest".

15 Cypherpunks Tonga é um influente site cypherpunk . Em sua página inicial encontra-se a sua missão: "cypherpunks.to é um centro de pesquisa e desenvolvimento de projetos *cypherpunk* como *remailers*, serviços anônimos *peer-to-peer*, túneis para segurança de rede, criptografia de voz para aparelhos móveis, dinheiro eletrônico não rastreável, ambientes operacionais seguros, etc." Disponível em: http://www.cypherpunks.to. Acesso em: 15/02/2015.

REVISTA ECO PÓS | ISNN 2175-8889 | CINEMA EXPERIMENTAL | V 19 | N.2 | 2016 | PERSPECTIVA

a queda das barreiras de entrada para as disputas por influência e poder. Nye vê que o anonimato e as novas vulnerabilidades nascidas a partir do uso intenso das redes digitais de comunicação permitiram e permitem que atores menores tenham mais capacidade de exercer o poder no ciberespaço do que em muitos outros domínios tradicionais da política internacional, retirando as grandes vantagens que existiriam se os confrontos fossem no terreno da guerra existente até a era industrial.

> Lutas entre governos, empresas e indivíduos não são novas, mas o baixo custo de entrada, o anonimato, e assimetrias nas vulnerabilidades significa que os atores menores têm mais capacidade de exercer o poder 'hard e soft' no ciberespaço do que em muitos outros domínios tradicionais do mundo político. Mudanças no cenário das informações sempre tiveram um impacto importante sobre o poder. (...) As características do ciberespaço reduzem alguns dos diferenciais de poder entre os atores, e, assim, proporcionam um bom exemplo da difusão do poder que caracteriza a política global neste século. As maiores potências não são capazes de dominar o ciberespaço tanto quanto eles dominam o mar ou o ar (Nye, 2010, p.19).

Esse cenário internacional gerou mudanças na estratégia de defesa norte-americana. A espionagem focalizada em alvos específicos foi substituída pela espionagem massiva no ciberespaço. Para reduzir as profundas incertezas do novo cenário, para mapear possíveis articulações terroristas, para manter o seu grau de influência e poder, os executores da estratégia norte-americana decidiram desenvolver soluções tecnológicas para a espionagem massiva de todos os usuários da Internet, tal como o sistema *Prism*, denunciado por Edward Snowden, em 2013. Utilizando técnicas de rastreamento de termos e de postagens em redes sociais, interceptando e escaneando *e-mails*, monitorando as mensagens de jovens em *chats*, processando essas informações em *softwares* de mineração de dados, *data minin*g e *big data*, as agências de inteligência, principalmente a NSA[16] (EUA) e a GCHQ[17] (Grã-Bretanha) invertem a lógica da presunção de inocência, base jurídica dos chamados Estados de Direito. Todos passam a ser possíveis culpados até prova em contrário. Todos são suspeitos, pois a qualquer momento um indivíduo conectado pode dar uma informação valiosa para os sistemas de inteligência. A doutrina da guerra assimétrica[18] na Internet levou a NSA a se tornar vigia de todo o ciberespaço, uma espécie de vigilante planetária.

A vigilância global das populações e a subordinação de todos os direitos civis às razões dos Estados para a manutenção de um equilíbrio de forças planetário vão sendo transformadas em uma espécie de mal menor. Nesse sentido, o filósofo e jurista Giorgio Agamben percebeu que após o 11 de setembro os estados de exceção se alastraram e se tornaram efetivamente o paradigma de governo. Diante de uma grave ameaça, o estado de exceção gera a suspensão temporária de direitos e garantias constitucionais. Tudo é subordinado à segurança de Estado. Como tem sido apontado pelo Wikileaks, o governo norte-americano e suas agências passaram a considerar todos os viventes, cidadãos ou não de seu país, terroristas em potencial, agentes que

16 NSA é o acrônimo de National Security Agency. Criada em 1952, responsável pela inteligência de sinais, interceptação de comunicações e criptoanálise.

17 O Government Communications Headquarters (GCHQ) é um serviço de inteligência britânico encarregado da segurança e da espionagem e contraespionagem nas comunicações, atividades tecnicamente conhecidas como SIGINT (Inteligência de sinais).

18 John Arquilla e David Ronfeldt trabalham a ideia de guerra assimétrica nas redes de informação desde a última década do século XX.

REVISTA ECO PÓS | ISNN 2175-8889 | CINEMA EXPERIMENTAL | V 19 | N.2 | 2016 | PERSPECTIVA

podem a qualquer momento abalar a segurança nacional. Ocorre que o estado de exceção "apresenta-se como a forma legal daquilo que não pode ter forma legal" (Agamben, 2004, p.12).

> O totalitarismo moderno pode ser definido, nesse sentido, como a instauração, por meio do estado de exceção, de uma guerra civil legal que permite a eliminação física não só dos adversários políticos, mas também de categorias inteiras de cidadãos que, por qualquer razão, pareçam não integráveis ao sistema político. Diante do incessante avanço do que foi definido como uma 'guerra civil mundial', o estado de exceção tende cada vez mais a se apresentar como o paradigma de governo dominante na política contemporânea. Esse deslocamento de uma medida provisória e excepcional para uma técnica de governo ameaça transformar radicalmente – e, de fato, já transformou de modo muito perceptível – a estrutura e o sentido da distinção tradicional entre os diversos tipos de constituição. O estado de exceção apresenta-se, nessa perspectiva, como um patamar de indeterminação entre democracia e o absolutismo (Idem, p.13).

A mudança do padrão de vigilância nas redes informacionais e a descrição proposta por Agamben do atual cenário de guerra civil legal corroboram com a fundamentação do que os *cypherpunks* denominam de militarização da Internet. A rede mundial passa a ser o terreno da vigilância de guerra e da excepcionalidade geral, uma vez que nessa conjuntura os direitos têm importância ínfima diante da necessidade de derrotar o inimigo.

3. Libertarianismo, anarquismo individualista e guinada à esquerda

As revelações de Edward Snowden, em 2013, se somaram às inúmeras denúncias apresentadas pelo *Wikileaks* confirmando um processo de ocupação militar e policialesca do ciberespaço para fins de uma vigilância global e manutenção do poder geoestratégico dos Estados Unidos. A violação da privacidade dos cidadãos norte-americanos para Snowden era inaceitável e representava um grande risco para a liberdade.

Apesar de não existir uma declaração de Edward Snowden se autodefinindo como um *cypherpunk*, é possível encontrar em seu discurso os fundamentos das práticas discursivas presentes nos manifestos aqui discutidos. Snowden alega ter se rebelado em defesa da liberdade e da privacidade dos próprios cidadãos norte-americanos diante do poder inaceitável de um Estado vigilante e controlador da vida das pessoas comuns. Snowden possui identificação com o posicionamento político libertário.

Logo após suas denúncias, a imprensa buscou saber quem seria aquele jovem que ousava enfrentar o poderio do Estado norte-americano. Logo ficou evidente que Snowden tinha uma grande proximidade política com a direita estadunidense. Em 2012, Snowden fez uma doação[19] para a campanha de Ron Paul[20], candidato libertário à presidência dos Estados Unidos nas prévias do Partido Republicano. Ron Paul é tido como o men-

19 Veja a matéria do Washington Post sobre a doação de Snowden: http://www.washingtonpost.com/politics/edward-snowden-says-motive-behind-leaks-was-to-expose-surveillance-state/2013/06/09/aa3f0804-d13b-11e2-a73e-826d299ff459_story.html. Acesso em 20 março de 2015.

20 Página do Instituto Ron Paul: http://ronpaulinstitute.org/about-us/. Acesso em 20 de março de 2015.

REVISTA ECO PÓS | ISNN 2175-8889 | CINEMA EXPERIMENTAL | V 19 | N.2 | 2016 | PERSPECTIVA

tor intelectual da ala libertária dos Republicanos, denominada *Tea Party*. Paul é um ferrenho crítico da política fiscal, dos impostos, do complexo industrial-militar dos Estados Unidos e da chamada "guerra às drogas"[21]. Na página do *Tea Party Tribune* foi possível encontrar já em junho de 2013 defensores da ação de Edward Snowden, como a colunista Rachel Alexander, também editora da publicação *Intellectual Conservative*[22]. Libertários no cenário político norte-americano são ultraliberais ou anarcocapitalistas.

A trajetória discursiva presente nos textos coletados do universo *cypherpunk*, a partir dos anos 1990, e seu rol de compromissos vão de uma grande desconfiança das autoridades, em geral, postura encontrada entre *hackers* e integrantes do *hacktivismo*, até a defesa da meritocracia, doutrina ancorada nos discursos libertários, liberais e neoliberais. Todavia, as condições políticas e conjunturais acabaram levando grande parte dos coletivos *cypherpunks* a se alinharem com movimentos sociais e coletivos ativistas de orientação de esquerda. Também reorganizaram tópicos liberais nitidamente contrários à visão de proteção e justiça social para colocar a individualidade e capacidade do *cypherpunk* de lidar com programas de computador à serviço da garantia dos direitos das pessoas sem habilidades para se defender dos Estados e corporações.

Como relatado anteriormente, algumas das ideias básicas do *Manifesto Cypherpunk*, escrito por Eric Hughes, em 1993, indicam a crítica aos diversos governos contemporâneos. No Manifesto, encontram-se afirmações de que a "privacidade é necessária para uma sociedade aberta na era eletrônica" e que "não podemos esperar que os governos, as empresas ou outras grandes organizações sem rosto nos conceda a privacidade". Quase como uma decorrência das passagens anteriores, o Manifesto indica que os *cypherpunks* escrevem códigos e "se alguém precisa escrever *softwares* para defender a privacidade... nós estamos indo escrevê-los" (Hugues, 1993).

A busca dos principais componentes discursivos presentes nos textos encontrados nos principais *sites* criados pelos *cypherpunks* permite-nos observar a tensão entre a origem anarcocapitalismo e os princípios mais recentes que denunciam os governos que comandam o mundo e detém a supremacia do capital. O *site Cypherpunks Tonga* é uma fonte crucial para entender a ambivalência aqui proposta. Os *sites Cypherpunks Canada* – um dos maiores distribuidores do OTR, *off-the-record messaging*, um programa para conversas *online* protegido por criptografia forte – e o Wikileaks oferecem um material de enfrentamento com a estrutura de poder mundial atual. O esforço de parte dos coletivos *cypherpunks* pode ser definido como integrante da luta anti-imperial (Hardt; Negri, 2005) ou mesmo com a perspectiva anti-imperialista (Chomsky; Vltchek, 2013).

A influência *cypherpunk* no cenário de militarização da Internet está na base da proliferação de uma série de eventos denominados *cryptoparties,* encontros que buscam reunir atividades de popularização das ferramentas criptográficas com atividades de entretenimento. O evento agrega pessoas interessadas a aprender a utilizar programas de criptografia e a compreender seus fundamentos, bem como busca finalizar com a cerimônia de troca de chaves criptográficas entre os presentes. Em uma *cryptoparty*, os *cypherpunks* ensinam as técnicas de proteção dos dados pessoais, da privacidade e do anonimato. A ideia desse evento, segundo o *The CryptoParty Handbook*, foi concebida após a aprovação da Lei Australiana de Cibercrimes, em 2011. O

21 Nesta página há um resumo do pensamento de Ron Paul: http://ontheissues.org/Liberty_Defined.htm. Acesso em 20 de março de 2015.

22 Edward Snowden: Traitor or Hero? Disponível: http://www.teapartytribune.com/2013/06/28/edward-snowden-traitor-or-hero/. Acesso em 20/03/2015.

REVISTA ECO PÓS | ISNN 2175-8889 | CINEMA EXPERIMENTAL | V 19 | N.2 | 2016 | PERSPECTIVA

movimento de organização de *cryptoparties* se tornou viral e dezenas de encontros autônomos vem sendo organizados em todo o planeta.

No Brasil, duas *CryptoParties* ocorreram, em 2013, uma em Salvador, Bahia, e outra na cidade de São Paulo. O maior desses eventos aconteceu em abril de 2014, no Centro Cultural São Paulo, contando com mais de dois mil participantes. Jeremie Zimmermann, do *La Quadrature Du Net*, e um dos principais *cypherpunks* da Europa abriu o evento brasileiro e afirmou nunca ter participado de um encontro de criptografia tão numeroso.

Os eventos *cypherpunks* pela popularização das ações de resistência ao recrudescimento da vigilância massiva global, praticada principalmente pelos Estados Unidos, contribuem para a formulação da hipótese aqui levantada de que, em sua fase mais recente, os *cypherpunks* foram levados de uma crítica liberal e libertária aos Estados, em geral, à formulação de um discurso claramente contrário à supremacia e à política belicista norte-americana. A conjuntura política concreta conduziu influentes *cypherpunks*, como Julian Assange, a enfrentar o poderio conservador dos Estados Unidos. Isso os aproximou do ativismo de esquerda. Não é por outro motivo que o Equador, um país latino americano, dirigido por um presidente de esquerda, decide conceder asilo político a Julian Assange, para tentar evitar que fosse enviado para a prisão nos Estados Unidos. Assange escreveu:

> Os *cypherpunks* originais, meus camaradas, foram em grande parte libertários. Buscamos proteger a liberdade individual da tirania do Estado, e a criptografia foi a nossa arma secreta. Isso era subversivo porque a criptografia era de propriedade exclusiva dos Estados, usada como arma em suas variadas guerras. Criando nosso próprio *software* contra o Estado e disseminando-o amplamente, liberamos e democratizamos a criptografia, em uma luta verdadeiramente revolucionária, travada nas fronteiras da nova internet. A reação foi rápida e onerosa, e ainda está em curso, mas o gênio saiu da lâmpada. O movimento *cypherpunk*, porém, se estendeu além do libertarismo. Os *cypherpunks* podem instituir um novo legado na utilização da criptografia por parte dos atores do Estado: um legado para se opor às opressões internacionais e dar poder ao nobre azarão. A criptografia pode proteger tanto as liberdades civis individuais como a soberania e a independência de países inteiros, a solidariedade entre grupos com uma causa em comum e o projeto de emancipação global. Ela pode ser utilizada para combater não apenas a tirania do Estado sobre os indivíduos, mas a tirania do império sobre a colônia. Os *cypherpunks* exercerão seu papel na construção de um futuro mais justo e humano. É por isso que é importante fortalecer esse movimento global (Assange, 2013, p.22).

O desenvolvimento de ferramentas para proteger a comunicação, o uso de softwares livres e auditáveis, a popularização e simplificação do uso da criptografia deixam de ser apenas atividades técnicas e assumem um caráter político. Sem dúvida, as tecnologias informacionais são ambivalentes e podem servir para a vigilância e espionagem globais. Podem igualmente ser utilizadas para proteger direitos e para avançar a articulação e a comunicação entre coletivos e movimentos que lutam por justiça social e pela ampliação da diversidade.

Da origem anarcocapitalista, os *cypherpunks* caminharam para a luta contra o poder global norte-americano e as corporações que o apoiam e dele se beneficiam. Isso não significa que as forças conservadoras do atual sistema de dominação não possuam condições de utilizar a criptografia para continuar oprimindo e restringindo liberdades. Também não implica que a maioria dos *cypherpunks* deixaram de apoiar suas convicções capitalistas. Aqui está proposta a hipótese de que nessa conjuntura específica, a criptografia e as práticas *cypherpunks* incomodam os articuladores do capitalismo que vivem da venda de dados pessoais e os beneficiários do poder político e militar global exercido pelos Estados Unidos.

4. Brevíssima conclusão

O que poderia parecer incompreensível para os movimentos sociais mais vinculados à esquerda e para aqueles oriundos das lutas socioambientais, agora passa a fazer sentido: a ideia de que a criptografia forte pode ser uma ação política para a mudança social e das estruturas de poder. As feministas, os indígenas, as lideranças dos movimentos pela reforma agrária e muitos sindicalistas perceberam que estão sendo vigiados. Informações dos movimentos e dos ativistas que lutam por direitos humanos são recolhidas para buscar criminalizá-los ou simplesmente para impedir as ações de denúncia dos aparatos de extermínio de jovens negros nas periferias das cidades brasileiras. Os *cypherpunks* passam a ser respeitados por sua inteligência e postura a favor das liberdades fundamentais. No atual cenário mundial, aqueles que lutam pela justiça precisam de um espaço de liberdade para comunicar e para agir. A liberdade de expressão e a privacidade, direitos caros ao liberalismo, parecem perder importância para as forças políticas que comandam o Estado norte-americano e seus aliados. A manutenção da atual estrutura de poder global depende da permanente tensão antiterrorista e da criminalização das diferenças políticas. Nesse contexto, os agrupamentos de esquerda descobrem a força do pensamento e da ação dos *cypherpunks* que se descolam gradativamente da origem anarcocapitalista.

Referências bibliográficas

ARQUILLA, John; RONFELDT, David (org.). *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica: RAND, 1997.

_____. *Swarming and the Future of Conflict*. Santa Monica: RAND, 2000.

ASSANGE, Julian et all. *Cypherpunks: liberdade e o futuro da internet*. São Paulo: Boitempo Editorial, 2013.

AGAMBEN, Giorgio. *Estado de exceção*. São Paulo: Boitempo, 2004 (Estado de sitio).

CASTELLS, Manuel. *Redes de indignação e esperança*. Rio de Janeiro: Zahar, 2013.

CHOMSKY, Noam; VLTCHEK, Andre. *On western terrorism*: from Hiroshima to drone warfare. London: Pluto Press,

REVISTA ECO PÓS | ISNN 2175-8889 | CINEMA EXPERIMENTAL | V 19 | N.2 | 2016 | PERSPECTIVA

2013.

DENNING, Dorothy E. The Future of Cryptography. In: LUDLOW, Peter (ed.). *Crypto Anarchy, Cyberstates, and Pirate Utopias*. Cambridge: The MIT Press, 2001.

FEENBERG, Andrew. Teoria Crítica da Tecnologia: um panorama. In: NEDER, Ricardo T. *Andrew Feenberg:* racionalização democrática, poder e tecnologia. Brasília: Observatório do Movimento pela Tecnologia Social na América Latina/Centro de Desenvolvimento Sustentável - CDS. Ciclo de Conferências Andrew Feenberg. Série Cadernos PRIMEIRA VERSÃO: CCTS - Construção Crítica da Tecnologia & Sustentabilidade. Vol. 1. Número 3. 2010.

FOUCAULT, Michel. *Arqueologia do saber.* Rio de Janeiro: Forense Universitária, 2008.

FRIEDMAN, David. *The machinery of freedom*. Guide to a radical capitalism. 1973. Disponível em: http://daviddfriedman.com/The_Machinery_of_Freedom_.pdf. Acesso em: 10/02/2015.

GALLOWAY, Alexander. *Protocol: how control exist after descentralization*. Cambridge, MA: MIT, 2004.

HARDT, Michael; NEGRI, Antonio. *Multidão*. Rio de Janeiro: Record, 2005.

HUGUES, Eric. *A Cypherpunk's Manifesto*. 1993. Disponível em:

http://www.activism.net/cypherpunk/manifesto.html. Acesso: 15/01/2015.

JORDAN, Tim; TAYLOR, Paul A. *Hacktivism and cyberwars*: rebels with a cause? New York: Routledge, 2004.

KIRBY, David; EKINS, Emily. *Libertarian Roots of the Tea Party*. Policy Analysis, No. 705, August 6, 2012. Disponível em: http://object.cato.org/sites/cato.org/files/pubs/pdf/PA705.pdf. Acesso em 20/03/2015.

LONG, Roderick. *The libertarian case against intellectual property rights.* 1995. Disponível em: http://freenation.org/a/f31l1.html. Acesso em: 20/02/2015.

LUDLOW, Peter. *Crypto anarchy, cyberstates, and pirate utopias.* Cambridge: MIT Press, 2001.

MAY, Timothy C. *The Cyphernomicon:* Cypherpunks FAQ and more, Version 0.666, 1994-09-10. Disponível em: https://www.cypherpunks.to/faq/cyphernomicron/chapter3.html#4. Acesso em: 08/01/2015.

MAY, Timothy C. *The Crypto Anarchist Manifesto*. 1992. Disponível:

http://www.activism.net/cypherpunk/crypto-anarchy.html. Acesso em: 15/01/2015.

NYE, Joseph S. *Cyber Power*. Belfer Center for Science and International Affairs. Cambridge: Harvard

Kennedy School, 2010. Disponível em: http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

NOZICK, Robert. *Anarquia, estado e utopia.* Rio de Janeiro: Jorge Zahar Editor, 1991.

PALMAS, Karl; VON BUSCH, Otto. *Abstract hacktivism*: the making of a hacker culture. London and Istanbul: Mute, 2006.

REVISTA ECO PÓS | ISNN 2175-8889 | CINEMA EXPERIMENTAL | V 19 | N.2 | 2016 | PERSPECTIVA

PEIRANO, Marta et all. *The CryptoParty Handbook*. 2012.

RAYMOND, Eric. *How To Become A Hacker*. 2001. Disponível:

http://www.catb.org/esr/faqs/hacker-howto.html#why_this. Acesso em: 10/03/2016.

SAMUEL, Alessandra. *Hacktivism and the Future of Political Participation*. Tese de doutorado em Filosofia na disciplina de Ciência Política. Harvard University Cambridge, Massachusetts. Setembro de 2004.

SINGH, Simon. *O livro dos códigos*. A ciência do sigilo – do antigo Egito à criptografia quântica. 2ª ed. Rio de Janeiro: Record, 2002.

SILVEIRA, Sergio Amadeu. *Ciberativismo, cultura hacker e o individualismo colaborativo*. REVISTA USP, São Paulo, n.86, p. 28-39, junho/agosto 2010.

TUCKER, Benjamin. *Individual liberty*. New York: Vanguard Press, 1926.

Disponível em: https://mises.org/sites/default/files/Individual%20Liberty_3.pdf. Acesso em: 10/02/2015.

VEGH, Sandor. The Media's Portrayal of Hacking, Hackers, and Hacktivism Before and After September 11, in *First Monday*, vol. 10, n. 2, February/2005.

WRAY, Stefan. Electronic Civil Disobedience and the World Wide Web of Hacktivism. New York: 1998. Disponível em: http://switch.sjsu.edu/web/v4n2/stefan . Acesso em: 10/03/2010.

REVISTA ECO PÓS | ISNN 2175-8889 | CINEMA EXPERIMENTAL | V 19 | N.2 | 2016 | PERSPECTIVA