DOI: 10.5216/sec.v15i1.20677

Controle social e prática hacker: tecnopolítica e ciberpolítica em redes digitais[1]

Henrique Parra
Doutor em Educação (Universidade Estadual de Campinas)
Professor na Universidade Federal de São Paulo
henrique.parra@unifesp.br

Resumo Ao analisar alguns casos concretos, relativos às possibilidades de controle e acesso à informação em redes digitais, discutiremos como essas situações dão forma à política na cibercultura. Trata-se de pensá-la simultaneamente como o conflito pelas configurações sociotécnicas das tecnologias digitais (*tecnopolítica*), e as dinâmicas da política ciberneticamente mediada (ciberpolítica). Ao articular essas duas dimensões, analisaremos como a constituição e os modos de apropriação desses dispositivos definirão o que adentra ou não o campo do visível e do enunciável, portanto, o campo da regulação pública e do controle, dando forma a novos territórios de direitos, resistência, conflitos sociais e exploração econômica.

Palavras-chave: tecnopolítica, ciberpolítica, cibercultura, controle, protocolo.

> *Whatever code we hack, be it programming* "language, poetic language, math or music, curves or colourings, we create the possibility of new things entering the world" (Mckenzie Wark)

Introdução

O artigo resulta de um momento exploratório da pesquisa que objetiva, neste primeiro movimento, mapear alguns problemas e questões em torno das formas contemporâneas de exercício do poder e da prática política no contexto das relações sociais cibermediadas. Na medida em que as tecnologias digitais modificam as fronteiras anteriormente estabelecidas em diversos domínio da vida social (trabalho e não trabalho; produção e consumo; público e privado, entre outras), observamos profundas reconfigurações nas dinâmicas sociais, econômicas e políticas que exigem uma observação empírica de processos muitas vezes "invisíveis". Simultaneamente, para dar "existência" e problematizar tais mutações, é também necessário encontrar (ou criar) referências analíticas apropriadas.

Partiremos, portanto, da escolha arbitrária de algumas situações consideradas exemplares, nas quais poderemos observar o impacto das

1. Versões preliminares deste trabalho foram apresentadas em 2011 no XI Congresso Luso Afro Brasileiro de Ciências Sociais (Conlab) e no 35° Encontro Nacional da Anpocs. Agradeço às críticas dos debatedores Claudio Luis de Camargo Penteado e Marcus Abilio Gomes Pereira e aos participantes do grupo de trabalho que contribuíram com sugestões para o aperfeiçoamento do texto.

tecnologias digitais de informação e comunicação nas dinâmicas que desejamos investigar. Ao descrever alguns casos concretos, relativos à produção e ao controle de informações em redes digitais, discutiremos como tais exemplos apresentam uma arena renovada de conflitos que dão forma a novos campos políticos. Aqui, trata-se de pensar a política na cibercultura em duas direções: como política das tecnologias digitais (tecnopolítica) e também como política ciberneticamente mediada[2] (ciberpolítica). Enquanto a primeira refere-se às disputas sobre as configurações sociotécnicas do dispositivo, portanto, constitutivas da própria tecnologia, a segunda diz respeito às ações políticas que se utilizam dessas tecnologias, sem necessariamente interrogar suas preconfigurações. Certamente, do ponto de vista prático, ambas as dimensões (tecnopolítica e ciberpolítica) misturam-se frequentemente.

Contexto

O contexto mais amplo em que nossas preocupações estão inseridas é o universo de relações sociais que se realizam através do crescente uso dos dispositivos de informação e comunicação em redes digitais. Seja nas novas formas de sociabilidade, seja nas dinâmicas de trabalho e consumo, seja nas experiências estéticas ou nas práticas políticas, a mediação sociotécnica desses dispositivos introduz, graças às suas especificidades, um potencial de rastreabilidade e de quantificação de toda ação cibermediada. Ora, o que significa interagir através de um *médium* capaz de registrar e produzir dados de transações e movimentos infinitesimais? Como participamos dessas dinâmicas? Que condição é esta em que a fruição espontânea ou o trabalho não remunerado podem ser convertidos em indicadores passíveis de mercantilização? Ou ainda, como produzimos através do livre uso dessas tecnologias o poder que nos controla?

No Brasil, tais questões ganham urgência e relevância no momento em que iniciativas legislativas no âmbito federal vão causar forte impacto sobre a regulação do ambiente digital em suas diversas manifestações: condições de acesso à rede, possibilidades de acesso, distribuição e compartilhamento de conteúdos (bens culturais e científicos), identificação e registro da comunicação dos internautas, infraestrutura de comunicação etc. Exemplo disso são: a proposta de Marco Civil da Internet; a Lei de Cibercrime (conhecida como AI-5 Digital); o projeto que regulamenta a proteção de dados pessoais; a reforma de Lei de Direitos Autorais e mesmo o Plano Nacional de Banda Larga.

Como expressão inicial deste cenário cibercultural (Trivinho, 2001), tomamos a emergência de uma fina malha informacional que recobre todo o planeta e que conecta de maneira indistinta seres biológicos e artificiais, máquinas cibernéticas, bancos de dados, instituições e outros objetos materiais e imateriais. No final do século XX, duas tecnologias originalmente concebidas para responder a demandas militares tornam-se amplamente disponíveis para uso civil e comercial. A partir dos anos 90, a internet passa a ser gerida por organizações da sociedade civil e acelera seu processo de expansão global impulsionada por empresas privadas, governos, universidades e organizações da sociedade civil.[3] Nesta mesma década, o governo Clinton decide "abrir" o sinal do sistema norte-americano GPS (Global Positional System), até então restrito à utilização militar, tornando-o disponível para uso civil e comercial.[4] O acesso ao sistema de geolocalização, através da introdução de uma transmissão não criptografada, permite aos equipamentos civis um grau de precisão inferior ao disponível para uso militar, no entanto, suficiente para permitir a localização geofísica de objetos com uma pequena margem de erro comercialmente aceitável.

Se, por um lado, a internet permitiu a interação sincrônica entre pessoas e objetos distantes fisicamente, criando uma situação de "superação" do espaço físico (desterritorialização) e nutrindo novas experiências e categorias espaciais, os dispositivos GPS, por sua vez, permitiram novamente "territorializar" as entidades comunicantes. Pode-se interrogar que esta mesma possibilidade de territorialização também está presente, sob certas condições, na arquitetura (física e lógica) da internet, na medida em que tanto sua infraestrutura física como a gestão global da rede respeitam uma certa ordem geopolítica, com expressão nos Estados nacionais.

De partida, é preciso reconhecer uma diferença fundamental na "natureza" dessas tecnologias: enquanto a internet é uma tecnologia cibernética, portanto dependente de um sistema de "retorno", o GPS funciona através da triangulação por radiodifusão gerada por um conjunto de satélites orbitais. Quando aciono meu aparelho de localização no automóvel, ele simplesmente captura os sinais emitidos pelos satélites do sistema GPS e obtenho minha posição física. Da mesma forma como no rádio analógico do

2. Sérgio Amadeu da Silveira refere-se a essas duas dimensões como "política *na* internet" e "política *da* internet" (2009).

3. Uma versão bem sintética da história da internet está disponível no livro de Manuel Castells (2003).

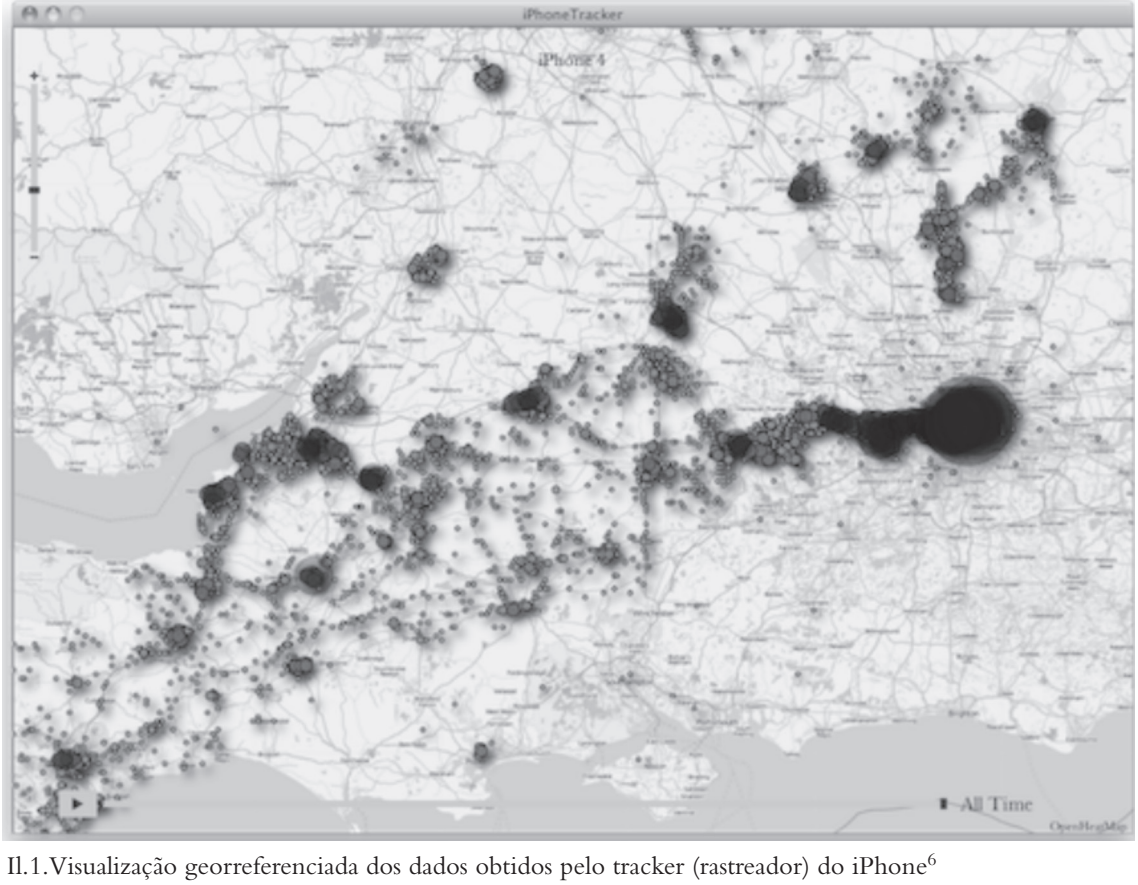
4. Na Wikipédia, em língua inglesa, há um boa descrição da história e do funcionamento do GPS. http://en.wikipedia.org/wiki/Global_Positioning_System. Acesso em: 31/5/2011.

meu automóvel, o emissor do sinal nada sabe a meu respeito: quanto tempo permaneci sintonizado na estação, qual estação eu ouvia antes e depois etc. Por outro lado, quando navegamos e acessamos um site na internet, tanto as condições técnicas (softwares e hardwares) que permitem esta comunicação, quanto os "rastros" (*digital footprints*) que deixamos no ciberespaço, dão margem a inúmeras possibilidades de coleta de informações a respeito dos internautas.

Guardadas as devidas diferenças entre essas tecnologias, o que nos interessa analisar a partir dessa simultaneidade histórica – que torna disponível aos civis duas tecnologias de uso militar – é o surgimento de uma "malha" informacional que recobre, como nunca antes na história da humanidade, toda a superfície do planeta e, potencialmente, todos os indivíduos que estão conectados aos dispositivos móveis de comunicação digital que oferecem acesso simultâneo à internet e aos sistemas de geolocalização.

Só para citar um exemplo do problema que nos ocupa, em abril de 2011, dois pesquisadores[5] demonstraram que o aparelho iPhone, da Apple, registrava dados geoespaciais do usuário em um arquivo que fica armazenado no dispositivo móvel e no computador com o qual seu proprietário faz a sincronização dos seus dados pessoais. Tal arquivo contém informações precisas sobre a localização e a movimentação do usuário em um determinado momento. Segundo os pesquisadores, não é possível afirmar que tais dados tenham sido acessados por terceiros ou pela própria Apple. No entanto, o principal problema apontado pelos pesquisadores é que tais informações são registradas sem o conhecimento dos usuários e ainda ficam relativamente disponíveis de forma não segura. A partir desses dados, os pesquisadores desenvolveram um aplicativo em software livre para realizar a visualização georreferenciada desses dados.

Sem adentrarmos em questões específicas às tecnologias de geolocalização, para nossa análise interessa apenas apontar como essas tecnologias combinam as dinâmicas de desterritorialização (através da comunicação em tempo real) com as dinâmicas de reter-



Il.1. Visualização georreferenciada dos dados obtidos pelo tracker (rastreador) do iPhone[6]

5. Conforme noticiado, os pesquisadores Ryan Neal e Paul Courbis foram, aparentemente, os primeiros a "descobrir" e examinar o arquivo com os dados georreferenciados. Fonte: *iPhone tracking: The day after*. Disponível em: http://radar.oreilly.com/2011/04/iphone-tracking-followup.html. Acesso em: 31/5/2011. Outras reportagens apresentam interessantes dados complementares. Veja: *Got an iPhone or 3G iPad? Apple is recording your moves*, http://radar.oreilly.com/2011/04/apple-location-tracking.html. Acesso em: 31/5/2011; iPhone Tracker, http://petewarden.github.com/iPhoneTracker/#8. Acesso em: 31/5/2011.

6. Os pesquisadores Alasdair Allan e Pete Warden desenvolveram um software livre (disponível para download) capaz de interpretar os dados registrados pelo iPhone e produzir mapas com os dados georreferenciados. Disponível em: http://petewarden.github.com/iPhoneTracker/#8. Acesso em: 31/5/2011.

ritorialização (comunicação geolocalizada), abrindo novas oportunidades para a produção e a gestão de informações. Quando essas duas dinâmicas se articulam, confrontamo-nos com novas possibilidades de coleta de dados informáticos transacionados nas redes digitais pelos sujeitos conectados, criando tanto possibilidades de interação e colaboração social como condições ampliadas de identificação e vigilância.

Ora, o que isso pode significar em termos de novas formas de controle social? Que formas de exercício do poder se desenham no momento em que todos podem se comunicar com "todos", em condições de completa "visibilidade"? Quais seriam as formas de controle engendradas pela crescente liberdade de comunicação e interação através das redes digitais?[7]

Assumo, como ponto de partida, que a internet, em sua configuração sociotécnica, é uma rede cibernética em que uma forma específica de "controle" está inscrita em seu funcionamento básico. Tal dinâmica, bem descrita por Alexander Galloway (2004) em termos de um "poder protocolar", é analisada no Brasil por pesquisadores[8] preocupados com os impactos sociais e políticos que as novas regulamentações[9] jurídicas poderão causar ao ambiente digital.

A comunicação cibernética ocorre graças a um ambiente devidamente ordenado por protocolos que definem regras específicas de funcionamento. Para que uma mensagem possa sair de um lugar e chegar noutro, por exemplo, os protocolos – padrões/convenções sobre especificações técnicas, mas também sociais[10] – asseguram que haja um "aperto de mãos" entre o emissor e o receptor. Nos dizeres de Alexander Galloway, o protocolo pode ser entendido como uma regra convencionada para governar de maneira distribuída um conjunto de comportamentos possíveis dentro de um sistema heterogêneo; ou, ainda, uma técnica para alcançar a regulação voluntária dentro de um ambiente contingente (2004, p. 8). Portanto, nesta acepção, o "controle" é entendido como um ordenamento específico e intrínseco ao processo comunicacional cibernético, e não como o exercício da dominação de um sujeito sobre outro. É sob esta perspectiva que iremos problematizar como esta forma específica de controle apresenta tanto um potencial de controle social (forma de dominação), como um potencial de descontrole (forma de resistência).

Na medida em que a comunicação em redes digitais funciona segundo determinadas configurações, resultantes de dinâmicas simultaneamente sociopolíticas e técnicas, a disputa sobre a regulação jurídica das atividades ciberneticamente mediadas torna-se fundamental para evitar a emergência de um controle social tirânico, seja ele corporativo ou estatal. É neste contexto que tais conflitos adquirem um importante significado político.[11] Vejamos a seguir três exemplos que revelam as tensões em jogo entre as dinâmicas de liberdade e controle social nas redes digitais. Na parte final do texto, indicaremos algumas questões que atravessam todos os casos analisados e que poderão servir como novas trilhas de pesquisa.

Dados pessoais e vigilância público-privada

Em ação desde 2006 – então conhecida apenas nos circuitos hacker e tecno-ativista – a pequena organização Wikileaks tornou-se mundialmente famosa em 2010. Foi neste ano que, graças à divulgação estratégica de um conjunto de documentos sigilosos do exército e da diplomacia norte-americana, a Wikileaks ganhou notoriedade internacional.

Logo após a publicação do vídeo *Collateral murder* – que mostra o ataque de helicópteros americanos a um grupo de civis iraquianos, matando entre eles dois funcionários (um repórter e um guia-motorista) da agência de notícias Reuters[12] –, um jovem mi-

7. Mais recentemente, durante as revoltas populares na Inglaterra, o governo e a polícia britânica colocaram em prática os potenciais de controle inscritos nessas tecnologias. Sobre o uso repressivo da vigilância de redes sociais na Inglaterra, veja: *Social networking surveillance: trust no one*. http://www.guardian.co.uk/commentisfree/cifamerica/2011/aug/12/social-networking-surveillance. *David Cameron considers banning suspected rioters from social media*: http://www.guardian.co.uk/media/2011/aug/11/david-cameron-rioters-social-media. *England riots: pair jailed for four years for using Facebook to incite disorder:* http://www.guardian.co.uk/uk/2011/aug/16/uk-riots-four-years-disorder-facebook

8. Os trabalhos de Sérgio Amadeu da Silveira são uma boa referência sobre o tema (Silveira, 2009, 2009-A).

9. Nos últimos anos, algumas iniciativas governamentais propuseram novos mecanismos legais para a comunicação eletrônico-digital. Até o momento, nenhuma dessas iniciativas foi concluída. Entre elas, poderíamos citar: o projeto de lei sobre proteção de dados pessoais; o projeto de lei que cria o Marco Civil da Internet; a reforma da Lei de Direitos Autorais, com novos dispositivos para o ambiente digital; o projeto de lei sobre cibercrimes.

10. Mesmo que se trate de uma especificação técnica, por envolver um desenho que interfere nas condições de interação entre os sujeitos, consideramos que muitos protocolos são simultaneamente técnicos e sociais, dado que prescrevem modos de comunicação e organização da informação.

11. Exploramos esses conflitos sob a perspectiva das transformações nas tecnologias de imagem e sua relação com os regimes de produção de conhecimentos (Parra, 2009).

12. A documentação jornalística sobre este vídeo e sua repercussão é muito ampla e está disponível em diversos sites. A página da Wikileaks sobre o episódio é uma excelente fonte sobre o caso, pois ela registra as muitas divergências entre as diferentes fontes utilizadas, bem como a disputa entre as versões sobre o episódio. Disponível em: http://en.wikipedia.org/wiki/July_12,_2007_Baghdad_airstrike#Leaked_video_footage. Acesso em: 31/5/2011.

litar foi preso pelas autoridades federais americanas sob a acusação de ser o "vazador" dos documentos publicados pelo site Wikileaks. Atualmente, o jovem encontra-se preso nos EUA e as informações sobre as circunstâncias de sua prisão e sua situação prisional são muito obscuras.[13]

A organização Wikileaks faz uso de um aparato tecnológico para garantir que o recebimento dos materiais a serem publicizados ocorra de forma a proteger o sigilo e o anonimato da fonte. Em recente entrevista, Julian Assange afirma que:

> As spokesperson for WikiLeaks, we are in a very difficult position concerning Bradley Manning. The difficulty of our position is that our technology does not permit us to understand whether someone is one of our sources or not, because the best way to keep a secret is to never have it. We are dealing with intelligence agencies that are very sophisticated. So instead of keeping source identity secret, we simply do not collect them at all, even in the first place. So we do not know whether Mr. Manning is our source or not, or whether he is some intermediary in this process or whether he knew a source. We have no understanding of this. And of course if we did know, we are obligated ethically to not reveal it.[14]

Portanto, pelas razões expostas, a organização não pode afirmar que tenha recebido os materiais do soldado Bradley Manning. A situação é especialmente complicada para Julian Assange, pois Manning é acusado de conspiração contra os EUA. Caso a investigação revele que a organização Wikileaks tenha incentivado Manning a fornecer os documentos, seus responsáveis poderão ser acusados do mesmo crime.

O problema sob análise neste artigo pode ser apreendido na própria superfície do evento, ou melhor, nas versões que circularam na imprensa norte-americana sobre a identificação de Bradley Manning. Tais relatos chamaram a atenção para um fenômeno importante a relativamente pouco investigado: a expansão e crescente cooperação entre os serviços privados e estatais de vigilância eletrônico-digital em escala planetária.

Segundo veiculado na imprensa,[15] antes de Manning "vazar" os documentos, ele teria feito contato, via e-mail, com Adrian Lamo, um conhecido ex-hacker,[16] para obter orientação para quem transmitir os materiais "sensíveis". Como analista militar de informações de segurança, Manning tinha acesso facilitado a um sistema integrado de informações sigilosas do exército e da diplomacia norte-americana. Segundo os relatos, Lamo não seria mais um hacker independente (as razões apresentadas são diversas) e estaria trabalhando como analista colaborador de uma empresa de segurança cibernética, que prestaria serviços diversos tanto no mercado privado como para agências governamentais.

Naquele momento, conforme noticiado em diversas revistas (*Forbes, Wired e Salon*[17]), o executivo Chet Urbe[18] se apresentou publicamente como o responsável por colocar Adrian Lamo em contato com os órgãos governamentais que efetuaram a prisão de Manning. Sua empresa – Project Vigilant –, na qual Lamo seria um "analista voluntário", foi então descrita como uma importante, discreta e bem-sucedida empresa de vigilância cibernética, capaz de monitorar e produzir perfis de indivíduos através do rastreamento e tratamento de informações disponíveis na rede. Conforme o relato da *Forbes*:

> According to Uber, one of Project Vigilant's manifold methods for gathering intelligence includes collecting information from a dozen regional U.S. Internet service providers (ISPs). Uber declined to name those ISPs, but said that because the companies included a provision allowing them to share users' Internet activities with third parties in their end

13. No momento, diversas organizações de defesa dos direitos humanos apóiam a defesa de Manning e questionam o governo dos EUA sobre as condições de sua detenção. Veja: http://www.bradleymanning.org/. Acesso em: 31/05/2011.

14. O texto citado é parte da entrevista concedida por Julian Assange ao repórter Martin Smith, para um documentário produzido pela PBS Frontline. A entrevista foi gravada em 4 de abril de 2011. Um arquivo bruto da entrevista está disponível em: http://wikileaks.midiaindependente.org/WikiSecrets-Julian-Assange-Full.html. Acesso em: 31/5/2011.

15. *Wired: Update: Ex-Hacker Denies Alleged WikiLeaker Gave Him Classified Documents*: http://www.wired.com/threatlevel/2010/08/lamo-classified-documents/. Acesso em: 31/5/2011.

16. Compartilho da distinção entre *hacker* e *cracker* proposta por Pekka Himanen (2001). O discurso midiático frequentemente mistura as duas coisas, criando uma confusão semântica sobre a caracterização política dos hackers. Sinteticamente, pode-se dizer que o cracker é aquele que faz uso dos seus conhecimentos informáticos para cometer delitos, enquanto o termo "hacker" refere-se àqueles com habilidades técnicas e disposição curiosa para a busca do livre conhecimento.

17. Reportagem da *Forbes: Stealthy Government Contractor Monitors U.S. Internet Providers*, Worked With Wikileaks Informant: http://blogs.forbes.com/firewall/2010/08/01/stealthy-government-contractor-monitors-u-s-internet-providers-says-it-employed-wikileaks-informant/ . Reportagem da *Wired: Update: Ex-Hacker Denies Alleged WikiLeaker Gave Him Classified Documents*: http://www.wired.com/threatlevel/2010/08/lamo-classified-documents/ . Reportagem da *Salon: Re-visiting Project Vigilant*: http://www.salon.com/news/opinion/glenn_greenwald/2010/08/05/surveillance/index.html. Acesso em: 31/5/2011.

18. Segundo reportagem de Mark Albertson, especialista em tecnologia da revista *The Examer*, Chet Uber é diretor do Projeto Vigilante e fundador da InfraGard (uma parceria entre o FBI e o setor privado) Fonte: *Big names help run Project Vigilant*, disponível em: http://www.examiner.com/technology-in-san-francisco/big-names-help-run-project-vigilant. Acesso em: 31/5/2011.

> user license agreements (EULAs), Vigilant was able to legally gather data from those Internet carriers and use it to craft reports for federal agencies. A Vigilant press release says that the organization tracks more than 250 million IP addresses a day and can "develop portfolios on any name, screen name or IP address".[19]

Glenn Greenwald escreveu dois bons artigos sobre o caso para a revista *Salon*.[20] No primeiro, ele descreve com relativa surpresa a enorme abrangência do Projeto Vigilante. Porém, alertado por alguns leitores, ele escreve um segundo artigo no qual interroga a capacidade atribuída a esta empresa, afirmando que os relatos veiculados na mídia a partir das entrevistas de Chet Urbe poderiam ter sido exagerados para funcionar, indiretamente, como uma campanha de promoção de sua própria empresa.

Independentemente da efetiva magnitude do Projeto Vigilante, tal situação chamou a atenção para um conjunto de empresas e programas governamentais com atuação semelhante. O primeiro artigo de Greenwald faz referência a um interessante relatório produzido pela American Civil Liberties Union (Aclu) em 2004, sobre a emergência do que eles denominam "Complexo Industrial de Vigilância" – Surveillance Industrial Complex. Uma das principais contribuições deste relatório é indicar as infinitas possibilidades de controle social que estão virtualmente inscritas nas tecnologias de comunicação digital quando submetidas a filtragem, retenção e análise das informações transacionadas nas redes digitais. Para esta organização (Aclu), o atual contexto tecnológico coloca novas ameaças às liberdades civis, uma vez que as condições jurídicas de intrusão do Estado, graças às alterações nas legislações após o 11 de setembro de 2011, criaram condições facilitadas de intervenção estatal sobre áreas da vida civil antes consideradas intocáveis.

O relatório da Aclu descreve detalhadamente um conjunto de programas governamentais e iniciativas corporativas que tem contribuído para criar um cenário de vigilância permanente sobre toda comunicação eletrônico-digital.[21] Outro ponto importante deste relatório é a descrição da expansão dos serviços privados que comercializam dados pessoais coletados a partir das pegadas digitais (*digital footprints*) produzidas por qualquer internauta. Em seguida, o relatório indica como essas empresas podem cooperar com os

Il.2 Imagem da página inicial do site da empresa *Project Vigilant*

19. Reportagem da *Forbes: Stealthy Government Contractor Monitors U.S. Internet Providers*, Worked With Wikileaks Informant: http://blogs.forbes.com/firewall/2010/08/01/stealthy-government-contractor-monitors-u-s-internet-providers-says-it-employed-wikileaks-informant/. Acesso em: 31/5/2011.

20. Gleen Greenwald, *Revista Salon*, (a) *Project Vigilant and the government/corporate destruction of privacy*: http://www.salon.com/news/opinion/glenn_greenwald/2010/08/02/privacy. (b) Re-visiting Project Vigilant: http://www.salon.com/news/opinion/glenn_greenwald/2010/08/05/surveillance/index.html. Acesso em: 31/5/2011.

21. O relatório *The surveillance-industrial complex: How the american government is conscripting businesses and individuals int the construction fo a surveillance Society*, produzido pela Aclu – American Civil Liberties Union, 2004, está disponível em: http://www.aclu.org/FilesPDFs/surveillance_report.pdf

serviços de segurança norte-americano, dando forma a uma complexa relação corporativo-governamental.

A "tese" do relatório é que tal articulação indica um processo de "terceirização" dos serviços de segurança estatal que, além de objetivar a redução de custos operacionais, estaria estrategicamente buscando um ambiente jurídico mais flexível à retenção e ao tratamento de dados pessoais, uma vez que as empresas privadas que atuam nas diversas "camadas"[22] do ciberespaço poderiam registrar e tratar um grande volume de informações em condições menos restritivas que o governo dos EUA. Ademais, graças ao comercio eletrônico e à crescente concentração de alguns serviços e sites corporativos na internet, o volume de informações pessoais transacionados com as empresas é consideravelmente maior do que com o Estado. Após "terceirizar" essa tarefa, os governos podem solicitar, sob determinadas condições, o acesso privilegiado a essas informações mantidas pelas empresas privadas. São exatamente essas "condições" que, em diferentes países, constituem atualmente um importante campo de batalha política e jurídica. Tal disputa dá-se, por exemplo, em torno das definições e regulamentações dos direitos de privacidade, direito à proteção de dados pessoais, nas tipificações sobre cibercrime, entre outros.[23]

É difícil confirmar a hipótese de uma "terceirização" deliberada, pois isso implicaria estabelecer relações diretas (causal e intencional) entre as ações e objetivos do Estado e das corporações. Em algumas circunstâncias, seus objetivos podem coincidir, mas em outras não. Podemos, ainda assim, aceitar a hipótese da "terceirização" da segurança cibernética e observar as evidências a partir da análise de um conjunto de casos empíricos (a verificação desta hipótese seria, por si só, um interessante projeto de pesquisa). Em se tratando do registro das informações (*logs*) de acesso e navegação de um internauta, a depender do ramo de atuação da empresa, se tal obrigação fosse imposta pelo Estado poderia significar custos financeiros elevados para a implementação das tecnologias de registro e armazenamento (se ela for, por exemplo, uma ISP – Internet Service Provider). Por outro lado, ter o direito e a proteção legal para registrar, tratar e comercializar informações pessoais de usuários da internet pode ser de especial interesse para empresas que lucram com a produção de perfis de consumidores. Portanto, a possibilidade de estabelecer relações entre um perfil on-line (internauta e seus avatares) e um perfil off-line (indivíduo de carne e osso) pode servir tanto a interesses de controle social (Estado) como para objetivos de ganhos monetários (empresas privadas).

Diante das múltiplas possibilidades de registro inauguradas pela análise dos dados trafegados nas redes cibernéticas, as iniciativas descritas são reveladoras dos atuais mecanismos de controle que surgem como o "outro lado da moeda" do livre uso das redes digitais de comunicação. Como bem analisado por alguns autores,[24] a ausência de uma regulação jurídica adequada para proteger a "neutralidade da rede"[25] e prevenir abusos na utilização dos controles embutidos nessas tecnologias deixará nas mãos das empresas que gerenciam o acesso e o tráfego na internet um poder que pode ameaçar os direitos cidadãos na era digital.

Neste sentido, fazendo uma analogia com os conceitos elaborados pelo filósofo Jacques Rancière, poderíamos dizer que as tecnologias digitais inauguram um novo campo político ao criar uma nova *partilha do sensível* (2005): elas redefinem os espaços da interação social; modificam o regime de visibilidade (quando definem o que pode ser tornado visível, por exemplo, através do rastro digital); transformam as possibilidades discursivas (diversificação e multiplicação dos "falantes"), dando lugar a novas lutas pelas formas de apropriação e distribuição dos recursos materiais e simbólicos que vão definir as relações de poder sobre as relações sociais mediadas pelas tecnologias digitais. Neste caso, as disputas pelo *partilha do sensível* dão forma simultaneamente à ciberpolítica e à tecnopolítica.

Heath Bunting: arte hacker e resistência política

Quase como um contraexemplo do que afirmamos até agora, o trabalho do artista Heath Bunting pode ser interpretado como um exercício de resistência criativa através da produção de situações de "des-

22. Referimo-nos aqui às diversas mediações físicas, lógicas e jurídicas que dão forma ao ciberespaço. Temos, por exemplo, a camada física da infraestrutura de cabos e satélites por onde flui a informação. Atualmente, a propriedade da maior parte desta estrutura está nas mãos de algumas poucas empresas. O provimento de acesso à rede (Internet Service Provider – ISP) é outra "camada" importante com poder de filtragem e registro (logs de acesso) dos seus clientes.

23. Na Europa, um bom exemplo disso é a Directive 2006/24/EC, que trata da condições de proteção e retenção de dados pessoais (Directive,2006), e a Convenção de Budapeste sobre Cibercrimes (2001). No Brasil, o Ministério de Justiça realizou (concluída em abril 2011) uma consulta pública on-line sobre uma proposta de lei que regulará as condições de "proteção de dados pessoais". O projeto de lei está disponível para consulta no link: http://www.culturadigital.br/dadospessoais.

24. Lawrence Lessig interpretou este problema com a máxima "o código é a lei". Ou seja, na ausência da lei, será o domínio sobre o código informático que vai prescrever o que pode ou não ser realizado (2006).

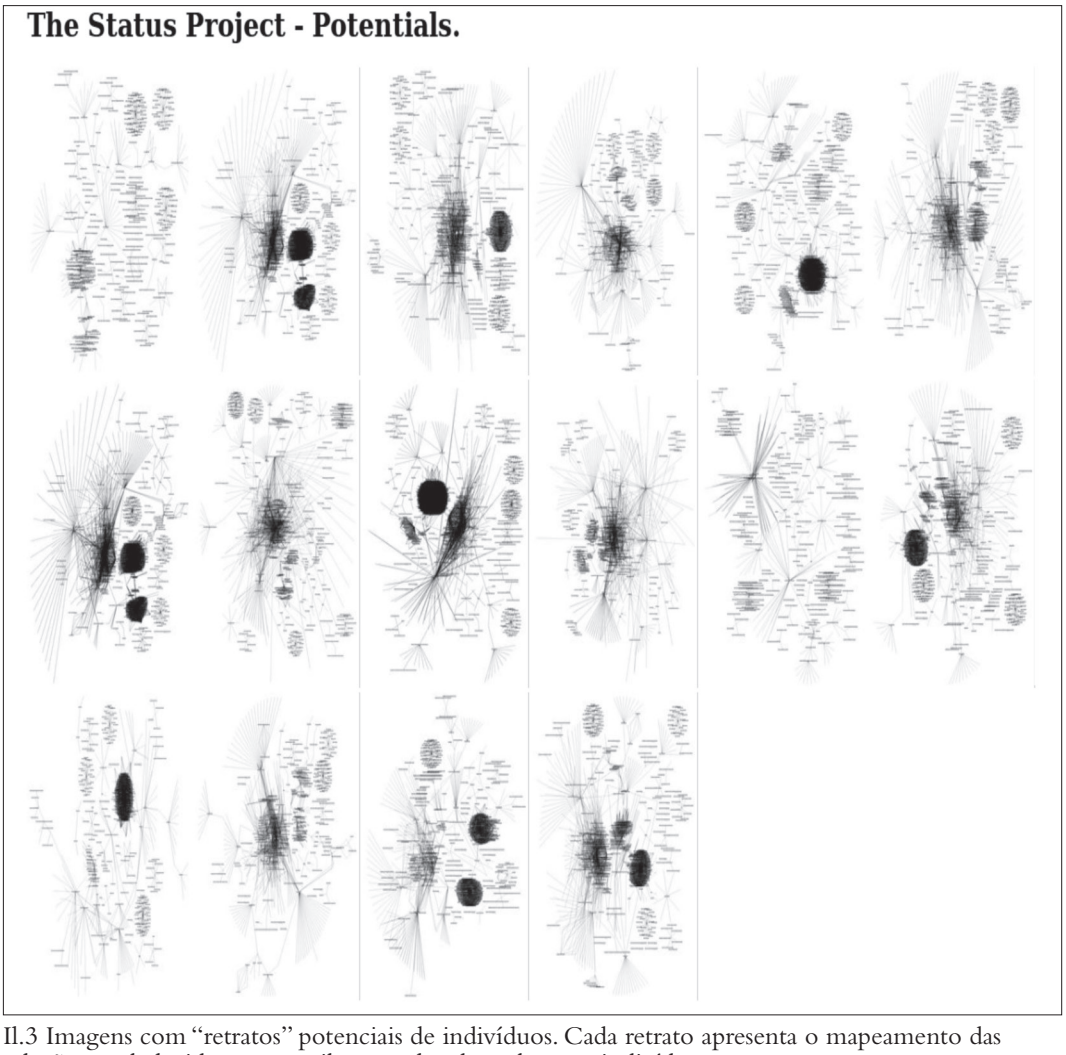
25. O conceito de "neutralidade da rede" é bem explicado por Carlos Afonso (2007).

controle" no uso das redes digitais. Sua produção artística ajuda a tornar visíveis os mecanismos sociais e tecnológicos de "classificação": o conjunto das informações registradas pelo uso cotidiano dos dispositivos de comunicação em redes digitais é ampliado pela integração de banco de dados informatizados (registros de bibliotecas, dados de compras eletrônicas, cadastros de lojas etc); em seguida, combina-se às categorias (sociais) e aos algoritmos (computacionais) na produção de "perfis" atuais e virtuais (presente e potencial) sobre indivíduos naturais (sujeitos biológicos) e indivíduos artificiais (avatares ou perfis estatísticos).

Neste caso, interessa-nos observar como se relaciona a seleção/produção dos indicadores (neste caso as categorias sociais) com a análise dos padrões virtuais (potenciais) emergentes de um comportamento considerado desviante. O artista em questão, ao identificar o funcionamento desses mecanismos, passa a produzir "identidades" que vão jogar com o sistema de controle. De maneira resumida, Heath Bunting faz uso de inúmeras fontes de dados informáticos pessoais para produzir representações (mapas visuais) nas quais ele apresenta graficamente os padrões de relacionamento entre as informações disponíveis sobre um sujeito, dando forma a um perfil.

O trabalho ganha maior interesse na medida em que ele explora diferentes mecanismos de produção desses perfis a partir de fontes diversas. No momento que ele "aprende" como um perfil específico é construído (que conjunto de relações perfaz uma identidade?), passa a criar novas "identidades" através da programação de softwares específicos. Por exemplo, que tipo de rastro digital ou de modos de relação entre informações pessoais perfaz o perfil de um terrorista em potencial?

Numa entrevista concedida a Marc Garrett, o artista afirma que está interessado em pesquisar o modo como a sociedade inglesa produz e administra, do ponto de vista dos dados informáticos gerados, as fronteiras entre um ser humano, uma pessoa física (indivíduo civil) e uma pessoa jurídica (empresa ou instituição), portanto, entre seres naturais e artificiais. Para isso, Heath Bunting retoma, de certa maneira, o conceito de "data body" (corpo de dados), desenvolvido há mais de dez anos pelo coletivo Critical Art Ensemble:



Il.3 Imagens com "retratos" potenciais de indivíduos. Cada retrato apresenta o mapeamento das relações estabelecidas entre atributos coletados sobre um indivíduo

> The total collection of records on an individual is his or her data body – a state-and-corporate-controlled doppelganger. What is most unfortunate about this development is that the data body not only claims to have ontological privilege, but actually has it. What your data body says about you is more real than what you say about yourself. The data body is the body by which you are judged in society, and the body which dictates your status in the world. What we are witnessing at this point in time is the triumph of representation over being. The electronic file has conquered self-aware consciousness. (CAE, 1995, apud Bunting, 2010)

Talvez, diversamente do que afirmam os artistas do CAE, ao invés do "triunfo da representação sobre o ser", estejamos atualmente diante do triunfo da simulação informacional, uma vez que este corpo de dados não mais precisa fazer referência a uma entidade física anterior. O importante para Bunting é tomar consciência e lutar pela apropriação deste processo de produção e gerenciamento do sistema de classificação. As "identidades" criadas pelo artista expressam as diferentes possibilidades de "ser" como formas de apresentação no interior da sociedade.

Bunting chega a produzir, fazendo uso dos próprios mecanismos de indexação disponíveis na sociedade (cartões de fidelização, registros de compras etc), identidades artificiais que, pelo acúmulo de informações e relações com outras entidades informacionais, adquirem "vida" e passam a "existir" como pessoas físicas. Esses "perfis", agora naturais, são em seguida vendidos em seu website com o "kit identitário" (o conjunto de documentos, bilhetes, cartões eletrônicos etc) que dá existência "real" a este indivíduo na sociedade.

Il 4. Conjunto de documentos que compõe uma "identidade"

Trata-se, neste caso, de um bom exemplo artístico do espírito hacker descrito por Mckenzie Wark: a capacidade de fazer novas coisas "entrarem" no mundo!

Ativismo hacker: quando novos sujeitos entram em cena

A partir de 2007, o Ministério da Cultura do Brasil iniciou um amplo debate sobre a reforma da Lei de Direitos Autorais (9.610/1998). Convencido da necessidade de buscar uma nova regulamentação para enfrentar as transformações inauguradas pelas tecnologias digitais, o MinC organizou um conjunto de atividades para debater a reforma, culminando com a criação em 2010 de uma plataforma on-line colaborativa, na qual uma primeira versão do projeto de lei foi submetida à consulta pública.

Este sistema, desenvolvido em software livre por opção do próprio MinC, permitia que qualquer usuário fizesse comentários diretamente a cada um dos itens do PL. Nesta configuração, o mesmo usuário (ou a mesma máquina utilizada pela mesma pessoa ou por pessoas diferentes) poderia contribuir mais de uma vez. Para fazer as sugestões diretamente na plataforma, era solicitado apenas que o indivíduo ou instituição (pessoas jurídicas também podiam fazer contribuições) se identificassem voluntariamente. Como não havia um mecanismo de certificação para garantir a veracidade das identidades, o sistema permitiu alguns "abusos". Aparentemente, tal possibilidade não preocupou os organizadores da consulta. O sistema, no entanto, registrou os números IP (Internet Protocol) de cada computador que fez contribuições no site. Ao final do processo (agosto de 2010), todas as contribuições realizadas na plataforma e as informações de identificação dos participantes ficaram disponíveis para download.

Logo após o fechamento da consulta pública on-line, uma comunidade de ciberativistas[26] analisou os dados disponibilizados pelo sistema e chegou a conclusões interessantes que foram publicadas num relatório.[27] Porém, somente alguns meses mais tarde seus "achados" ganhariam um novo fôlego político.

Neste ano, com o início do governo Dilma Rousseff, o Ministério da Cultura passou a uma nova administração (com a ministra Ana de Hollanda). Iniciou-se, então, uma outra batalha política, dado que uma nova composição de forças sociais disputava os rumos dos reforma da Lei de Direitos Autorais. Num dado momento, quando pressionada a retomar

26. Comunidade Transparência Hacker: http://thacker.com.br

27. Observatório da Consulta Pública da Revisão da Lei de Direito Autoral, disponível em: http://consultalda.thacker.com.br/. Acesso em: 15/6/2011.

os resultados daquele processo de consulta on-line realizado no ano anterior, a ministra afirmou que aquela consulta indicava, com base nos dados, que 70% das contribuições realizadas diziam "não concordar" com a mudança da lei (Ortellado & Souza, 2011).

Respondendo a essa manifestação da ministra, os pesquisadores Pablo Ortellado e Allan Rocha de Souza retomam o relatório produzido pela Transparência Hacker para qualificar os tais 70%. A ação desta comunidade de ciberativistas permitiu dar maior visibilidade a alguns dados que passam frequentemente despercebidos para a maioria dos usuários da internet. Ao trabalhar com os números IP registrados pelo software da consulta on-line, foi possível dar outra complexidade aos dados quantitativos e interrogar o argumento de representatividade numérica daqueles 70%. Para sintetizar, a análise dos pesquisadores revelou que:

> Basta selecionar os cinco maiores participantes individuais e chegamos a incríveis 652 contribuições, 644 discordando da proposta e apenas 8 concordando, sendo responsáveis por 8,29 % das 7.863 contribuições feitas diretamente na plataforma. E, ainda mais interessante, certas frases eram repetidas ao infinito por estas pessoas. [...] Uma análise inicial quantitativa indica 339 (4,31%) aportes diretamente dos computadores do ECAD, realizados por 70 pessoas diferentes. A Abramus, associação líder no ECAD, por sua vez, contribuiu 231 vezes (2,94%). A Abramus discordou sempre, enquanto o ECAD em 98,52% das vezes. Somando apenas estes dois grupos, que não se sobrepõem, chegamos a 15,54% das contribuições. Tudo indica que o ECAD mobilizou dezenas de pessoas – talvez funcionários – para atacar diretamente a reforma. (Ortellado & Souza, 2011)

Este episódio é exemplar da maneira como a ciberpolítica, como prática de atuação política através das tecnologias de comunicação digital, articula-se à tecnopolítica, como configuração social e política dos dispositivos técnicos. Neste caso, o conhecimento das características da comunicação cibernética permitiu que um novo grupo social modificasse o campo sob disputa, ao introduzir na cena política uma nova "contabilidade". Finalmente, como os próprios ativistas escrevem, a utilização de tecnologias livres pelo MinC foi também uma importante decisão que reflete a não neutralidade dos dispositivos tecnológicos:

> Foi justamente essa escolha política, traduzida na interface, que deu espaço para uma ação articulada de um grupo de interesse contrário à reforma. Esse grupo se impõe não com o intuito de debater mas sim gerar volume, produzindo uma falsa sensação de representatividade. [...] Cabe também esclarecer que, na nossa avaliação, a realização da consulta em uma ferramenta baseada em software livre fortalece a transparência do processo, porque permite a todos nós, "cidadãos curiosos", vivenciar a democracia em múltiplas e complexas camadas, gerando apropriações dos códigos binários e legislativos. (Thacker, 2010)

Conclusão

Nos exemplos descritos, destacamos algumas especificidades sociotécnicas que caracterizam as tecnologias digitais de comunicação, procurando indicar como elas participam das novas práticas política, de controle e de resistência. Neste percurso, problematizamos como essas características, em especial, a rastreabilidade, são reguladoras da fronteira entre o visível e o invisível, portanto, como elas estabelecem, criam ou ocultam a "existência" de novos sujeitos políticos. Em suma, a própria configuração tecnológica constitui um campo de batalha que define o desenho (quem são os sujeitos, quais são suas relações, quais as possibilidades de relação entre eles etc.) da esfera política.

Nesse sentido, tanto a tecnopolítica como a ciberpolítica indicam a importância das condições sociais, econômicas e culturais de comunicação para a distribuição do poder numa sociedade em que as relações sociais cibermediadas avançam cotidianamente sobre novos territórios da vida. Sinteticamente, dentre os diversos fatores que participam dessa dinâmica, o artigo destacou os seguintes, que indicam possíveis caminhos para recortes específicos de pesquisa:

1. Posições desiguais dos atores no interior de uma rede cibernética. Quais as condições de acesso, gestão e monitoramento das informações transacionadas na rede? Os sujeitos e grupos sociais gozam de posições muito diversas no que diz respeito ao controle sobre aspectos técnicos da internet. Aqui, o regime de propriedade e o desenho institucional da gestão e operação da rede têm um peso importante nas condições políticas de comunicação. Por exemplo, as empresas provedoras de acesso à internet (ISP) ou as empresas de telecomunicações proprietárias da infraestrutura física das redes estão em situação privilegiada com relação aos usuários. Como evitar que elas tomem ações arbitrárias que ameacem os direitos dos cidadãos?

2. Condições de privacidade, anonimato e retenção de dados pessoais ganham novos contornos com a convergência digital. Qual o impacto das escolhas tecnológicas em termos das possibilidades de vigilância e controle? Quem tem acesso? Quem armazena, quem pode tratar e comercializar essas informações? Para quais fins e sob que condições?

3. Tensões entre a transparência e a opacidade na atuação política através das tecnologias digitais. Como equilibrar as condições de visibilidade política

com as novas possibilidades de controle? Privacidade para os cidadãos e transparência para os governos e empresas poderosas? Como equilibrar o desejo de onisciência (vontade infinita de saber) com os riscos do registro total de uma tecnologia que nunca esquece? Tecnocracia *versus* tecnocidadãos?

4. Participação voluntária e disponibilização gratuita dos dados pessoais. Cada vez mais os internautas convivem em ambientes e plataformas corporativas que funcionam como ilhas fortificadas no interior da internet (Berners-Lee, 2010). Os usuários percebem benefícios imediatos na participação em redes sociais corporativas (Facebook, Orkut etc.), ao mesmo tempo, formas de controle são "contrabandeadas" por esta adesão voluntária. Se, por um lado, observamos novas formas de ação social e política através da internet, não estaríamos também diante de novas formas de "servidão voluntária"? Como equacionar e reconhecer novas formas de dominação e exploração econômica a partir de um poder que se exerce docemente através da nossa adesão voluntária a estes dispositivos? Na realidade, como redefinir esses termos?

Na medida em que adentramos um universo cada vez mais mediado pelas tecnologias de informação e comunicação, o conhecimento sobre suas configurações sociotécnicas faz-se fundamental para que possamos compreender seus impactos sociais, econômicos e políticos. Nos termos de Galloway, o "protocolo" como padrão tecnológico que materializa práticas de dominação é, para as sociedades contemporâneas, o equivalente do dispositivo panóptico para as sociedades disciplinares (2004, p.13). Andrew Feenberg, na perspectiva mais ampla de suas análises sociológicas sobre o desenvolvimento tecnológico (e não apenas digital), apresenta o problema nos seguintes termos:

> as formas modernas de opressão não estão tão baseadas em falsas ideologias quanto em técnicas efetivas "codificadas' pela hegemonia dominante para reproduzir o sistema. Enquanto a escolha permanece escondida, a imagem determinística de uma ordem social justificada tecnicamente se projeta. A efetividade legitimadora da tecnologia depende da inconsciência do horizonte político-cultural em que ela foi concebida. (2001)

Para concluir, cabe perguntar: quais são os horizontes políticos e culturais sob disputa dentro dos quais as tecnologias de comunicação estão sendo desenvolvidas e implementadas?

Referências

AFONSO, Carlos A. *Todos os datagramas são iguais perante a rede!*. 2007. Disponível em: <http://www.cgi.br/publicacoes/artigos/artigo43.htm>. Acesso em: 19/6/2008.

BERNERS-LEE, Tim. Long live the Web: a call for continued open standards and neutrality. *Scientific American*, November, 2010. Disponível em: http://www.scientificamerican.com/article.cfm?id=long-live-the-web. Acesso em: 15/6/2011.

BUNTING, Heath. The status projetc: data mining our identities. Entrevista com Marc Garrett, *Furtherfield*, 2010. Disponivel em http://www.furtherfield.org/interviews/status-project-data-mining-our-identities. Acesso em: 31/05/2011.

CASTELLS, Manuel. *A galáxia da internet:* reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar, 2003.

CONVENÇÃO de Budapeste sobre Cibercrime, 2001. Disponível em: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm. Acesso em: 31/5/2011.

CRITICAL ART ENSEMBLE (CAE). The mythology of terrorism on the net. Summer 95. Disponível em: http://www.t0.or.at/cae/mnterror.htm. Acesso em: 31/5/2011.

DIRECTIVE 2006/24/EC of the European Parliament and of the Council. *Official Journal of the European Union*, Apr. 2006. Disponível em: <http://www.ispai.ie/DR%20as%20published%20OJ%2013-04-06.pdf>. Acesso em: 11/7/2007.

FEENBERG, Andrew. Racionalização subversiva: tecnologia, poder e democracia. *Cibercultura On-line*, v. 4, 2001. Disponível em: http://members.fortunecity.com/cibercultura/vol4/racsub.html. Acesso em: 31/5/2011.

GALLOWAY, Alexander. *Protocol:* how control exists after decentralization. Cambridge: MIT Press, 2004.

HIMANEN, Pekka. *The hacker ethic and the spirit of the information age*. New York: Random House, 2001.

LESSIG, Lawrence. *Code v. 2.0*, New York: Basic Books, 2006. (versão atualizado de Code and Other Laws of Cyberspace, de 1999). Disponível em: http://codev2.cc/download+remix/Lessig-Codev2.pdf. Acesso em: 31/5/2011.

ORTELLADO, Pablo & SOUZA, Allan Rocha. Neste carnaval, MinC veste a fantasia errada!, 2011. Disponível em: http://www.gpopai.org/ortellado/2011/03/neste-carnaval-minc-veste-a-fantasia-errada/ Acesso em: 31/5/2011.

PARRA, Henrique, Z. M. *O Leviatã e a rede:* mutações e persistências político-estéticas. Tese (Doutorado) – Unicamp, Campinas, 2009.

RANCIÈRE, Jacques. *A partilha do sensível:* estética e política. Tradução de Mônica Costa Netto. São Paulo: Editora 34/EXO, 2005.

SILVEIRA, Sergio Amadeu. Novas dimensões da política:

protocolos e códigos na esfera pública interconectada. *Revista Sociologia Política*, Curitiba, v. 17, nº 34, p. 103-113, out. 2009 .

_____. Redes cibernéticas e tecnologias do anonimato. *Comunicação & Sociedade*, ano 30, nº 51, p. 113-134, jan./jun. 2009-A.

THACKER (Transparência Hacker). Uma leitura dos dados gerados pela consulta pública da nova Lei de Direitos Autorais, 2010. Disponível em: http://consultalda.thacker.com.br/2010/08/31/uma-leitura-dos-dados-gerados-pela-consulta-publica-da-nova-lei-de-direitos-autorais/. Acesso em: 15/6/2011.

TRIVINHO, Eugênio. *O mal-estar da teoria:* a condição da crítica na sociedade tecnológica atual. Rio de Janeiro: Quartet, 2001.

WARK, McKenzie. *A hacker manifesto*. Subsol. 2004. Disponível em: <http://subsol.c3.hu/subsol_2/contributors0/warktext.html>. Acesso em: 11/3/2009.

Social control and hacker practice: technopolitics and cyberpolitics in digital networks

Abstract

By examining a few specific cases, concerning the possibilities of control and access to information on digital networks, we will discuss how these conditions shape up the politics in cyberculture. This is simultaneously understood as the conflict over the socio-technical configuration of digital technologies (technopolitics) and the dynamics of cybernetically mediated politics (cyberpolitics). By articulating these two dimensions, we will analyze how the configuration and appropriation modes of these devices will define what enters or does not enter the field of the visible and of the enunciable, therefore, the field of public regulation and control, creating new territories of rights, resistance, social conflicts and economic exploitation.

Key words: technopolitics, cyberpolitics, cyberculture, control, protocol.

Control social y práctica hacker: tecnopolítica y ciberpolítica en redes digitales

Resumen

A través del análisis de algunos casos concretos, relativos a las posibilidades de control y acceso a la información en las redes digitales, se discute cómo estas situaciones dan forma a la política en la cibercultura. Se trata de pensar en la política, simultáneamente, como el conflicto por las configuraciones sociotécnicas de las tecnologías digitales (tecnopolítica) y las dinámicas de la política cibernéticamente mediada (ciberpolítica). Mediante la articulación de estas dos dimensiones se analizan cómo la constitución y los modos de apropriación de estos dispositivos pueden definir lo que entra o no en el campo del visible y enunciable, por lo tanto, el campo de la regulación pública y control, formando nuevos territorios de derechos, de resistencia, de conflictos sociales y de explotación económica.

Palabras-clave: tecnopolítica, ciberpolítica, cibercultura, control, protocolo.

Data de recebimento do artigo: 25/10/2011
Data de aprovação do artigo: 29/01/2012