Anonimato e Criptografia: a criação de novas relações de força no contexto do Comum

Giuliano Djahjah Bonorandi[1]

Universidade Federal do Rio de Janeiro

RESUMO

Este trabalho busca investigar o contexto da criação de práticas de anonimato e criptografia no bojo das lutas biopolíticas que vêm se afirmando nas redes de comunicação distribuída. Neste artigo analisamos os fenômenos do *Bitrorrent, Bitcoin e Wikileaks,* que diante desse quadro de conflito entre autonomia e controle, exprimem novas criações que extrapolam o uso do anonimato e criptografia para manutenção da privacidade e os utilizam para permitir novos tipos de conversações e parcerias anônimas nas redes. Considerando que as redes são cada vez mais o lugar de exercício de um biopoder, essas práticas demonstram o caráter vivo deste trabalho e sua luta para a construção do Comum.

PALAVRAS-CHAVE

Internet; Anonimato; Comum; Criptografia; Controle

É necessário pensar o Comum a partir de determinados pressupostos, sem excluir os recursos naturais nem os bens materiais, mas ampliando esse conceito para todas as relações humanas: hábitos, ideias, afetos, linguagens, métodos, invenções, códigos... subjetividades; o comum deixa de ser algo estático, mas uma relação, algo que é construído. Há duas operações nessa mudança. A primeira é desconsiderar a natureza humana como a questão condicionante da soberania, e sim, considerar as subjetividades como ao mesmo tempo produtoras de relações sociais e sujeitas as condições de produção. A outra é não admitir o meio natural como algo separado do humano, algo exterior a ser preservado e explorado racionalmente, mas sim como parte da relação que se estabelece na construção de um Comum, com letra maiúscula; uma concepção biopolítica, como definem Hardt e Negri:

> "A concepção biopolítica de comum permeia igualmente todas as esferas da vida, se referindo não somente à terra, o ar, os

[1]Doutorando no Programa de Comunicação e Cultura da ECO/UFRJ. Email:boreste@gmail.com

> elementos, ou mesmo a vida vegetal e animal, mas também a elementos constitutivos da sociedade humana, tais como linguagens comuns, hábitos, gestos, afetos, códigos. Por outro lado, se de acordo com a noção tradicional, para pensadores como Locke e Rosseau, a formação da sociedade e o progresso da história destroem o comum, e por isso é necessário cercá-lo como propriedade privada, uma concepção biopolítica de comum enfatiza não só a preservação do comum mas também a luta pela condições de produzi-lo, assim como selecionar suas qualidades, promovendo suas forma benéficas e varrendo a sujeira de suas formas corruptas. Nós podemos chamar isso de uma ecologia do comum – uma ecologia focada igualmente na natureza e na sociedade, em mundos humanos e não-humanos em uma dinâmica de interdependência, cuidado e transformação mútua. ” (HARDT, NEGRI, 2009:171)

Para Foucault (1993) o poder se exerceria a partir de positividades e não de repressão. Dito em outras palavras o poder não cala, mas faz falar. Os regimes disciplinares e as arquiteturas de poder são , portanto, dispositivos de produção de discursos, que capilarizados e dispersos no bojo da sociedade teriam como objetivo “administrar e produzir a vida”. A passagem de um regime de soberania para um regime disciplinar no século XVII demonstra como os modos de produção de saber e poder se tornaram bastante distintos de um regime para o outro. No regime disciplinar, o corpo era o principal alvo do poder, e o objetivo era administrar os corpos sob o modelo do confinamento, idealizado na arquitetura do panóptico. Em um momento de transição para uma sociedade capitalista, este poder sobre os corpos era essencial para o controle de populações e adestramento do trabalho fabril. Era necessário que os corpos fossem saudáveis, dispostos, presentes e dóceis. Um poder, portanto, que investia sobre a vida, sobre a produção de subjetividades.

A passagem do regime da disciplina para o regime do controle nos leva a um aprofundamento do conceito de biopoder. Ora, se a partir da lutas anti-disciplinares agora a fábrica está dispersa em toda a sociedade, o biopoder amplia seu leque de investimento. Não é só mais o corpo o alvo do adestramento, mas “todo o seu meio ambiente, sua comunicação, os seus conhecimentos e seus afetos”. (ANTOUN, MALINI, 2010:4).

O prolema do biopoder é portanto um problema de governança. Reconhecer a passagem de um regime de disciplina para um regime controle é portanto, reconhecer modos de governança distintos. Novamente a pergunta é como governar uma multidão de singularidades? Como torná-la produtiva? A grande questão que ficou sem resposta

no pensamento de Foucault é: se o poder está onipresente na sociedade é possível se falar em uma resistência que esteja fora do poder? Negri e Hardt vão assumir em oposição ao biopoder sobre a produção da vida, uma biopolítica, que, pelo contrário, busca formas alternativas de produção de subjetividade, que não só resistem ao poder mas buscam uma autonomia em relação a ele.

> "Nossa leitura não identifica a biopolítica com poderes localizados e produzidos sobre a vida – ou seja, a produção de afetos e linguagens através da cooperação social e da interação dos corpos e desejos, a invenção de novas formas da relação entre o eu e os outros, e por aí em diante – mas também afirma a biopolítica como a criação de novas subjetividades que são apresentadas de uma só vez como resistência e desubjetivação." (HARDT, NEGRI, 2009:58)

As contradições das formas contemporâneas do desenvolvimento capitalista, a dispersão da fábrica na sociedade, permitem a expansão do Comum, visto que a produção de cada vez mais dependente de níveis de liberdade e acesso a banco de dados, redes de comunicação e circuitos culturais. O capital se torna portanto cada vez mais biopolítico, criando, investindo e ordenando de acordo com suas hierarquias de valor econômico, a produção da vida. Assim, cada vez o mais o econômico se torna indistinto do político, já que a criação de valores na economia se torna cada vez mais a criação de relações sociais, de formas de vida, "e, em última análise, a própria sociedade" (HARDT, NEGRI, 2005). A biopolítica seria definida portanto pela potência da vida em governar-se, e o biopoder, um comando contra a autonomia da vida, que expropria sua produção comum. O Comum que queremos pensar aqui, portanto, deve brotar a partir desta relação biopolítica.

O Comum só pode partir portanto do conceito de multidão, o conjunto de singularidades que produz através de vastas de redes de comunicação e cooperação, aparatos linguísticos e todo o trabalho imaterial que é hegemônico para a criação de valor na economia capitalista atual. O paradoxo é que o capital depende desse trabalho vivo e dialógico para criar valor de troca mas ao mesmo tempo ele tenta sempre "transformar a multidão em uma unidade orgânica assim como a soberania moderna quis transformá-la em um povo".(HARDT, NEGRI, 2005)

A inovação é fruto de redes descentralizadas e mentes coletivas, um cérebro disperso, policêntrico, no bojo da sociedade. O paradoxo em questão é que para ampliar sua produtividade o capital depende cada vez mais da inovação, e consequentemente,

desse Comum, mas, para mantê-lo produtivo ele não pode abrir mão do comando, da transformação desse comum em unidade orgânica, em propriedade privada. Não é por acaso que nas últimas décadas as patentes e direitos de autor vem intensificando seu papel de controle sobre diversos bens imateriais, especificamente sobre códigos genético, formas de vida, fórmulas farmacêuticas, softwares, e bens culturais como filmes e músicas. Mas se por um lado cada vez mais a legislação é restritiva pra uma gestão comum desses bens, da mesma maneira os meios para que esse conhecimento circule são cada vez mais ubíquos, e a produção biopolítica do comum cada vez mais excedente. O capital necessita que cada vez mais canais de comunicação sejam abertos, mas ao mesmo tempo precisa criar maneiras de expropriar o comum produzido no seio dos fluxos informacionais.

Nesse contexto, é necessário reconhecer a relevância da transparência e da opacidade como valores fundamentais na produção e aplicação dos códigos nas redes distribuídas de comunicação e das suas consequências políticas. Essa centralidade se torna ainda mais relevante diante da constatação de que quanto mais interativas são as tecnologias, mais capazes de coletar informações dos indivíduos elas se tornam, transformando-se em potenciais dispositivos de vigilância. O que vai operar o caráter e a profundidade da participação e da vigilância é o código que media as interações, e sua transparência e/ou opacidade passam a ser os atributos determinantes para o controle da comunicação.

A comunicabilidade crescente de uma sociedade cada vez mais atravessada por redes interativas coloca em destaque a seguinte questão: a arquitetura dos meios pelos quais a comunicação é mediada não deveria ser alvo de um controle público?

> "Podemos partir do pressuposto que os assuntos e os temas que definem o modo, a forma e os limites de como as pessoas podem comunicar-se e interagir socialmente deveriam ser assuntos públicos. Um software e um protocolo de comunicação fechado é opaco e sem transparência diante das pessoas que o utilizam e têm seu comportamento por ele regrado. Um software e os protocolos de comunicação como linguagens básicas da sociedade em rede devem ser propriedade privada de algumas empresas ou devem ser públicos? Quais os riscos da adoção de um ou outro modelo para a liberdade de expressão e comunicação? Qual a possibilidade da constituição de uma esfera pública a partir de redes cujas linguagens essenciais são de domínio restrito?" (SILVEIRA, 2006)

Em oposição a afirmação da transparência como condição, para a cultura *hacker*, a privacidade individual é um valor inexorável. Sua função é garantir a liberdade de movimentos de indivíduos através das redes, o que desabilita o controle governamental ou corporativo sobre os fluxos da comunicação. Dessa maneira, a transparência dos códigos de mediação deve garantir a opacidade do anonimato. Para os *hacker*s, a privacidade significa o poder de um indivíduo sobre as informações que ele gera, podendo selecionar quais partes das informações ele quer que se tornem públicas. A preocupação dos *hacker*s com a preservação do anonimato é frequentemente associada a ameaça de agentes externos. A vigilância é associada ao modelo panóptico das sociedades disciplinares apontadas por Focault, um modelo onde todos sabem que são vigiados por um dispositivo central, porém, não sabem onde se encontra o olhar vigilante. 1984, livro de George Orwell, é o exemplo trágico dessa sociedade, onde um estado totalitário é o centro vigilante que controla mentes e corações. A aversão a interferência estatal nas atividades do ciberespaço demonstra a fé na Internet como um território livre da vigilância.

A participação através de *blogs*, redes sociais, e diversas ferramentas interativas, possui em seu cerne uma ambiguidade fundamental. Se por um lado as novas tecnologias de comunicação são celebradas por ultrapassar a mediação centralizada da mídia de massa, por outro, quanto mais participativas elas o são, mais capazes de coletar informações sobre indivíduos elas se tornam. ”São ao mesmo tempo uma dimensão potencial de resistência às práticas de vigilância e controle, e uma fonte profícua de dados e conhecimento que nutrem essas mesmas práticas, sobretudo as de vigilância digital.” (BRUNO, 2008) Andrejevic demonstra como na esfera das redes interativas, “cada ação e transação gera informação sobre si.” (2007). O autor compara esse fenômeno com os cercamentos de terra associados ao início da acumulação capitalista e do controle dos meios de produção. Os cercamentos digitais estariam da mesma maneira dividindo a sociedade entre os que controlam a informação e os que a geram:

> “Uma divisão similar de grupos pode ser distinguida no emergente cercamento digital entre aqueles que controlam espaços interativos privatizados e aqueles que se submetem a formas particulares de monitoramento para obter acesso a bens, serviços e conveniências.”(ANDREJEVIC, 2007)

Toda interação é potencialmente uma ferramenta de vigilância. Bruno aponta como o monitoramento de informações é imanente a ferramentas de busca e redes

sociais, que para serem eficientes, necessitam analisar, cruzar e manipular informações geradas por usuários, incorporando a suas engrenagens e critérios dispositivos de vigilância (BRUNO,2009). Andrejevic, cético em relação ao caráter libertário da Internet, dá vários exemplos de como agentes privados se beneficiam desta prática. A Google, uma das maiores empresas da Internet, tem como seu principal bem o registro das ações de seus usuários. Seus códigos coletam, organizam e analisam dados para possibilitar uma publicidade direta, customizada e eficaz, antecipando os desejos de consumidores.

Por mais que instrumentos de mapeamento, verificação e coleta de dados tenham diversos fins, todos são potencialmente dispositivos de vigilância. Muitas vezes os objetivos se transformam, como no exemplo das câmeras de supermercados inicialmente instaladas para evitar furtos e que passaram a registrar através de *softwares* as escolhas e a circulação dos consumidores nos estabelecimentos. Porém, sendo estes dispositivos destinados à vigilância ou não, o que se destaca em todos estes exemplos é que a ação, a circulação e a produção de indivíduos se tornam cada vez mais transparentes para empresas, governos e para os outros. Por outro lado os códigos e suas interfaces de mediação que exercem a coleta e a mineração desta enxurrada de dados lhes são opacos.

> "[...]é o retorno da privacidade como uma vingança: para nós é quase impossível saber o que está sendo feito com toda informação sobre nós mesmos, graças a barreira de privacidade alegada por organizações comerciais e a confidencialidade e segurança nacional evocadas pelo estado. O resultado pode ser descrito como um perda assimétrica de privacidade: indivíduos estão se tornando cada vez mais transparentes para agências de monitoramento tanto públicas como privadas, mesmo que as ações destas agências permaneçam obstinadamente opacas junto a tecnologias fazem com que coletar, compartilhar, analisar grandes quantidades de informação se torne mais fácil do que nunca" (ANDRJEVIC, 2007)

Por mais que a Internet seja um conjunto de protocolos abertos e recombináveis, ela também é povoada paralelamente por diversos códigos, proprietários e opacos, que são empreendidos em múltiplas interfaces de participação. A opacidade destes códigos é necessária para estes agentes por garantir opacidade dos dados coletados diante da transparência da privacidade de indivíduos. O paradoxo apontado por Andrejevic é que a privacidade de uns se torna propriedade privada de outros. Esta constatação coloca em

cheque o caráter democratizador associado às novas tecnologias de comunicação e aponta para um panorama onde o acesso, manipulação, e compreensão dos códigos se tornam então questões de conflito.

Esse conflito nos último anos vêm ganhando novos contornos. Em artigo recente Chris Anderson (2010) proclama: a *web* está morta. Ele se refere ao crescente número de plataformas de serviços que funcionam em ambientes semi-fechados que usam a Internet, ou seja o TCP/IP, para transportar os dados, mas não usam o navegador como interface. É sobre a camada de aplicação que uma *web* aberta e uma *web* fechada entram em conflito. Serviços como Twitter[2] e Facebook[3] mediam um fluxo de mensagens de milhões de usuários, mas estes só são acessíveis a partir de suas interfaces, de seus "jardins murados". Mesmo a prática de disponibilizar API's[4] para que outros aplicativos possam acessá-las se limita a enriqeucer estes jardins. De fato é como um *firewall* de mensagens, as mensagens podem sair e entrar, mas da maneira e nas condições que os proprietários destes "jardins" impõe.

A mesma preocupação é externada por Tim Berners-Lee, o criador da *web*. A grande questão para os defensores da *web* aberta é a padronização dos protocolos, pois estes, ao serem abertos e padronizados permitem a universalização do acesso e a interoperabilidade. As ilhas de internet semi-fechadas que estão emergindo com os novos serviços e configurações ativam uma nova prática de privatização de novas camadas, isolando dados de acordo com as conveniências comerciais. A neutralidade da rede também vêm sendo ameaçada por provedores de acesso que privilegiam largura de banda para determinados provedores de conteúdo.

Os conflitos entre transparência e opacidade, vigilância e privacidade, propriedade e acesso abordados até aqui demonstram como o código e a arquitetura de rede se tornaram centrais para o entendimento da contemporaneidade e consequentemente são de fundamental importância para se pensar o problema do Comum. Para diversos autores, o fato de os princípios organizacionais da rede estarem sendo ameaçados constantemente refletem uma guinada em direção a utilização da Internet como mecanismo de controle. Consideram portanto, que a Internet e seus princípios organizacionais fundadores eram livres de tais ameaças, e que permitiam,

[2]Disponível em: http://twitter.com
[3]Disponível em: http://facebook.com
[4]API, de *Application Programming Interface* (ou Interface de Programação de Aplicações) é um conjunto de rotinas e padrões estabelecidos por um software para a utilização das suas funcionalidades por programas aplicativos que não querem envolver-se em detalhes da implementação do software, mas apenas usar seus serviços. Fonte: Wikipedia

pelo contrário, um ambiente de liberdade e ausência de controle. (BERNERS-LEE,2010)

Galloway discorda dessa concepção ao afirmar que o controle é endêmico em qualquer rede distribuída. "O controle estava lá desde o dia um. Os princípios fundadores da Internet são controle e não liberdade" (2004:141). Para o autor, o que seria uma garantia de liberdade - a universalização e padronização dos protocolos - são caraterísticas que permitem o funcionamento desse novo diagrama de poder. São elas que permitem que nada se exclua da rede, que tudo esteja dentro e nada esteja fora.

> "Nossas redes são armas. Nossas *web*s são também as nossas próprias armadilhas. A interatividade é penosa. A transparência vem com o custo de se fecharem todas as coisas. Essa é a condição do cidadão digital hoje. É nossa tarefa, portanto, não festejar o heroísmo da rede, mas, em vez disso, oferecer uma reconstrução crítica do código, de forma a que o próprio aparelho seja reformulado como um instrumento de prática, e não como um instrumento de gestão, como permanece hoje." (GALLOWAY, 2010:98)

Esse principio é nos dias atuais capaz de dar forma a um novo tipo de poder: a análise dados. Esse poder, agrupando todos os tipos de dados que circulam pelas diversas camadas de rede de aplicações existentes, unido-se a bancos de dados de cartão de crédito, telefonia móvel é capaz de extrair os mais variados tipos de informação, construir análises de comportamentos, agrupamento de perfis e produzir modulações de afetos. Fenômeno também conhecido como Big Data, pode processar com fins distintos e com algorítimos cada vez mais eficazes, uma quantidade avassaladora de dados. A revelação da existência do PRISM[5] através do vazamento de informações do analista da CIA, Edward Snowden, desvendou o projeto técnico do algoritmo para vigilância dos fluxos de informação que passam por redes proprietárias. Dentre as maiores: Facebook, Google, MSN, Skype e Youtube colaboravam com o governo americano, especificamente com a agência NSA, para realizar suas práticas de vigilância

Nesse contexto o anonimato e a criptografia surgem como instrumentos bipolíticos de luta pela autonomia da multidão na sociedade de controle. Sua emergência não é nova, pois, desde que o poder computacional e a interação de computadores em rede passou a se incorporar nas relações sociais, institucionais e

[5] Disponível em: <http://pt.wikipedia.org/wiki/PRISM_(programa_de_vigil%C3%A2ncia)>. Acesso em 09 de maio de 2013.

econômicas, o anonimato e criptografia aparecem tanto no centro quanto nas bordas dos dispositivos informacionais.

A própria criptografia, prática milenar, tecnologia de guerra, se torna ferramenta essencial para a expansão global das transações financeiras e comerciais. Mas paralelamente, no contexto da cultura hacker, novos agenciamentos forjaram novas práticas como estratégias de se opor ao monitoramento, à modulação dos afetos permitida pelo poder de análise, pelo vigilantismo permanente das redes de comunicação.

Um dos principais marcos deste percurso foi a invenção da criptografia assíncrona ou criptografia de chave pública[6], acontecimento que partiu do artigo *"New Directions in Criptography"* dos pesquisadores autônomos Whitfield Diffie and Martin E. Hellman (2013, ONLINE) e o advento do protocolo RSA[7], em 1977. A partir da criptografia assíncrona, o embaralhamento de uma mensagem poderia então ser feito sem que necessariamente o emissor houvesse tido algum contato anterior com o receptor da mesma, ou seja, sem que chave de acesso fosse previamente compartilhada. Essa descoberta metodológica e matemática, que mais tarde foi incorporada por bancos e grandes empresas, abria o caminho para que parcerias e conversações anônimas pudessem permanecer anônimas. O estímulo para a criação era uma previsão do que iria acontecer em breve. Em um mundo onde as conversações seriam cada vez mais estabelecidas em redes interconectadas, como garantir a privacidade de atores que não se conhecem pessoalmente, ou em outras palavras, como garantir novas conversações anônimas?

Desde aquele momento, a *National Security Agency (NSA)*, agência estadunidense que hoje está no centro dos escândalos de espionagem do governo americano revelados por Edward Snowden, e que desenvolvia secretamente tecnologias de criptografia para o exercício de de suas funções, entrou em conflito com estes pensadores autônomos da criptografia. Investigações, processos judiciais, intervenções, foram práticas recorrentes da agência com o objetivo de impedir a disseminação dessas tecnologias, ou pelo menos, controlar seus parâmetros (como limitar o número de bits ou impor *backdoors* dentro do código) (LEVY, 2001) . De fato, a criptografia era considerada uma arma de guerra, e esse era o argumento para exercer tal controle.

[6]Disponível em: <http://pt.wikipedia.org/wiki/Criptografia_de_chave_p%C3%BAblica>. Acesso em 09 de maio de 2013.
[7]Disponível em: <http://pt.wikipedia.org/wiki/RSA>. Acesso em 09 de maio de 2013.

Quando Phil Zimmerman publicou suas versões do *Pretty Good Privacy* (PGP) [8], em 1992, foi processado pela exportação ilegal de armamentos. Mas a Internet já era uma realidade bem disseminada, e o código do PGP já estava armazenado em diversos discos rígidos fora da fronteiras dos Estados Unidos.

Mas se todo esse espírito de proteção da privacidade individual prevaleceu nos anos 70, tal preocupação se manteve nos anos 80, no destaque que é dado à criptografia no contexto da cultura hacker e em sua ramificação *Cyphepunk.* O Manifesto *Cypherpunk*, escrito por Eric Huhges, retrata a importância da privacidade para os primeiros ocupantes do ciberespaço e demonstra uma percepção otimista das tecnologias eletrônicas.

> "Nós devemos defender nossa própria privacidade se esperamos ter alguma. Devemos nos juntar e criar sistemas que permitam transações anônimas. As pessoas vêm defendendo sua própria privacidade por séculos através de segredos, escuridão, envelopes, portas fechadas, cumprimentos secretos e *couries*. As tecnologias do passado não permitiam uma privacidade forte, porém, as tecnologias eletrônicas permitem." (HUGHES, 1993)

Porém, o que queremos destacar neste trabalho é que se o anonimato e a criptografia em um primeiro momento surgem como ferramentas de defesa da liberdade individual e garantia de privacidade, estes passam a ser embutidos dentro de códigos de aplicações para dar vida a novos possíveis, para forjarem novas relações de força. De outro modo, podemos dizer que não deixam de ser ferramentas de resistência à vigilância , mas também se tornam criadoras de novos agenciamentos.

Três exemplos são importantes para ilustrar tal fenômeno. O primeiro se refere a prática de compartilhamento de arquivos. O evolução das tecnologias de troca de arquivos teve um desenvolvimento "darwiniano" (MALINI e ANTOUN, 2013), onde cada tecnologia se que se sobrepunha a anterior permitia mais eficiência e mais anonimato para os usuários. O melhor exemplo é o protocolo *Bittorrent*. Sua foi inovação foi colocar as informações sobre os arquivos e a localização dos nós em um outro arquivo, é que estas ficam então independentes do sistema como um todo: não há lista de usuários, listas de arquivos, ou qualquer tipo de indexação ligada ao sistema.

Em um primeiro momento , a instância que fez essa operação são os chamados *trackers*. Os *trackers* são servidores aos quais os arquivos *.torrent* estão atrelados. Por

[8] Disponível em: http://pt.wikipedia.org/wiki/PGP. Acesso em 09 de maio de 2013.

isso os clientes de *Bit torrent* não possuem sistemas de busca internos, mas a a busca pelos arquivos é realizada nos *trackers* que os disponibilizam. Essa característica foi importante para desassociar as indexações de arquivos do sistema de compartilhamento fazendo com que este fique imune a apelações judiciais por quebras de propriedade intelectual, função que fica destinada aos *trackers.* Se um *tracker* cai, o sistema não para, novos *trackers* podem surgir no seu lugar. Ao proceder com o enxame de nós, o *Bit torrent* elimina o individuo da ação da troca. Não há um ente que oferece e um outro que recebe o arquivo, mas são diversos que oferecem e recebem pedaços de arquivos simultânea e aleatoriamente, uma operação coletiva e anônima, pois não há mais um receptor e um emissor: o código induz a prática ao anonimato. Sim, não é impossível descobrir IP's de quem esteja utilizando o protocolo e há formas de identificação e de bloqueio de tráfego de dados, mas, fundamentalmente, o *Bittorrent* transforma uma operação individual em uma multiplicidade de operações anônimas.

Outra manifestação importante é a prática cada vez mais recorrente das moedas criptográficas. Estas efetuam a possibilidade de fazer transações financeiras e comerciais através de moedas que estejam desvinculadas do sistema econômico formal, sem controle por Bancos Centrais e instituições financeiras. A de mais renome, e a que hoje em dia mobiliza mais transações e afetos é a moeda *BitCoin*[9]. Sua matemática é complexa, mas a ideia por trás do código é bem simples. Em primeiro lugar, ela é capaz de possibilitar que transações financeiras sejam realizadas ponto-a-ponto (P2P) sem a mediação de instituições, e de forma anônima, através de protocolos abertos de autenticação por chave criptográficas. O emissão da moeda é controlada por um algoritmo que prevê um número determinado de *Bitcoins* (21 milhoẽs até 2100), criando dessa forma um lastro permanente. A emissão da moeda é também controlada por um sistema matemático, onde aqueles que se dispõem a armazenar transações de *bitcoins*, em um banco de dados distribuído, fazem a mineração (como uma analogia a mineração de metais para criação de lastro de moedas) disponibilizando o processamento de dados de seus hardwares para armazenar os blocos de transações (*blockchains*) que precisam passar por cálculos criptográficos impostos pelo protocolo do bitcoin.

Fechado pelo FBI em 2013, o site de comércio *The Silk Road* era local de encontro para a realização de transações ilegais utilizando *Bitcoin*, principalmente para a comercialização de drogas. Mas seus mecanismos têm criado todo um ecosistema em

[9] Disponível em: http://pt.wikipedia.org/wiki/PGP. Acesso em 09 de maio de 2013.

torno do Bittcoin, desde empresas de câmbio, fazendas de mineração, especuladores; e seu futuro como uma moeda ainda é incerto, mesmo que venha cada vez a mais a ser utilizado por estabelecimentos comerciais. O *Bitcoin* emerge de uma cultura de programadores que valoriza o código aberto. Sua arquitetura e implementação criam um tipo de relação onde convivem a transparência das transações e a opacidade daqueles que as executam. Ele revela um uso das práticas de criptografia e anonimato para tentar reinventar o mundo da economia, através do código. Esse desenvolvimento é também um reconhecimento da liberdade de interação econômica como um uma necessidade ética. Todos as informações de transações econômicas atualmente são registrados nos banco de dados de poucas instituições, possibilitando – ironicamente, em um ambiente onde o capital financeiro é cada vez mais desregulado - um controle restrito sobre estas atividades. Essencialmente, as criptomoedas são uma reação às manipulações monetaristas do capitalismo contemporâneo e à fragilizaçãocada vez maior da privacidade financeira.

O protocolo *Bitcoin* e as moedas criptográficas têm ainda um longo caminho pela frente para se estabelecer efetivamente. Já existem enfrentamentos legais e ainda há questões técnicas para garantir um anonimato permanente. Mas sua arquitetura, suas implementações, as ideias que estão por trás de suas interfaces já são uma realidade, e ampliam o escopo de mundos possíveis que podem se efetuar no campo das interações econômicas livres e descentralizadas.

Por último, gostaríamos de destacar o fenômeno dos vazamentos de informações protagonizados pela entrada em cena do *WikiLeaks* no jogo da guerra em rede (ARQUILLA e RONFELTD, 2003). O que o *Wikileaks* propôs é estabelecer uma cultura de vazamento para que "cidadãos comuns" possam anonimamente, utilizando a criptografia, denunciar abusos de poder, documentações sigilosas, segredos de Estado e de Corporações que comprometam diversas esferas da vida pública. Seguindo o lema de transparência para os poderosos, privacidade para o povo, a organização vêm desde 2006 acumulando casos de vazamentos sejam de arquivos da Guerra do Iraque, Guerra do Afeganistão, e o famoso *Cablegate* onde correspondências do corpo diplomático americano forma massivamente divulgadas revelando conteúdos constrangedores para o governo estadunidense. Sua atividade abre precedentes para novas relações no campo do jornalismo e no próprio jogo da governabilidade. Pois no mundo das interações em rede permanentes, no mundo do Big Data e poder de análise das grandes corporações e

governos, o *Wikileaks* inventou um contra poder, um Big Data da multidão, capaz de intervir, através da rede, nos processos de criação de narrativas da geopolítica mundial.

> "A ciberguerra começou. Não uma ciberguerra entre Estados como se esperava, mas entre os Estados e a sociedade civil internauta. Nunca mais os governos poderãoestar seguros de manter seus cidadãos na ignorância de suas manobras. Porque enquanto houver pessoas dispostas a fazer leaks e uma internet povoada por wikis surgirão novas gerações de wikileaks." (CASTELLS, 2010, ONLINE)."

Pois ao utilizar o anonimato e a criptografia no interior das redes distribuídas de comunicação, o *Wikileaks* utilizou o anonimato e a criptografia, não para defender a privacidade de indivíduos, mas para criar um ruído dentro de comunicações sigilosas.

Enxergamos, portanto, o *Wikileaks* como uma ferramenta de força ativa que usa o anonimato e a criptografia para promover interferências em determinados fluxos de comunicação, reinventando os usos de códigos para dar transparência a determinados processos sem abrir mão de garantir as privacidades individuais. Se todos os nós estão conectados em redes, algumas opacas, mas a maioria transparentes, o *Wikileaks* intervêm e abre a possibilidade da inversão dessa lógica em qualquer ponto desse emaranhado de arestas.

> "Dado ao fato de internet ter se tornado, no campo da circulação midiática, uma mídia de vazamento, o controle da produção da informação também mudará de função. No lugar de bloquear a informação, sonegá-la, algo compartilhado tanto pelas fontes estatais, quanto pelos próprios veículos tradicionais de comunicação (parte do seu valor será extraído das chantagens e promiscuidade com determinadas figuras do poder). A internet ocupa assim um hiato entre um poder pós-moderno que sonega e uma sociedade que se libera dos antigos pólos de emissão. É por isso que no lugar de polícia contra a mídia de vazamento, o novo cerceamento do poder à sociedade será marcado pela capacidade de controle da produção da linguagem (essas narrativas sociais) produzida pela multidão de singularidades em rede." (ANTOUN e MALINI, 2013, ONLINE)

O Comum, portanto, está embricado neste jogo de criação de códigos, no bojo desta ciberguerra. A partir dessas premissas é possível pensar o Comum – e o anonimato e a criptografia - também como um êxodo. Um êxodo da relação com o capital, do poder de análise, da modulação de afetos: a construção de uma autonomia ao comando e uma busca por condições de produção de subjetividade que estejam sob os

próprios termos da multidão, com seus próprios mecanismos de cooperação e comunicação.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDERSON, C. **The Web Is Dead. Long Live the Internet.** Wired Magazine**.**Disponível na Internet: http://www.wired.com/magazine/2010/08/ff_webrip/all/1 Acesso em: 22/12/2010

ANDREJEVIC, M. "**The Work of Watching One Another: Lateral Surveillance, Risk, and Governance**" In **Surveillance & Society**, 2(4): 479-497, 2005.

_____ iSpy . University Press of Kansas, 2007

ANTOUN, H. MALINI, F. **Ontologia da Liberdade na Rede: as multimídias e os dilemas da narrativa coletiva dos acontecimentos**. In: xix Econtro da Compós. Anais. 2010

ANTOUN, H MALINI, F. **Controle e biolutas na cibercultura: monitoramento, vazamento e anonimato na revolução democrática do compartilhamento.** In: XX Encontro da Compós, 2011, Rio Grande do Sul. [Trabalhos apresentados]. Rio Grande do Sul: 2011. Disponível em: <http://bit.ly/MRKo9F>. Acesso em 17 de março de 2013.

ARQUILLA, J. RONFELDT, D. C**uál es el futuro de las redes y de las guerras em rede?** In:_____. Redes y guerras em rede: el futuro del terrorismo, el crime organizado y el activismo político. Madri: Alianza editorial, 2003.

BERNERS-LEE. T. **Long Live the Web: A Call for Continued Open Standards and Neutrality**. Disponível na Internet: http://www.scientificamerican.com/article.cfm?id=long-live-the-web. Acesso em: 22/12/2010

BRUNO, F. **Monitoramento, classificação e controle nos dispositivos de vigilância digital**.
Famecos, 2008

_____. **Mapas de crime: vigilância distribuída e participação na cibercultura**. Compós, 2009

CASTELLS, M. **A ciberguerra do Wikileaks**. Observatório da Imprensa, 15 dez. 2010, d 620. Disponível em: <http://www.observatoriodaimprensa.com.br/news/view/a-ciberguerra-do-wikileaks>. Acesso em: 26 de abril de 2013.

DIFFIE, W. HELLMAN, M. **New Directions in Criptography**. Disponível na Internet: http://www.cs.tau.ac.il/~bchor/diffie-hellman.pdf. Acesso em: 22/12/2013

FOUCAULT, Michel. **História da Sexualidade I: A Vontade de Saber**. Rio de Janeiro: Graal, 1993

_____. **Multidão**. São Paulo. Record, 2005

_____. **Commonwealth**. Cambridge. Harvard Univesersity Press. 2009

LEVY, S. **Crypto**. New York. Penguin Books. 2001

MALINI, F. e ANTOUN, H. **A internet e a rua**: ciberativismo e mobilização nas redes sociais. Porto Alegre, Sulina Publishing House, 2013.

SILVEIRA, S. **Sociedade dos Códigos: entre a opacidade e a liberdade**. Comunicação & Sociedade, São Bernardo do Campo /SP, v. 27, n. 45, p. 57-78, 2006.