II Encontro Internacional Participação, Democracia e Políticas Públicas
27 a 30 de abril de 2015, UNICAMP, Campinas (SP)

A DISSEMINAÇÃO DOS COLETIVOS CYPHERPUNKS E SUAS PRÁTICAS DISCURSIVAS

Sergio Amadeu da Silveira
CECS - UFABC

RESUMO

O texto traz a análise de um tipo específico de ciberativismo, os cypherpunks. Esses coletivos ganharam destaque mundial principalmente a partir das denuncias realizadas pelo Wikileaks, obtendo ainda mais força 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 pesquisa pretende mostrar uma modalidade de ativismo e de engajamento político específica, bem como, suas relações ambivalentes com o discurso de esquerda ao mesmo tempo que os componentes fundamentais do pensamento cypherpunk recebem influência direta do ultraliberalismo ou anarco-capitalismo de matriz norte-americana.

PALAVRAS-CHAVE: cypherpunk, ciberativismo, criptografia, cultura hacker, privacidade.

O QUE CARACTERIZA OS CYPHERPUNKS

O cypherpunk é um ativista que defende uso generalizado da criptografia forte[1] como caminho para a mudança social e política. Existe um movimento cypherpunk ativo desde os anos de 1990, fortemente influenciado pela cultura hacker e pelas ideias libertárias. Ganhou destaque o empenho de Philip Zimmermann, em 1991, ao desenvolver e distribuir o software PGP com a intenção de dar acesso a criptografia para todos. Durante a maior parte da década de 90, havia uma lista de discussão cypherpunk extremamente ativa. Grande parte dos cypherpunks estavam envolvidos em intensas controvérsias políticas e jurídicas em torno do direito ao uso de criptografia. Os coletivos cypherpunks estão crescendo e sendo chamados a participar da luta política na defesa da

1 Criptografia forte é aquela que utiliza algoritmos robustos e chaves formadas por gigantescas combinações alfanuméricas. Para tentar decifrar uma chave de 2048 bits os computadores levariam muito tempo. Já uma chave de 128 bits seria bem mais fácil, por isso pode ser considerada criptografia fraca. A força da criptografia é aferida pelo tempo e pelos recursos exigidos para se decifrar os dados encriptados.

privacidade, anonimato e 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. 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 sobre a questão da privacidade. Em 1994, May lançou, na lista de correio eletrônico que ajudou a criar, o FAQ[2] sobre os c*ypherpunks* 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 mais a frente.

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 dos seguintes pontos:

> "- Que o governo não deve possa espionar as atividades das pessoas;
> - Que a proteção de conversas e negociações das pessoas seja um direito básico;
> - Que esses direitos possam ser assegurados pela tecnologia **em vez** das leis;
> - Que o poder da tecnologia muitas vezes crie novas realidades políticas (daí o mantra: 'Cypherpunks escrevem códigos')" (May, 1994, online)

Uma análise dos recursos narrativos empregados no discurso de May evidencia claramente a desconfiança dos governos e a negação do seu poder de vigilância sobre as pessoas. Como a lei do Estado não pode garantir o direito à privacidade, uma vez que o governo é o o grande interessado na coleta de informações dos 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

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

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 eles 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 tecnologia parece mais como ambivalente e passível de disputa.

Dorothy E. Denning, uma importante pesquisadora de segurança da informação norte-americana, considera os cypherpunks uma ameaça, principalmente a vertente cripto-anarquista, devido a 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 a aplicação da lei e exigências de segurança nacional para a descodificação de emergência e fornecer a proteção de privacidade para os usuários.” (Denning, 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 poder superiores. 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 anarco-capitalista 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 com 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 rosto nos conceda a privacidade por sua caridade." (Hugues, 1993, online)

Hugues trouxe no texto 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 uma ação nos parlamentos ou a mobilização coletiva pela aprovação de leis ou pela a pressão contra governos intrusores 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. 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 selectivamente ao mundo". Poder é 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 do livro Cypherpunks, de Julian Assange, vinte anos após o lançamento do Manifesto de Hugues, dita por Jacob Appelbaum[3], 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 medida em que existe a cooperação dos semelhantes na sociedade. (Hugues, 1993, online)

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). O compartilhamento do conhecimento e das técnicas de criptografia não retiram a primazia do indivíduo que é cultuado pelos cypherpunks.

A análise discursiva dos principais textos dos cypherpunks evidencia a origem cypherpunk 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 anacocapitalistas é o fato de todas elas defenderem a liberdade de contratos entre indivíduos, a liberdade irestrita de mercado e as possibilidades de vida social sem Estado (Friedman; Tucker; Nozic). O texto *The Crypto Anarchist Manifesto*, escrito por Tim May, em 1992, lançado antes do *A Cypherpunk's Manifesto*, redigido por Eric Hugues, em 1993, contém uma evidente adesão ao

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

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 interagir 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.
> (May, 1992, online)

Percebe-se que o Manifesto marca o seu início com a aposta na adesão dos indivíduos e grupos à um tipo específico de interação social em que a confiança em perfis e nicknames online passa a substituir até mesmo os intermediários tradicionais das transações econômicas nos mercados. As tecnologias da informação e a criptografia permitiriam, na visão de Tim May, superar a justificativa para a interferência das instituições controladoras, até mesmo 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 ligado a uma identidade civil, formalmente reconhecida pelo governo. A confiança se adquire na prática de rede. É a chave pública de alguém sem nome que permitiria a construção de uma reputação, de um estilo, de uma verdade efetiva de como aquele indíviduo 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 utilizam de 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. (May, 1992, online)

Este 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 (p. 108). ” É também curioso que o final do Manifesto contenha um ataque à ideia de propriedade intelectual. Os principais pensadores libertários norteamericanos 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, online). A criptoanarquia defendida por May é mais voltada à defesa do livre compartilhamento de códigos, textos e ideias nas redes informacionais. O que poderia ser visto como uma atitude anticapitalista nada mais é do que a absorção de uma das mais tradicionais correntes anarcocapitalistas dos Estados Unidos.

11 DE SETEMBRO E A ESPIONAGEM MASSIVA

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*[4] 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 a exatamente nesses momentos em que a comunidade que defende a privacidade deve brilhar de modo mais forte."[5] (Cypherpunks Tonga[6])

O atentado de 11 de setembro de 2001 marcou importantes mudanças no sistema de espionagem e de contra-espionagem dos Estados Unidos da América. A atitude de vigilância global e de populações civis que eram praticadas nos tempos da Guerra Fria foram retomados e ampliados. Teóricos importantes como Joseph Nye, no livro Cyberpower, advogam a maior relevância da cibersegurança contra as fragilidades criadas pela expansão da Internet e seus riscos para o poder nacional. Ativistas, ciberativistas e hackers são considerados tão perigosos quanto terroristas e passam a ser alvos de observação do Estado norte-americano. Ao mesmo tempo, grandes corporações e fundações vinculadas ao esquema de manutenção de poder desenvolvem um discurso de incentivo às práticas de hacking contra governos autoritários, mas que tenham uma orientação anti-americana.

Joseph Nye considera que o poder depende do contexto onde é exercido. Para ele,

---

4 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.

5 Disponível: http://www.cypherpunks.to/remailers/ Acesso 15/02/2015. 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.

6 Cypherpunks Tonga é um influente site cypherpunk < http://www.cypherpunks.to/ >. 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." Acesso em 15/02/2015.

o rápido crescimento do ciberespaço altera o cenário do poder e um novo contexto emerge na política mundial. Isso ocorre principalmente pela disseminação das tecnologias de informação e comunicação que geraram a queda da barreira 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 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)

A interpretação desse cenário internacional gerou mudanças na estratégia de defesa norteamericana. A espionagem focalizada em alvos específicos foi substituida 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 decidem construir ferramentas 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 mining e big data, as agências de inteligência, principalmente a NSA (EUA) e a GCHQ (Grã Bretanha) invertem as bases 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 nas redes levou a NSA se tornar a polícia que vigia todo o ciberespaço.

O filósofo e jurista Giorgio Agamben percebeu que o Estado norte-americano se tornou um estado de exceção. Todas as regras estão subordinadas à defesa da

segurança de Estado. O governo e suas agências passaram a considerar todos os viventes, cidadãos ou não de seu país, terroristas em potencial ou, no mínimo, agentes que podem a qualquer momento abalar a segurança nacional. Para Agamben, o Estado de exceção “apresenta-se como a forma legal daquilo que não pode ter forma legal” (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 politico. 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 politica 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 perceptvel- a estrutura e o sentido da distinção tradicional entre os diversos tipos de constituição. 0 estado de exceção apresenta-se, nessa perspectiva, como um patamar de indeterminação entre democracia e o absolutismo. (Agamben, 2004 ,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 a fundamentação do que os cypherpunks denominam de militarização da Internet. A rede mundial passa a ser o terreno da guerra e da excepcionalidade geral, uma vez que em um estado de guerra os direitos têm importância ínfima diante da necessidade de derrotar o inimigo.

ANARQUISMO INDIVIDUALISTA E GUINADA À ESQUERDA

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 idéias básicas do Manifesto Cypherpunk, escrito por Eric Hughes, em 1993, indicam a complexidade do seu discurso para as posições de diversos governos contemporâneos. No Manifesto, encontra-se a afirmação 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, online).

A busca dos principais componentes discursivos presentes nos textos encontrados nos principais sites criados pelos Cypherpunks, permite-nos observar a tensão entre a origem anarco-capitalismo e os princípios mais recentes que denunciam os principais governos que comandam o mundo e mantém a supremacia do capital. O site Cypherpunks Tonga é uma fonte crucial para entender a ambivalência aqui proposta. Os sites Cypherpunks Canadá -- um dos maiores distribuidores do OTR, off-the-record messaging, um cliente de conversas online protegido por criptografia forte -- e o Wikileaks dispõem de um material que deixa claro o enfrentamento com a estrutura de poder atual, o que se confunde com a luta anti-imperial (Negri) ou mesmo com a perspectiva antiimperialista (Chomsky; Vltchek).

A influência cypherpunk no cenário de militarização da Internet está na base da proliferação de uma série de eventos denominados CryptoParties. São 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. Na CryptoParty, os hackers 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 movimento de organização de CryptoParties se tornou viral e dezenas de encontros

autônomos vem sendo organizados em todo o planeta. "O uso do TOR [software e rede para a navegação anônima] na Austrália disparou após ocorrerem 4 CryptoParties".

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, os discursos do Wikileaks, a popularização das ações de resistência ao recrudescimento da vigilância massiva global, praticada pelos Estados Unidos, contribuem para a hipótese aqui levantada de que, em sua fase mais recente, os Cypherpunks foram levados de uma crítica liberal e libertária aos Estados à formulação de um discurso claramente contrário à supremacia e a política belicista norte-americana. A conjuntura política concreta conduziu influentes cypherpunks, tais como Julian Assange a enfrentar o poderio conservador dos Estados Unidos, incluindo corporações como o Google. Isso os aproximou de um ativismo mais próximo da 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 que se irradia para os diversos sentidos políticos. Sem dúvida, as tecnologias informacionais são ambivalentes e podem servir para a vigilância e espionagem globais, mas podem igualmente serem utilizadas para proteger direitos e avançar a articuação e a comunicação de coletivos que lutam por justiça social e pela ampliação da diversidade.

Da origem estritamente anarco-capitalista os cypherpunks caminharam para a luta contra o poder global norte-americano e o sistema que beneficia as corporações que o apóiam e dele se beneficiam e muitas vezes dele dependem. Isso não significa que as forças conservadoras do atual sistema de dominação não possuam condições de organizar mobilizações que utilizem a criptografia para continuar oprimindo e restringindo liberdades. Também não implica que a maioria dos cypherpunks tenha deixado de apoiar suas convições capitalistas. Aqui está proposta a hipótese de que nessa conjuntura específica, a criptografia e as práticas cypherpunks incomodem os articuladores do capitalismo que vivem da venda de dados pessoais e os beneficiários do poder político e militar global exercido pelos Estados Unidos.

CONCLUSÃO

O que poderia parecer incompreensível para os movimentos sociais mais vinculados à esquerda e aqueles oriundos das lutas socioambientais passa a fazer sentido: a ideia de que a criptografia forte é um caminho para a mudança política e social. As feministas, os indígenas, as líderanças 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 denuncia dos aparatos de extermínio de jovens negros nas periferias das cidades brasileiras. Os cypherpunks passam a ser respeitados pela sua coragem, inteligência e por sua postura a favor das liberdades fundamentais. No atual cenário mundial, aqueles que lutam pela justiça precisam de 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 comanadam o Estado norte-americano e seus aliados, tais como a Inglaterra. A manutenção da atual estrutura de poder global depende da manutenção da permanente tensão antiterrorista e da criminalização das diferenças políticas. Nesse universo, as forças de esquerda descobrem a força do pensamento e da ação dos cypherpunks.

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, 2013.

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

FEENBERG, Andrew. Teoria Crítica da Tecnologia: um panorama. In: Andrew Feenberg: racionalização democrática, poder e tecnologia / Organização: Ricardo T. Neder. 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: http://daviddfriedman.com/The_Machinery_of_Freedom_.pdf Acesso 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: 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.

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

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

MAY, Timothy C.. The Crypto Anarchist Manifesto. 1992. Disponível: http://www.activism.net/cypherpunk/crypto-anarchy.html Acesso 15/01/2015.

NYE, Joseph S. Cyber Power. Belfer Center for Science and International Affairs. Harvard Kennedy School. 2010. Disponível: http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf

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

PEIRANO, Marta e outros. The CryptoParty Handbook. 2012. Disponível: https://www.cryptoparty.in/documentation/handbook#download_the_handbook

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.

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

Sergio Amadeu da Silveira é doutor em Ciência Política e professor da UFABC.
Contato: sergio.amadeu@ufabc.edu.br