Ecopolítica. Governamentalidade planetária, novas institucionalizações e resistências na sociedade de controle.

Internet

Em 1978, o ex-engenheiro de telecomunicações da CIA, David L. Watters, afirmou que a *National Security Agency* (NSA – Agência de Segurança Nacional) gravava milhões de conversas telefônicas nos Estados Unidos e outros países. Diante disso, o então presidente estadunidense James Carter estabeleceu o *Foreign Intelligence Surveillance Act* (FISA)[1] que autorizava as escutas que fossem aceitas pelo governo enquanto uma medida para garantir a segurança nacional.

Nesse período a internet ainda estava em desenvolvimento e era utilizada por militares e pesquisadores de algumas universidades. Na década de 1980, com a abertura da rede, novos atos foram promulgados, como o *Electronic Communications Privacy Act* (ECPA) de 1986[2] que expandiu as mesmas leis telefônicas para a internet, até então não era necessária autorização para grampear trocas de e-mails.

O ECPA é uma atualização do *Federal Wiretap Act* de 1968 que abordava o recolhimento de informações via telefone. E naquele momento, com o ECPA, as comunicações digitais também poderiam ser grampeadas.

Esses atos entre a década de 1960 e 1980 são importantes tanto por terem passado por algumas atualizações como por terem dado suporte para a promulgação de outros atos. É a partir desses, também, que se desdobraram recentes programas de monitoramento de informações em escala planetária pelo governo dos Estados Unidos.

Em outubro de 1994, foi promulgado o *The digital Telephony Act* (CALEA) que estava em discussão no congresso estadunidense desde 1992. O projeto só ganhou força para ser aprovado quando o Louis Freeh, então diretor do FBI, o definiu como uma de suas prioridades.

O CALEA tinha como alvo a rede de circuitos e pretendia financiar a fabricação de fibras óticas que facilitassem a instalação de escutas telefônicas autorizadas pelo

[1] É possível ler a transcrição da audiência do FISA em: U.S. Hearing FISA. Whashigton: U.S. Government Printing Office, 1978. http://www.intelligence.senate.gov/pdfs/s1566.pdf (acesso em 05/03/2015).

[2] U.S. ECPA. 1986. Disponível em: http://www.justice.gov/sites/default/files/jmd/legacy/2013/09/06/act-pl99-508.pdf (acesso em 05/03/2015).

governo. O projeto investiu 500 milhões de dólares na troca dos cabos das operadoras telefônicas. Tal financiamento foi aprovado em 1996 e o CALEA regulamentado pela *Federal Comunication Comission* em 1999.

Louis Freeh, o diretor do FBI, apesar de não ter solicitado que o CALEA fosse complementado com regulamentações a respeito de criptografia, já pretendia solicitar legislação adicional. Mesmo a discussão aparecendo legalmente somente neste momento, documentos publicizados em 1996 mostraram que em 1991 o governo Bush entendia a telefonia digital como um dos pontos principais de pesquisa para explorar a criptografia.[3]

Assim, com a aprovação do CALEA os fabricantes de redes de circuito de informação foram obrigados a adaptarem seus equipamentos com uma *backdooor*[4], uma porta dos fundos, para que a comunicação possa ser grampeada com maior facilidade (SILVEIRA, 24/03/2014).

Posteriormente, em 26 de outubro de 2001, foi promulgado o *Patriot Act*[5]. Esse foi um dos efeitos dos ataques de 11 de setembro daquele ano e suspendeu uma série de restrições que se tinha para a realização das escutas e de quebra de e-mails[6].

No Título II do documento (*Enhanced Surveillance Procedures*) aué autorizado aos EUA interceptar comunicações orais ou eletrônicas suspeitas de terrorismo ou de fraudes de computador. Entetanto, para isso ocorrer seria necessária uma ordem judicial do governo dos EUA (U.S., 2001).

Já no Título V (*Removing obstacles to investing terrorism*) as NSL (*National Security Letters*) que até então só podam ser utilizadas para a investigação sobre terrorismo, agora estavam autorizadas para qualquer outra investigação.

---

[3] Esses documentos foram divulgados pela *Electronic Privacy Center*. Disponível em: http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/epic-foia-images/scowcroft-memo.html (acesso em 02/03/2015).

[4] *Backdoor* é um recurso utilizado por sites e softwares para que se tenha o acesso remoto ao sistema ou à rede. Pode-se tanto ter acesso aos dados do computador, por exemplo, como também possibilita a recuperação de informações. Hackers também fazer uso do *backdoor* para a instalação de softwares ou para o acesso aos dados. Fonte: WIKIPEDIA. *Backdoor*. Disponível em: http://pt.wikipedia.org/wiki/Backdoor (acesso em 04/03/2015).

[5] U.S. Patriot Act. 26/10/2001. Disponível em: http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf (acesso em 02/03/2015).

[6] Em 2011, Julian Assange solicitou para Eric Schmidt, presidente da Google, vazar para o Wikileaks os pedidos de informação que o governo dos EUA tinha feito a partir do Patriot Act. Schmidt apenas afirmou que é ilegal revelar essas solicitações (ASSANGE, 2015, p. 30).

As NSL dão ao FBI (*Federal Bureau Investigation*) o poder de coletar informações confidenciais de empresas ou órgãos de governo. Por meio delas não há a necessidade de qualquer autorização judicial, qualquer explicação ou justificativa. E a empresa ou órgão que entrega a informação deve permanecer em sigilo, não podendo nem divulgar o recebimento da carta (SILVEIRA, 24/03/2014). Portanto, legalmente não há restrição para o governo dos EUA monitorar informações de qualquer pessoa no planeta, basta essa ser suspeita de estar cometendo algo contra o país.

Ainda nesse título V, o FISA de 1978 foi atualizado e as escutas poderiam ser instaladas também em casos de suspeita de terrorismo (GREENWALD, 19/06/2013).

Em 2005, o CALEA foi atualizado e direcionado para as redes de pacotes de dados e seus protocolos (IP, VOIP, Internet), nesse momento passou a ser necessário a *backdoor* nos softwares. Portanto, o CALEA passa a obrigar as empresas de softwares e de telefonia a deixarem um acesso para os possíveis grampos. [7]

A aliança do CALEA com o *Patriot Act* intensificou os monitoramentos. Em 2008, o congresso aprovou novas modificações no FISA e que possibilitava os grampos sem a necessidade de mandado da NSA (GREENWALD, 19/06/2013).

Em 2006, Nigel Gilbert, professor na Universidade de Surrey, foi chefe de um estudo sobre monitoramento da Royal Academy. O estudo mostrou que dali 5 anos, ou seja, em 2011, a Google teria informações suficientes para rastrear os movimentos e intenções exatos de cada indivíduo por conta de seus inúmeros aplicativos (Google Earth, Google Calendar)[8]. O estudo de Gilbert é interessante por também sinalizar para a aliança que se fortaleceria alguns anos depois entre as empresas de comunicação e governos.

No ano de 2009, o governo dos EUA fundou um setor nas Forças Armadas para proteger seus dados, era o *Cyber Command* (USCYBERCOM). O almirante Michale S. Rogers, que também é chefe da NSA, é o responsável pelo *Cyber Command* e cabe a este orientar operações digitais ofensivas do governo estadunidense (SHILLER,

[7] SILVEIRA, Maria Rublescki. CALEA, Patriot Act e o fim da privacidade. 24/03/2014. Disponível em: http://listas.softwarelivre.org/pipermail/cisl-comunidade/2014-March/001122.html (acesso em 03/03/2015).

[8] O estudo não ficou restrito apenas à internet. Gilbert mostrou que em 2006 havia mais de 4,2 milhões de câmeras espalhadas pelo Reino Unido, ou seja, 1 câmera por 14 habitantes. A cada ano são instaladas 300.000 novas câmeras e um habitante de Londres pode ser gravado até 300 vezes em um único dia. (NOTICIASDOT. Vigilância electronica puede ser aprovechada por delincuentes. Disponível em: http://www.noticiasdot.com/wp2/2007/03/28/vigilancia-electronica-puede-ser-aprovechada-por-delincuentes/ (acesso em 08/03/2015).

05/11/2014). Atualmente Rogers dirigi 40.000 pessoas em ataques de redes e monitoramentos (APPLEBAUM; GIBSON et al, 17/01/2015).

O USCYBERCOM está localizado em Fort Meade, em Maryland. Não foi possível coletar muitas informações a seu respeito já que o acesso ao site é barrado. Só podem acessar o site, aparentemente, aqueles que possuem IP de território estadunidense[9]. Entretanto, o site do Departamento de Defesa dos EUA disponibiliza algumas informações a respeito do USCYBERCOM.

O USCYBERCOM é composto por várias forças militares: exército, marinha, fuzileiros navais e forças aéreas. Essas forças se subdividem em áreas centrais de ação:

1. Exército: *Army Cyber Command/Second Army*
    a. *Army Network Enterprise Technology Command/9th Army Signal Command*[10]
    b. *U.S. Army Intelligence and Security Command*
2. Marinha: *Fleet Cyber Command/Tenth Fleet*[11]
    a. *Naval Network Warfare Command*
    b. *Navy Cyber defense Operations Command*
    c. *Naval Information Operation Command*
    d. *Combined Task Forces*
3. Força Aérea: *Air Forces Cyber/Twenty-Fourth Air Force*
    a. *67th Cyberspace Operations Wing*
    b. *688th Cyberspace Operations Wing*
    c. *624th Operations Center*
    d. *5th Combat Communications Group*
4. Fuzileiro Navais: *Marine Corps Cyberspace Command*

Esses 4 setores são comandados pela NSA e possuem como objetivo fortalecer o monitoramento de informações e quebrar qualquer entrave para que isso ocorra. A sessão da marinha do *Cyber Command*, por exemplo, afirma a respeito de suas ações:

> *Fleet Cyber Command*'s vision is to condut operation in and through cyberspace, the electromagnetic spectrum, and space to ensure Navy and Joint/Coalition freedom of action and decision superiority while denying the same to our adversaries. We will win in these domains through our collective commitment to excellence and by strengthening

[9] Optou-se por não acessar o site com um IP falso a partir de softwares crackers.

[10] Fundado em 1º/10/2002. NETCOM. Disponível em: http://www.netcom.army.mil/ (acesso em 07/03/2015).

[11] Responsável pelos programas da marinha na *cyberwar*. Essa sessão foi fundada em janeiro de 2010 e é comandada por Jan E. Tighe. (U.S.FCC). Disponível em: http://www.fcc.navy.mil/ (acesso em 07/03/2015).

> our alliances with entities across the US government, Department of Defense, academia, industry, and our foreign partners.
> The mission of Fleet Cyber Command is to serve as central operation authority for networks, cryptologic/signals intelligence, information operations, cyber, electronic warfare, and space capabilities in support of forces afloat and achore; to direct Navy cyberspace operations globally to deter and defeat aggression and to ensure freedom of action to achieve military objectives in and through cyberspace; to organize and direct Navy cryptologic operations worldwide and support information operations and space planning and operations, as directed; to execute cyber missions as directed; to direct, operate, maintain, secure, and defend the Navy's portion of the Department of Defense Information Networs (DoDIN) to deliver integrated cyber, information operations, cryptologic, and space capabilities; to deliver a global Navy cyber common operational picture to develop, coordinate, assess, and prioritize Navy cyber, cryptologic/signals intelligence, space, information operations, and electronic warfare requirements; to assess Navy cyber readiness; and to exercise administrative and operational control of assigned forces[12].

Assim, A NSA conduz essas *cyber* forças. Essa aliança é parte estratégica do Tratado de Segurança UK-USA (*UK-USA Security Agreement*) de 1946. Tal tratado foi assinado primeiramente entre EUA e Reino Unido, posteriormente foram incluídos Canadá, Austrália e Nova Zelândia, formando os 5 olhos (*five eyes*). No tratado, os EUA são a "primeira parte" contendo a NSA como a "parte principal" e os outros países seriam as "partes secundárias". Essa divisão diz respeito ao compartilhamento de inteligência de monitoramentos em que a NSA é o centro.

> Todos esses países – além de se comprometerem a garantir o monitoramento das comunicações em determinada região, compartilhar sua infraestrutura com os Estados Unidos e realizar

[12] A visão da Frota de Comando Cibernético (Fleet Cyber Command) é a realização de operações através do ciberespaço, o espectro eletromagnético, e o espaço para garantir à Marinha a superioridade de articulação/aliança de liberdade de ação e decisão negando assim o mesmo para os nossos adversários. Vamos ganhar esses domínios por meio de nosso compromisso coletivo com a excelência e reforçando nossas alianças com entidades de todo o governo dos EUA, Departamento de Defesa, academia, indústria e nossos parceiros estrangeiros. A missão da Frota de Comando Cibernético (Fleet Cyber Command) é servir como autoridade operacional central para as redes de criptologia/inteligência de sinais, operações de informação, cibernéticos, guerra eletrônica e espacial, capaz de apoiar às forças navais e terrestres; para dirigir as operações do ciberespaço da Marinha a uma esfera global para deter e derrotar agressividade e para garantir a liberdade de ação alcançando assim os objetivos militares através do ciberespaço; para organizar e direcionar as operações criptológicas da Marinha por todo o mundo e apoiar as operações de informação e planejamento espaciais e operações, como direcionado; para executar missões cibernéticas como indicado; para dirigir, operar, manter, proteger e defender a parte da Marinha do Departamento de Defesa de Redes de Informação (Dodin); para integrar ações de informação, criptologia e capacidades espaciais; para entregar um cenário operacional comum cibernético da Marinha; para desenvolver, coordenar, avaliar e priorizar a Marinha cibernética, criptologia/inteligência de sinais, espaço, informações operacionais, e os requisitos de guerra eletrônica; para avaliar de prontidão a Marinha cibernética; e exercer o controle administrativo e operacional das forças designadas. U.S. FCC. Disponível em: http://www.fcc.navy.mil/ (acesso em 08/03/2015).

> operações conjuntas com eles – podem acessar as informações coletadas em conformidade com os procedimentos estabelecidos por Washington (SCHILLER, 05/11/2014).

Entretanto, os acordos se expandem e existem as "terceiras partes" deste sistema que é composta por países não assinantes desse tratado, mas assinantes do Tratado Atlântico Norte e outros. Essa terceira parte possui acesso restrito às informações coletadas.

> Foi o caso, por algum tempo, do Irã, bem localizado para observar o sul da União Soviética. Com a revolução de 1979, os Estados Unidos tiveram de encontrar um substituto. Então, institucionalizaram os laços com a República Popular da China, e as relações entre os dois países melhoraram após a visita secreta de Henry Kissinger, em abril de 1970. A província de Xinjiang parecia um lugar conveniente para espionar os russos: Deng Xiaoping, o grande arquiteto da abertura da China para a economia de mercado, autorizou a CIA a construir duas estações de monitoramento, com a condição de que fossem ocupadas por técnicos chineses. Operacionais desde 1981, elas funcionaram pelo menos até meados da década de 1990. (SCHILLER, 05/11/2014).

O jornalista Greenwald, responsável pela publicização dos arquivos de Edward Snowden no jornal *The Guardian* publicou uma troca de e-mails com Jamel Jaffer, diretor da *American Civil Liberties Union* (UCLA), em que este revela sua preocupação com o monitoramento de informações dos estadunidenses:

> On its face, the 2008 law gives the government authority to engage in surveillance directed at people outside the United States. In the course of conducting that surveillance, though, the government inevitably sweeps up the communications of many Americans. The government often says that this surveillance of Americans' communications is 'incidental', which makes it sound like the NSA's surveillance of Americans' phone calls and emails is inadvertent and, even from the government's perspective, regrettable (Jaffer apud GREENWALD, 19/06/ 2013).[13]

***

O empreendedor do Vale do Silício Andrew Keen (2009) afirmou que a *idade da vigilância* não ocorre de cima para baixo, mas ela também está ocorrendo pela obsessão de transmitirmos tudo o que fazemos a todo momento. Diferente de autores como Clay Shirky (2011; 2012), Juliano Spyer (2007), Bill Tancer (2009) e jovens empreendores

[13] "À primeira vista, a lei de 2008 dá ao governo autoridade para exercer a vigilância sobre as pessoas de fora dos EUA. Na realização dessa vigilância, entretanto, o governo inevitavelmente varre as comunicações de muitos estadunidenses. O governo afirma que muitas vezes essa vigilância é "incidental", o que torna a vigilância das chamadas telefônicas e dos e-mails dos estadunidenses pela NSA de forma inadvertida lamentável, mesmo do ponto de vista do governo".

do Vale do Silício (de Larry Page da Google ao jovem empregado de uma *startup*[14]), Keen acredita que a internet tem um efeito destrutivo na cultura, economia e valores já que seus usuários só produzem mediocridades.

Para Keen essa vigilância ocorre também porque revelamos muito sobre nós: na página do Facebook e do MySpace, nos vídeos no YouTube, nos blogs. É uma cultura confessional, segundo Keen, resultando em uma explosão-cultural de auto-revelação pessoal, sexual e política.

A privacidade já não é mais o que está em jogo para esses usuários, por isso há tantos sites confessionais anônimos[15]. Entretanto, esses sites utilizam *cookies* para identificar os leitores e os escritores. Não há anonimato na internet.

Segundo Keen é questão de tempo para que algum hacker vaze a verdadeira identidade das pessoas que postam suas confissões nesses sites. Para o empreendedor, a melhor cúpula de espionagem não são alguns especialistas reunidos em algum lugar secreto, mas são esses inúmeros usuários amadores conectados que formam uma multidão de *policiais secretos democraticamente organizados* (KEEN, 2009, p. 166).

A internet, então, é uma mídia democratizada em que a peça fundamental é o usuário que recebe e gera informação. Esse mesmo usuário consegue espionar todos ao mesmo tempo em que é alvo dessa espionagem. Para Keen trata-se de um *panóptico digital*, agora todos podem ser o *Grande Irmão*.

Assim, as linhas entre público e privado estão se apagando Todas as nossas pesquisas em sites de busca e comentários e postagens em redes sociais são possíveis de serem acessadas por outros (KEEN, 2009).

Os recentes vazamentos de Edward Snowden abalaram esses usuários, entretanto, esse abalo logo foi contornado. Edward Snowden pretendia com os seus vazamentos que as pessoas tomassem conhecimento das práticas de espionagem e monitoramento do governo estadunidense. Mas, o que se comprovou, foi que as pessoas desejam que seus e-mails sejam monitorados, como mostrou David Price, antropólogo da Universidade de Washington :

[14] A esse respeito ver série *Sillicon Valley* da HBO que traz a história de jovens programadores no Vale do Silício.

[15] Disponível em: http://www.dailyconfession.com/; http://www.notproud.com e a versão brasileira: http://www.euconfesso.com/ (acesso em 09/02/2015).

> Segundo pesquisa realizada pelo jornal *Washington Post* alguns dias depois das declarações de Snowden, 56% da população julga que o programa PRISM é "aceitável" e 45% acredita que o Estado deve "ser capaz de vigiar os e-mails de qualquer pessoa na luta contra o terrorismo". Esses resultados não surpreendem: há mais de dez anos, os meios de comunicação, especialistas e dirigentes políticos vêm apresentando a vigilância como arma indispensável à guerra contra o terrorismo.[16]

Diante disso, a leitura de Keen se mostra importante por caracterizar os usuários como policiais. Entretanto, aquilo que ele chamou de *panóptico digital* não se trata da internalização da vigilância para a produção de uma conduta economicamente útil e politicamente dócil. O que ocorre é um monitoramento central (governo dos EUA articulado com servidores) e uma *bisbilhotagem* entre os próprios usuários que denunciam uns aos outros[17]. O *Grande Irmão* não é a Google e não possui sede na cidade de Mountain View no Vale do Silício. Não há um *Grande Irmão*, mas o monitoramento de informações de cada um a partir da aliança entre governo e empresas e a adesão de usuários aos infindáveis protocolos.

Essa adesão ao monitoramento ganhou força na sociedade estadunidense com os ataques ao World Trade Center e ao Pentágono em 11 de setembro de 2001.

> Algumas semanas antes do atentado de 11 de setembro de 2001, o jornal *USA Today* publicava a manchete: "Quatro em cada dez norte-americanos não confiam no FBI" (20 jun. 2001).[18]

Julian Assange, o diretor-chefe do Wikileaks, em livro lançado este ano, marca seu distanciamento com Edward Snowden ao mostrar que seja Estado ou empresas, ambos monitoram os dados, não há como medir qual o melhor e qual o pior monitoramento:

> Há uma disposição constrangida entre os que defendem a privacidade de tomar partido contra a vigilância em massa do Estado, mas não contra métodos semelhantes de vigilância utilizados com fins lucrativos pelas grandes empresas. [...] Individualmente, muitos defensores da privacidade, inclusive os mais comprometidos, admitem ser viciados em programas de uso fácil, mas que acabam com a privacidade, como é o caso do Gmail, do Facebook e dos produtos da Apple. Consequentemente, os que defendem a privacidade muitas

[16] PRICE, David. A história social das escutas telefônicas. *Le monde diplomatique*. 01 de agosto de 2013. Disponível em: http://www.diplomatique.org.br/artigo.php?id=1476 (acesso em 05/03/2015).

[17] Um exemplo são as denúncias diárias ao Facebook sobre a postagem de alguém.

[18] PRICE, David. A história social das escutas telefônicas. *Le monde diplomatique*. 01 de agosto de 2013. Disponível em: http://www.diplomatique.org.br/artigo.php?id=1476 (acesso em 05/03/2015).

> vezes negligenciam os abusos das empresas privadas. Quando se voltam contra os abusos de empresas como o Google, eles tendem a apelar para a lógica do mercado, exigindo que as empresas façam pequenas concessões à privacidade do usuário para melhorar sua provação. [...] Muitos dos que defendem a privacidade justificam o foco predominante nos abusos do Estado alegando que o Estado possui o monopólio da força coercitiva. Por exemplo, Edward Snowdem disse supostamente que as empresas de tecnologia não "dirigem ogivas contra as pessoas". [...] Essa visão diminui a importância do fato de que empresas poderosas fazem parte do centro do poder de Estado e podem usar seu poder de coerção, do mesmo modo que o Estado muitas vezes exerce sua influência por intermédio de empresas poderosas. O movimento para acabar com a privacidade é uma faca de dois gumes. Defensores da privacidade que veem apenas um dos gumes serão feridos pelo outro (ASSANGE, 2015, p. 50-51).

Os procedimentos de monitoramento do governo dos EUA só podem ser compreendidos quando articulados com a Google.

> Em 2003, a Agência de Segurança Nacional (NSA, na sigla em inglês) já violova sistematicamente a Lei deVigilância de Inteligência Estrangeira (Fisa, em inglês), sob a direção do general Michael Hayden. Isso foi na época do programa Total Information Awareness [Conhecimento de Informação Total]. Antes que se sonhasse com o Prism, por ondem da Casa Branca de Bush a NSA já tinha o objetivo de "coletar tudo, farejar tudo, saber tudo, processar tudo, explorar tudo". Nessa mesma época, o Google – cuja missão publicamente declarada é coletar e "organizar as informações do mundo e torná-las universalmente acessíveis e úteis" – aceitou um financiamento da NSA da ordem de US$ 2 milhões para fornecer à agência ferramentas de busca para vasculhar um tesouro de conhecimento roubado que não parava de crescer.
>
> Em 2004, depois de adquirir a Keyhole, uma start-up de mapeamento cofinanciada pela Agência Nacional de Inteligência Geoespacial (NGA, na sigla em inglês) e pela CIA, o Google desenvolveu a tecnologia do Google Maps e uma versão empresarial que, desde então, é fornecida ao Pentágono e a órgãos federais e estaduais associados mediante contrato milionários. Em 2008, o Google ajudou a lançar um satélite estão da NGA, o GeoEye-1. O Google compartilha as imagens captadas pelo satélite com as comunidades militares e de inteligência dos Estados Unidos. Em 2010, a NGA firmou com o Google um contrato de US$ 27 milhões para "serviços de visualização geoespacial" (ASSANGE, 2015, p. 38-39).

O documentário premiado no Oscar em 2015 foi o *CitizenFour* de Laura Poitras [19] e que retrata como foi o processo de publicização dos documentos de Snowden. *CitizenFour* era como Snowden assinava os e-mails criptografados que enviava a Poitras e Greenwwald. No documentário, Poitras recolhe o depoimento de

[19] Laura Poitras, juntamente com Glenn Greenwald, foi um primeiros contatos que Snowden estabeleceu para transmitir as informações que detinha.

William Binney, um cripto matemático da NSA que durante a Guerra Fria analisou dados de ameaças nucleares e na década de 1990 passou a se dedicar à internet e métodos de análise de grandes volumes de dados.

> Passei cerca de 4 anos no exército e depois fui diretamente para a NSA, então... assim, eu acabei com cerca de 37 anos de serviço acumulado. A maior parte foi muito divertido! Eu lhes digo, foi realmente muito divertido, quebrando enigmas[...] Fundamentalmente comecei a trabalhar com dados, analisando dados e sistemas de dados [...]. Eu estava desenvolvendo o conceito de análise onde você poderia colocá-lo de tal maneira que poderia ser codificado e executado eletronicamente. Ou seja, você pode automatizar a análise. E isso tem a ver com metadados e usando relações de metadados. Então, isso era tudo, esse era todo o meu tema lá no NSA o qual foi eventualmente finalizado, eu era o único lá fazendo isso, por sinal. Então de qualquer forma, vocês sabem, 11/09 aconteceu. [...] Poucos dias depois, não mais do que uma semana após 11/09 eles decidiram começar ativamente a espionar todos neste país. E eles queriam essa parte do nosso programa para executar toda a espionagem. Então, isso foi exatamente o que eles fizeram. E depois eles começaram a tomar os dados das telecomunicações, e expandiram depois disso. Então, quero dizer, o único que eu conhecia era AT & T, e apenas ele fornecia 320 milhões de registros de todos os dias (BINNEY in POITRAS, 2014).

A respeito do PRISM, Snowdem afirmou no documentário de Poitras:

> Então, eu não sei o quanto são os programas e as atuais capacidades técnicas. [...] mas existe uma infra-estrutura no local, nos Estados Unidos e em todo o mundo, que a NSA construiu em cooperação com outros governos, que intercepta basicamente todas as comunicações digitais, todas as comunicações de rádio, cada comunicação analógica que tem sensores para detectar. E com esses recursos, basicamente a grande maioria dos humanos e das comunicações computador para computador, dispositivos baseados em comunicação, que trocam esse tipo de continuidade das relações entre seres humanos são ingeridos automaticamente sem orientação.
> [...] Assim, por exemplo, se eu quisesse ver o conteúdo do seu e-mail ou, você sabe, as chamadas de telefone de sua esposa ou qualquer coisa assim. Tudo que tenho que fazer é usar o que é chamado de "seletor". Qualquer tipo de coisa na cadeia da comunicação que possam exclusivamente ou quase exclusivamente identificá-lo como um indivíduo. E eu estou falando sobre coisas como endereços de e-mail, endereços de IP, números de telefone, cartões de crédito, até mesmo senhas que são exclusivos para você, que não são utilizados por mais ninguém (SNOWDEN in POITRAS, 2014).

***

Alexander Galloway pensa as *interfaces* como zonas autônomas de atividade. Interfaces não são objetos, apesar de existirem materiais particulares da interface (telas, teclados, mouses). Interfaces são essas zonas produzem efeitos de variados tipos. Por isso, em Galloway, interessa os *efeitos da interface* (GALLOWAY, 2012, 8).

Interfaces são mediações entre algo que em um primeiro momento não se conecta, como o modem e o computador. As interfaces possibilitam isso.

Nesse sentido, Evgeny Morozov vai de encontro com o que afirma Galloway ao mostrar que na vida digital cada vez mais temos intermediários, mesmo porque, a internet já parte da intermediação da interface.

Acredita-se que a internet possa por fim a intermediação com as possibilidades de e-gov, manifestações individuais via redes sociais e etc. Entretanto, a partir da leitura de Morozov, é possível afirmar que o que temos é uma *hiperintermediação* (11/10/2012). Por exemplo, uma pessoa que possui uma conta no Facebook e ali mantém seus comentários diários, a todo momento terá a informação intermediada. O Facebook, antes de mais nada, é uma empresa que coopera com os programas de monitoramento do governo dos EUA e possui um sistema para dizer se uma postagem pode ser ou não autorizada.

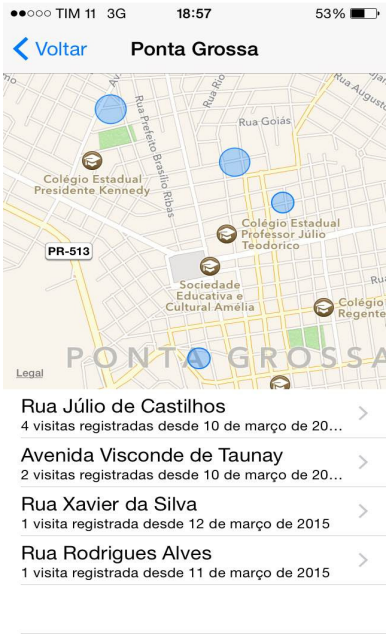
Morozov, apesar de ter esse ponto de encontro com Galloway ao constatar a *mediação*, se distancia ao entender que a internet não é democrática. Galloway, quando realizou seus estudos sobre protocolos entendeu que uma rede marginal, um contra-protocolo, poderia vir fortalecer a democracia. A visão realista de Morozov vai contra essa leitura e leituras empolgadas (comuns à esquerda) com a internet. A leitura de *hipermediação* de Morozov já se distancia da leitura de Galloway porque esse entende que essa mediação não fortalecerá a democracia.

Em relação à internet mais especificamente, Morozov faz uma desconstrução desta. *The internet* é o nome que se dá a um conjunto de coisas, um substantivo que designa uma série de tecnologias interligadas, não se pode dizer que a internet faz ou deixa de fazer algo, não é possível personificá-la. Ela está em vários aparelhos, modula as nossas relações e tem inúmeros componentes (protocolos, monitoramentos, interfaces...). Por isso, nas obras de Morozov, a internet sempre aparecerá entre aspas ou em itálico.

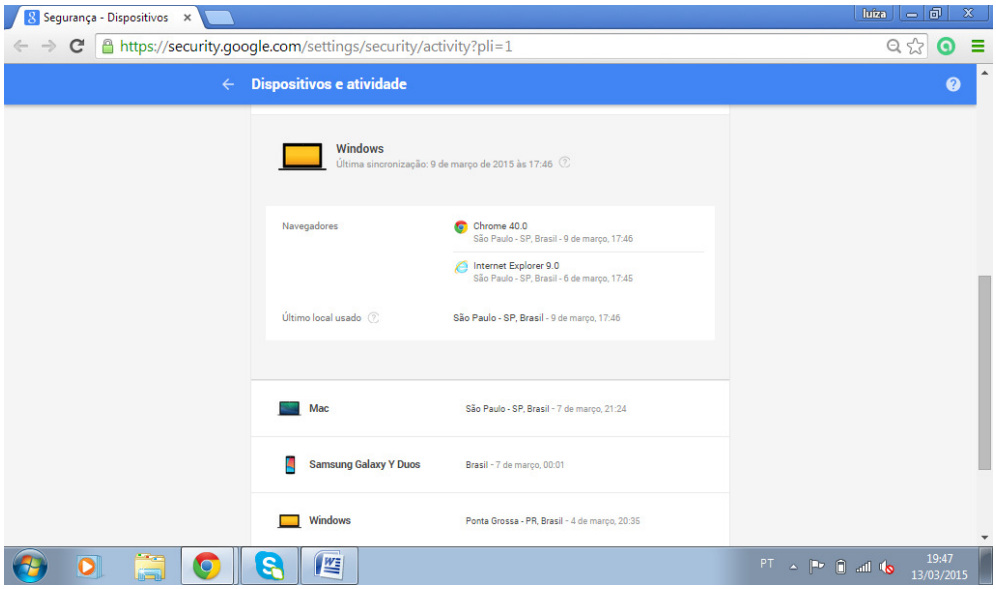
Morozov também não compactua com Andrew Keen, não entende que a internet destrói valores. Da mesma maneira, também não entende que se trata de defender o compartilhamento e vislumbrar um futuro horizontal que possa derrubar hierarquias. Morozov busca compreender como os dados de usuários são utilizados, como dados são importantes tanto para a economia como também para influenciar medidas de austeridades.

Somos dependentes desse processo chamado internet. Essa dependência faz com que distorçamos processos sociais e políticos. Acreditamos que o que vemos na tela é um reflexo fidedigno do que ocorre quando se está longe de conexões. Mas os sites como Google, Twitter, Facebook, Linkedin possuem seus algoritmos que fazem seleções do que cada um verá. O que as pessoas veem passou por uma seleção: a propaganda é individual e a busca trará um resultado para cada usuário. Todos os nossos acessos, todas as nossas pesquisas, todas as fotos postadas estão em um banco de dados unificado que terceiros podem vasculhar para oferecer aquilo que cada um espera.

Acreditamos que os serviços da Google são gratuitos, que o acesso à internet é gratuito (ou que pagamos apenas um valor pela conexão), mas todos os nossos dados estão rastreados. Fornecemos dados que geram lucro para grandes servidores e nos abrimos para qualquer monitoramento. Os sistemas iOS dos iPhones da Apple extraem esses dados e acompanham os passos do usuário. A partir disso, a central da Apple sabe todos os locais que uma pessoa foi e com qual frequência (o mesmo ocorre em smartphones com sistema Android). Da mesma maneira, basta acessar uma conta do Google que ele armazenará os dados do aparelho que está conectado e o local de onde se acessa:



Exemplo de monitoramento de localização no iPhone.



Rastreamento de acesso à conta Google.

Os algoritmos que fazem esses mapeamentos também são aliados da polícia, como boa parte do Vale do Silício. O Facebook utiliza algoritmos articulados com dados do histórico dos usuários para tentar prever quais deles cometeriam crimes usando a rede social. Por exemplo, se um usuário tem um comportamento suspeito (conversar com somente uma pessoa no bate-papo do Facebook ou usar palavras como sexo ou encontro) um funcionário examinará o perfil deste e, caso considere necessário, reportará à polícia (MOROZOV, 2014, p. 186).

Em 2011 o Facebook passou a utilizar o PhotoDNA, desenvolvido pela Microsoft, para scanear todas as fotos que são postadas, posteriormente as compara com imagens de pornografia infantil do banco de dados do FBI. Esse programa se expandiu e agora scanea qualquer imagem para barrar pornografia em geral.

> Facebook is at the cutting edge of algorithmic surveillance here: just like police departments that draw on earlier crime statics, Facebook draws on archives of real chats that preceded real sex assaults.
> Curiously, Facebook justifies its use of algorithms by clamming that they tend to be less intrusive than humans. “We’ve never wanted to set up an environment where we have employees loking at private communications, so it’s really important that we use technology that has a very low false-positive rate,” Facebook’s chief of security told Reuters.[20] (MOROZOV, 2014, p. 186).

[20] O Facebook é a vanguarda do algoritmo de vigilância: da mesma forma que a polícia se baseia em estatísiticas de crimes anteriores, o Facebook se baseia em arquivos de bate-papos que precederam agressões sexuais. Curiosamente, o Facebook justifica a utilização do algoritmo por conta de solicitações para serem menos intrusivos que as pessoas. “Nós nunca quisemos criar um ambiente onde os funcionários olham as comunicações privadas, por isso é muito importante utilizarmos a tecnologia que possui um baixo índice de erro,” chefe de segurança do Facebook à Reuters.

Todo esse recolhimento de informações modifica a maneira de identificar o potencial terrorista e, para Morozov, pretende diminuir crimes e punir mais:

> No passado, a propensão de uma pessoa ao terrorismo era medida com base nos livros que ela lia e nos sermões que ouvia; hoje, ela é medida pelos cliques de seu uso da Web e pelos apps que a pessoa baixa. Não é que livros e sermões tenham perdido a importância --eles continuam a ter papel crucial--, mas hoje são consumidos de modo digital, de uma forma que deixa uma trilha, e essa trilha permite estabelecer padrões. Os livros que você comprou hoje na Amazon são mais radicais do que aqueles que comprou no mês passado? Se são, você pode se tornar objeto de interesse para os serviços de segurança (MOROZOV, 27/7/2013).

Vale ressaltar que esse recolhimento de dados não ocorre apenas quando se está conectado por meio de smartphones, tablets ou computadores, mas também por meio de outros aparelhos domésticos. As futuras casas inteligentes serão compostas por eletrodomésticos que colherão dados ininterruptamente. As TVs inteligentes já estão presentes e ligadas ao NetFlix ou ao Youtube, mapeando todas as nossas preferências. Em breve, da escova de dente à geladeira, todos serão *smarts*. Essa é a *internet das coisas* em que a Google investe com a sua filial Nest[21]. Todo esse recolhimento de dados permitiria, em mio a tantas informações, a Google oferecer exatamente o que a pessoa procura. O melhor resultado seria encontrado, o produto mais adequado seria ofertado no momento exato.

> Menos obcecada pela moral que pela eficiência econômica e o interesse do consumidor, a abordagem do Google, por si, junta-se à ideologia neoliberal norte-americana. Apesar de suas pretensões de inovação e perturbação da ordem estabelecida, o debate contemporâneo sobre a tecnologia fica, portanto, apertado em um constrangimento conhecido: se consideramos a informação como mercadoria, ele se integra perfeitamente ao paradigma liberal (MOROZOV, 02/10/2014).

Portanto, múltiplas funções desses bancos de dados: identificar suspeitos de terrorismos e ofertar o produto adequado para todas as necessidades. Mas não somente isso, com esses dados recolhidos também é possível: salvar o planeta e aumentar a eficiência de nossas ações.

Em *To save everthing, click here*, Morozov descreve o projeto BinCam que pretende modernizar as lixeiras e está em fase de elaboração na Alemanha e na Grã-

[21] A Nest produz termostatos inteligentes, alarmes de fumaça (tanto para cigarros como para incêndios), e câmeras para os cômodos da casa que podem ser acessadas de qualquer lugar. Disponível em; https://nest.com/.

Bretanha. Uma câmera é acoplada à tampa da lixeira e cada vez que algo for descartado e a tampa fechada, uma foto é tirada. A imagem é enviada para a Amazon que analisa o que cada um jogou: "What is the total number of items in the Picture? How many of them are recyclabe? How many are food items?"[22] Depois dessa etapa, a foto é postada no perfil do Facebook do dono da lixeira. Dependendo de como era a foto, o usuário ganha pontos em um jogo online de consumo verde. "Mission accomished; planet saved"(MOROZOV, 2014, p. 2).

Esse sistema de pontuação é a *gamification*, por meio de rankings e pontos atingem-se determinadas metas, por exemplo, jogar Nintendo Wii para emagrecer. Morozov aponta outro exemplo:

> Recyclebank, a company that uses points and rewards to nudge consumers to perfom eco-friendly activities, is another one. Once you accumulate enough points for your green behavior, Recyclebank allows you to convert them into discounts, free offers, and gift cards[23] (MOROZOV, 2014, p. 297).

A *gamification* também é um meio de aumentar a eficiência. Os aplicativos HabitRPG ou The Habit Factory, por exemplo, auxiliam seus usuários a construírem uma rotina como se estivessem em um jogo de RPG. A cada atividade feita o usuário deve colocá-las no aplicativo, ações como leitura e trabalho produtivo valem pontos, por outro lado, comer porcaria leva a perda de pontos. A premiação é ficar acima no ranking e passar de level. A *gamification*, então, renova a recompensa para evitar a ineficiência, motivar com pontos e tornar hábito práticas ecológicas e saudáveis.

Morozov mostra que a *gamification* não é uma característica apenas do ocidente, ou que se desenvolveu nos EUA. O autor viveu os últimos anos do regime soviética na Bielorússia e, sobre esse período, recorda:

> As someone who grew up in the final years of the Soviet Union, even I remember the penchant that Soviet managers had for gamification: students were shipped to the fields to harvest wheat or potatoes, and since the motivation was lacking, they too were assigned points and badges. (MOROZOV, 2014, p. 351)[24].

[22] Qual é o total de itens na imagem? Quantos deles são recicláveis? Quantos são comida?

[23] Recyclebank é mais uma, é uma companhia que usa pontos e recompensas para incentivar os consumidores a tomarem atitudes ecológicas. Uma vez que você acumula pontos pelo seu comportamento verde, Recyclebank possibilita que você os converta em descontos, ofertas gratuitas e cartões de presente.

[24] Como alguém que cresceu nos últimos anos da URSS, sempre me lembro da propensão que os gestores soviéticos tinham para a *gamification*: os estudantes eram enviados para campos de colheita de batatas ou trigo, e quando a motivação baixou, foram atribuídos identificações e pontos.

Para demonstrar o funcionamento da *gamification*, Morozov faz um paralelo entre o psicólogo Burrhus Frederic Skinner e o engenheiro Frederic Taylor para afirmar que sejam ratos ou trabalhadores ao prometer mais comida ou bônus, pode-se extrair um melhor desempenho desses corpos. Assim, Morozov mostra que as ações humanas podem ser influencias por motivações extrínsecas, seja pela punição seja pela busca de prazer/recompensa (MOROZOV, 2014, p. 302).

Entretanto, os humanos não são incitados apenas por motivações extrínsecas, mas intrínsecas também. Estas ocorrem quando se realiza algo porque se acredita que é o que se quer, porque se acha que é o correto a se fazer. A grande questão da *gamification*, então, é como fazer que as motivações extrínsecas tornem-se intrínsecas.

A *gamification* é uma expressão da crença no *solucionism* e que impera no Vale do Silício, segundo Marazov. O *solucionism* é a ideia de que a tecnologia irá sanar todos os problemas: desde a obesidade até as mudanças climáticas. Com os novos aplicativos poderemos nos monitorar e saber se nossa prática é adequada ou não.

Essa é uma das ideologias que atravessa o Vale do Silício atualmente, onde o lema já não é mais "Innovate or die", mas "Ameliorate or Die". Há uma crença que a tecnologia pode tornar as pessoas melhores, uma *orgia do melhoramento*, "Or, as the geeks would say, given enough apps, all humanity's bugs are shallows"[25] (MAROZOV, 2014, VIII).

Outra ideologia presente no Vale do Silício e que gera tais afirmações é o *internet-centrism*, que se pauta na crença de que estamos vivendo tempos revolucionários, em que as verdades anteriores já não possuem funcionalidade e a necessidade de *consertas as coisas* é mais urgente do que nunca (MOROZOV, 2013, p. 16). As duas ideologias seriam efeitos da difusão da *razão instrumental*. Esta nunca foi tão difundida e está presente na educação e na cultura.

O *internet-centrism* tornou-se algo como uma religião que crê na internet um modelo para a sociedade (MOROZOV, 2013, p. 62). Por exemplo, acredita-se que o *crowdfunding* é uma alternativa aos financiamentos para realizar um projeto. Entretanto, este é um suplemento, é somente uma outra forma de financiamento.

Nestes financiamentos, é muito provável que em um site *crowdfunding* um projeto sobre aquecimento global e que seja divulgado entre ativistas será financiado.

[25] Ou, como os geeks diriam, com aplicativos, todos os bugs da humanidade são superficiais.

Enquanto um projeto de documentário sobre as causas da Primeira Guerra Mundial não conseguirá ser realizado se depender apenas desse meio de financiamento. O *crowdfunding*, como todo financiamento, é seletivo. E para Morozov é um erro acreditar que as pessoas assumiram papéis antes realizados por instituições públicas (MOROZOV, 2013, p. 28).

Não somente no *crowdfunding*, mas a articulação do *solutionism* com o *internet-centrism* produz a crença de que a internet pode trazer transparência e nos possibilitar maior responsabilidade civil. Também pode, como visto anteriormente, além da *gamification*, prever crimes, punir mais, salvar o planeta por meio de aplicativos e ter uma vida mais saudável.

Entretanto, para Morozov, não precisamos que a internet se sobreponha à sociedade, mas entender como tecnologia e sociedade se relacionam. Não se trata de uma visão Se o *internet-centrism* está presente, precisamos de uma *secularização* da comunicação.

> Such secularization can no longer be postponed. We need to find a way to temporarily forget everything we know about "the internet" - we take too many things for granted these days - roll up our sleeves, and work to ensure that technologies do not just constrain human flourishing but also enable it (MOROZOV, 2013, p. 62)[26].

Morozov não é um tecnofóbico, nem um tecno-otimista, mas critica o imperativo do *melhoramento* e rejeita o determinismo tecnológico. É preciso se afastar do *internet-centrism* e do *solucionism* e refletir sobre o impacto da tecnologia:

> only by unlearning solutionism — that is, by transcending the limits it imposes on our imaginations and by rebelling against its value system — will we understand why attaining technological perfection, without attending to the intricacies of the human condition and accounting for the complex world of practices and traditions, might not be worth the price (MOROZOV, 2013, p. XIII)[27].

[26] Esta secularização não pode mais ser adiada. Precisamos encontrar uma maneira de esquecer temporariamente tudo o que sabemos sobre "*the internet*" – tomamos muitas coisas para permitir esses dias –, arregaçar as mangas, e trabalhar para assegurar que as tecnologias não vetem o crescimento humano, mas o faça prosperar.

[27] Nos desvencilhando do *solutionism* – isto é, transcendendo os limites que ele impõe em nossas imaginações e rebelando-se contra o seu sistema de valores – é que vamos entender por que alcançar a perfeição tecnológica, sem atentar para a complexidade intrínseca ao homem e sem compreender o complexo mundo de práticas e tradições, pode não valer o preço.

A proposta de Morozov para as relações na internet é uma política de internet inteligente, com uma rede de segurança digital que poderia ser mais humana sem barrar a inovação ao mesmo tempo.

> Designers and social engineers don't have to become unambitious bureaucrats scares of innovating, but perhaps they could practice innovation in a different key. The goal of their interventions – in both products and policies – should be not just to provide answers but also to make it easier to pose new questions. If technological fixes are inevitable, and if some forms of solutionism cannot be avoided, let us as least sure that this solutionism is of the self-reflexive, perhaps even neurotic, kind. Only through radical self-doubt can solutionism transcend its inherent limitations (MOROZOV, 2013, p. 352)[28].

[28] Designers e engenheiros sociais não devem se tornar burocratas ansiosos com medo da inovação, mas, por outro lado, eles podem praticar a inovação de um modo diferente. O objetivo das intervenções – em produtos e políticas – não devem apenas prover respostas, mas também deixar mais fácil a postura de novas questões. Se a tecnologia determinar que são inevitáveis, e se algumas formas de soluções não podem ser evitadas, devem deixar claro ao menos que essas soluções são auto-reflexivas, talvez, de um certo modo, até neuróticas. Somente por meio do auto-questionamento radical pode-se solucionar e transcender suas limitações inerentes.

Bibliografia

APPELBAUM, Jacob; GIBSON, Aaron; GUARNIERI, Claudio; MÜLLER-MAGUHN, Andy; POITRAS, Laura; ROSENBACH, Marcel; RYGE, Leif; SCHUMUNDT, Hilmar; SONTHEIMER, Michael. *The digital arms race: NSA preps America for future battle*. Disponível em: http://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409.html.

GALLOWAY, Alexander R. *The interface effect*. Cambridge/Malden: Polity Press, 2012.

GREENWALD, Glenn. *Fisa court oversight: a look inside a secret and empty process*. The Guardian. Edição: 19/06/2013. Disponível em: http://www.theguardian.com/commentisfree/2013/jun/19/fisa-court-oversight-process-secrecy.

KEEN, Andrew. *O culto do Amador: como blogs, MySpace, YouTube e a pirataria digital estão destruindo nossa economia, cultura e valores*. Tradução de Maria Luiza X. de A. Borges. Rio de Janeiro: Zahar, 2009.

MOROZOV, Evgeny. *Na vida digital cada vez mais intermediários*. Folha de São Paulo. Edição: 11/10/2012. Disponível em: http://www1.folha.uol.com.br/colunas/evgenymorozov/2012/10/1175587-na-vida-digital-cada-vez-mais-intermediarios.shtml.

_____. *'Big data' poderia ter impedido o 11 de setembro?* Folha de São Paulo. Edição: 23/07/2013. Disponível em: http://www1.folha.uol.com.br/colunas/evgenymorozov/2013/07/1300648-big-data-poderia-ter-impedido-o-11-de-setembro.shtml.

_____. *Da utopia digital ao choque social*. Le monde Diplomatique Brasil. 02/10/2014. Disponível em: http://www.diplomatique.org.br/artigo.php?id=1744.

SCHILLER, Dan. *Geopolítica da espionagem*. Le Monde Diplomatique Brasil. 05/11/2014. Disponível em: http://www.diplomatique.org.br/artigo.php?id=1762.

SHIRKY, Clay. Lá *vem todo mundo: o poder de organizar sem organizações*. Rio de Janeiro: Zahar, 2012.

_____. *A cultura da participação: criatividade e generosidade no mundo conectado*. Rio de Janeiro: Zahar, 2011.

SILVEIRA, Maria Rublescki. CALEA, Patriot. *Act e o fim da privacidade*. 24/03/2014. Disponível em: http://listas.softwarelivre.org/pipermail/cisl-comunidade/2014-March/001122.html.

SILVEIRA, Sérgio Amadeu da. *O fenômeno Wikileaks e as redes de poder*. Compolítica, 2011. Disponível em: http://www.compolitica.org/home/wp-content/uploads/2011/03/Sergio-Amadeu.pdf.

U.S. Hearing FISA. *Whashigton: U.S*. Government Printing Office, 1978. http://www.intelligence.senate.gov/pdfs/s1566.pdf.

_____. *ECPA*. 1986. Disponível em: http://www.justice.gov/sites/default/files/jmd/legacy/2013/09/06/act-pl99-508.pdf.

_____. *Top Secret document: Legislate Strategy for Digital Telephony.* 17/01/1991. Disponível em: http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/epic-foia-images/scowcroft-memo.html.

Filmes

POITRAS, Laura. *Citizenfour*. EUA/Alemanha: Paris Films, Participant Media, HBO Films, 2014.