

Hackear ou ser hackeado: o quase-totalitarismo das redes de segurança globais¹

To hack or be hacked: the quasi-totalitarianism of global trusted networks

*Athina Karatzogianni*² e *Martin Gak*³

1 Athina Karatzogianni destaca as contribuições da Conferência do Liberty Fund "Totalitarianism, democracy, and liberty" (Totalitarismo, democracia e liberdade), realizada em outubro de 2014 na Cracóvia (Polônia), pela experiência intelectual significativa refletida no desenvolvimento das ideias incluídas no presente artigo. A autora agradece também ao Economic and Social Research Council (ESRC), que financiou o projeto "The common good: ethics and rights in cyber security" (O bem comum: ética e direito na cibersegurança). Tradução do inglês: Andrea Limberto. andrealimberto@gmail.com.

2 Docente na área de Novas Mídias e Comunicação na Universidade de Leicester (Inglaterra). Foi diretora dos Programas de Mídia do Departamento de Ciências Sociais da Universidade de Hull (Inglaterra). Autora de *The politics of cyberconflict* (2006); *Power, conflict and resistance: social movements, networks and hierarchies* (2010), entre outros trabalhos. athina.k@gmail.com.

3 Doutor em Filosofia pela New School for Social Research (Estados Unidos). Pesquisa na interface da Ética e da Metafísica, seus interesses de pesquisa relacionam-se com a política, religião e jurisprudência. martin@martingak.com.

Resumo

O presente artigo se concentra nas questões ideológicas da vigilância digital, examinando exemplos empíricos específicos retirados de reportagens publicadas sobre o caso Snowden, com o objetivo de matizar o lugar da política, da ética, dos valores e afetos mobilizados por governos e pela elite corporativa justificando a prática de coleta de dados pessoais numa associação entre três das redes globais de "segurança". Analisa-se a constituição de um espaço político como esfera de atuação que emerge em contraposição ao que estamos nomeando como mecanismos "quase-totalitários", baseados na ideia de alinhamento, conluio e imbricamento das três redes de segurança. Os diferentes aspectos desse quase-totalitarismo incluem: o monopólio do planejamento digital em relação à vigilância e a comunicação secreta entre governos, a elite corporativa e, algumas vezes, ONGs; o papel das ONGs na sociedade civil como forma de contornar processos democráticos; as políticas de associação entre empresas que assegurem o duplo objetivo do estado (segurança) e do capital (lucro); a dimensão inigualável da estrutura de aquisição de dados pelas matrizes da inteligência ocidental; a perseguição e julgamento de jornalistas, denunciantes e atores lutando em favor da transparência fora da esfera dos grupos da sociedade civil; e a significativa, mas insuficiente, contestação por parte do público de crimes contra as liberdades civis.

Palavras-chave

Segurança, ideologia, quase-totalitarismo, Snowden, redes digitais.

Abstract

This article focuses on digital surveillance ideology by examining specific empirical examples drawn from media reports of the Snowden affair, in order to nuance the politics, ethics, values and affects mobilized by governments and corporate elites to justify the collect-it-all practices by a *ménage à trois* of "trusted" global networks. It charts this political space as a sphere of action emerging against the backdrop of what we call 'quasi-totalitarian' mechanisms, which are fostered by alignment, collusion and imbrication of the three trusted authoritative networks. The distinct features of this quasi-totalitarianism include: the monopoly of digital planning on surveillance resting on back-channel and secret communication between government, tech corporate elites and, sometimes, NGOs; the role of civil society NGOs as mechanisms for circumventing democratic processes; enterprise association politics that ensures that the dual goal of state (security) and capital (profit) continues unabated and unaccounted; the unprecedented scope in the form of total structural data acquisition by western intelligence matrixes; the persecution and prosecution of journalists, whistleblowers and transparency actors outside the scope of civil society groups; and, the significant if insufficient contestation by members of the public concerning the infringement on civil liberties.

Keywords

Surveillance, ideology, quasi-totalitarianism, Snowden, digital networks.



Figura 1: Restos de um computador que continha arquivos vazados por Edward Snowden ao jornal The Guardian e foi posteriormente destruído a pedido do governo inglês. Fotografia de Roger Tooth

Quem tem informações sobre você? São as empresas privadas, não nós, que sabem de tudo – há um compartilhamento massivo de dados.
Ian Lobham⁴

A reação do público nos Estados Unidos e na Europa sobre as revelações recentes indicando a vigilância e o controle estatal e corporativo tem ido da perplexidade genérica a uma raiva marginal. O público tem sido lento em sua reação e o resultado político dessas revelações ainda terá que ser acompanhado. Governos e elites da tecnologia acusaram uns aos outros de serem responsáveis por uma perda de confiança por parte do público e por comprometerem a privacidade e a integridade das redes em si. Os programas da Agência de Segurança Nacional (NSA) americana foram implementados e estiveram em funcionamento durante anos sem atenção do público ou sem passarem pelo

4 Ex-diretor do Centro de Comunicação do Governo da Inglaterra (Government Communications Headquarters – GCHQ).

apropriado debate. O governo de Barack Obama justificou a implementação dos programas por parte da agência de inteligência militar – a NSA é um setor do Departamento de Defesa americano – dizendo que eles eram cruciais para prevenir ataques terroristas. Essa justificativa foi contestada, o que fez pouca diferença na continuada execução dos mesmos programas. No intercâmbio entre privacidade e segurança os governos têm defendido a necessidade de fazer exceções em relação ao quadro legal vigente com a justificativa de proteger o próprio público.

Enquanto isso, a elite tecnológica manifesta sua exasperação ao mesmo tempo em que continua bem apagada no debate sobre essas práticas situadas no limite entre privacidade e segurança. Com o objetivo de garantir suas próprias fontes de renda e suas reputações como atores corporativos socialmente responsáveis, os capitalistas da tecnologia mantiveram uma atitude que não pode ser considerada inteiramente consistente com o que deveriam ser suas próprias práticas. Um terceiro grupo de origem duvidosa também assumiu um papel de destaque nos debates. As organizações da sociedade civil advogam em favor da transparência e de resoluções pelo acesso aberto, assim como também supervisionam esses tipos de processo chamando para si a voz do público. O envolvimento dessas entidades gerou todo tipo de cruzada em favor de princípios democráticos putativos e pelas garantias constitucionais, que estão sendo evitadas pelos órgãos governamentais.

Essa relação entre as três redes de segurança globais – governos, corporações e ONGs – está de fato tendo o controle do mandato e o poder efetivo no planejamento do campo do digital. Eles se vestem com uma falsa roupagem de representatividade pública e nesse papel usurpam o agenciamento político de integrantes da sociedade. Na verdade, essas três supostas redes de segurança constituem um oligopólio que domina o espaço em que a governança é negociada. Elas relegam a esfera individual à um lugar de marginalidade e à uma posição de aguda precariedade a partir da qual elas acionam uma ameaça à privacidade por parte de agentes de vigilância. E, ainda assim, é

o indivíduo que acaba pagando para ter equipamento, acesso à internet e pelo seu necessário letramento digital e, nesse sentido, depende de compras, conectividade e treinamento. Também é o próprio indivíduo que tem de adquirir a competência e os softwares recomendados para proteger sua privacidade em relação às verdadeiras casas digitais criadas pelas elites tecnológicas e que são supervisionadas pelos governos (em nome da segurança) e pelas corporações (em razão do lucro).

O cidadão é colocado em uma situação impraticável, na qual precisa simultaneamente adquirir as ferramentas para aplicação das garantias legais geralmente atribuídas ao Estado para proteger seus direitos e, ao mesmo tempo, desenvolver outras ferramentas para poder aplicá-las. Nesse ambiente, em que o Estado ameaça a privacidade em nome da segurança, os interesses comerciais estão em conluio com o Estado oferecendo um falso abrigo e as entidades da sociedade civil sequestram a própria possibilidade de uma voz de engajamento político, restando ao indivíduo uma única opção: "hackear ou ser hackeado". É esse, então, o estado precário dos direitos relacionados ao desenvolvimento tecnológico e que inspiram e se apresentam a nós como a motivação para o presente artigo.

Nosso principal objetivo neste artigo é, então, mapear esse espaço político entendido como uma esfera de ação que emerge em contraposição ao que chamamos de mecanismos "quase-totalitários", que sucedem com base em alinhamento de posições, conluio e imbricamento entre as três redes autoritárias de segurança. Esta abordagem dá conta de uma questão perturbadora na articulação das políticas do digital. Trata-se do processo de eliminação de franquias por parte das empresas visando lucro, governos procurando regular os fluxos de informação e grupos da sociedade civil tentando chamar para si uma preocupação legítima dos usuários em benefício de sua própria subsistência política e financeira. A rearticulação do atual cenário político em relação à esfera do digital, em termos da dinâmica que descrevemos, deve ajudar a mostrar também que as transformações tecnossociais nas formas de agenciamento

devem promover a possibilidade de um tipo de associação civil inspirada por uma política democrática radical que seja capaz de contestar as práticas das três mencionadas redes de segurança.

À deriva em campos digitais

As três redes mencionadas (corporativa, governamental e sociedade civil) vivem pelo controle da performance de comunicação individual, mas nenhuma delas foi completamente bem-sucedida. Nem precisamos dizer que essas redes não estão pareadas com atores políticos em particular e são estruturalmente e formalmente similares na lógica de sua forma hierárquica, social e de uma economia política baseadas num desejo reativo. Essas redes autoritárias são propriedades emergentes de uma dinâmica de poder hierárquica com suas propriedades endógenas que podem ser observadas por toda parte.

Caso esse oligopólio de vigilância semicentralizada fosse bem-sucedido no controle assertivo, somente as comunicações com intenções claramente visíveis a essas redes poderiam ser consideradas lícitas. Para o poder governamental isso remonta a uma lógica que transforma todo o ato de comunicação digital em pernicioso a menos que ele se prove como inócuo. Para o poder corporativo, essa lógica remonta à comodificação de cada ato de comunicação digital. E para a sociedade civil, a mesma lógica remonta à capitalização política dos direitos e numa obrigação de engajamento digital por parte do indivíduo diante das duas primeiras redes.

Com o objetivo de demonstrar esse ponto, fazemos uma analogia com o argumento de Hayek em relação ao controle econômico e o totalitarismo. No capítulo 7 de seu livro *Road to Serfdom*, o autor destaca a suposição comum de que o controle econômico não afeta a liberdade. Podemos dizer algo muito similar em relação à suposição comum de que o controle digital não afeta os direitos fundamentais. Isso é o que acontece quando substituímos a palavra

“econômico” por “digital” em uma das passagens mais conhecidas da obra de Hayek (2007, p. 127):

A chamada liberdade digital prometida pelos encarregados do planejamento significa justamente que nós nos liberamos da necessidade de resolver nossos próprios problemas em relação ao digital e deixamos que as amargas escolhas geralmente envolvidas sejam tomadas por nós. Já que na vida moderna dependemos dos meios para praticamente tudo que nossos encarregados fornecem, o planejamento digital envolveria dar informações de praticamente nossa vida toda. Há poucos aspectos dela, desde nossas necessidades básicas ao nosso relacionamento com nossa família e amigos, da natureza do nosso trabalho aos momentos de prazer, sobre os quais os planejadores não exerceriam seu controle “consciente”⁵.

Da mesma maneira que em relação às questões econômicas, nas questões do digital a anuência tácita do agente do poder não verificado dos “planejadores digitais” – na forma de órgãos governamentais nacionais e internacionais, políticas de vigilância perpetradas pelo Estado profundo e a tecnologia desenvolvida por atores corporativos – são mecanismos cruciais em sociedades de controle e devem ser pontos focais de qualquer debate sobre a questão. Os recentes documentos de Snowden e os cabos do Wikileaks de Assange vazados por Manning nos oferecem evidência significativa, apresentada em diversos documentos, de que há uma autoridade transnacional americana reconhecida pelas redes de segurança globais atualmente realizando a vigilância em praticamente toda a rede digital e operando nas sombras.

Essa autoridade informal parece ter a colaboração, ainda que hesitante, das elites corporativas transnacionais da área de tecnologia e, no limite, tem a concordância de atores da sociedade civil que também almejam um papel na

5 Do original: “The so called *digital* freedom which the planners promise us means precisely that we are to be relieved of the necessity of solving our own *digital* problems and the bitter choices which this often involves are to be made for us. Since under modern life we are for almost everything dependent on means, which our fellow men provide, *digital* planning would involve direction of almost our whole life. There is hardly an aspect of it, from our preliminary needs to our relations with our family and friends, from the nature of our work to the use of our leisure, over which the planner would not exercise his ‘conscious’ control.”

governança digital. Devido à crescente e cada vez mais fortalecida formação de um oligopólio para a vigilância, o poder sobre a informação e sobre a comunicação exercido por essa autoridade não é nada menos que o controle tanto do consumo digital quanto de sua produção. Mecanismos similares de controle podem ser encontrados na China e no Irã, por exemplo, atestando que este fenômeno ocorre em escala global.

Interessa-nos, assim, não só o poder e o alcance do oligopólio dos planejadores do digital, mas os tipos específicos de posicionamento ideológico e a lógica de sua necessidade política e comercial implantada para justificar a fonte de seu poder e o motivo de seu exercício. A forma de controle que os planejadores exercem coletivamente sobre as informações e sobre a comunicação fica evidente nos programas de vigilância bem como na implacável repressão governamental em cima de movimentos a favor da transparência e da defesa por novas alternativas.

O entendimento de que tais ações de controle e usurpação direcionam-se “a outros e não a mim” pode servir como confirmação parcial da proposta de Wacquant (2008 apud MCCA HILL; FINN, 2014, p. 4) em relação aos impactos “não solidários” da vigilância “sinóptica” e da vigilância “lateral”. Os indivíduos e grupos que são alvo de vigilância, como imigrantes, manifestantes, crianças em idade escolar e indivíduos sob liberdade condicional, entrevistados por McCahill e Finn (2014, p. 80), embora sofressem com difíceis desafios impostos pela vigilância, puderam desenvolver um capital de vigilância:

Ativistas mais antigos utilizaram seu capital econômico, social e cultural para escapar ou contestar a vigilância que sofriam de diversas maneiras [...] a experiência subjetiva da vigilância foi muitas vezes manifestada em termos positivos, sendo que muitos manifestantes descrevem suas experiências como um “jogo” ou como uma “animação”, ou ainda como “formadora de uma identidade” mais do que em termos de “opressão” ou “coerção”⁶.

6 Do original: “long-term activists utilized economic, social and cultural capital to evade or contest surveillance in various ways...the subjective experience of surveillance was often expressed in positive terms with many protesters

De todo modo, no final das contas do caso Snowden, a noção de não solidariedade desenvolvida por Wacquant fica evidente, enquanto o capital de estratégias de vigilância certamente se desenvolve na população em geral. Isso se explica porque o poder de vigilância não está mais restrito à prevaricação, ilegalidade, resistência ou dissidência. A vigilância tornou-se a condição mesma do engajamento civil na esfera do digital e isso requer uma discussão teórica mais ampla.

Aspectos do totalitarismo

Apesar da alta conceptualização das utopias e distopias digitais, a velha demanda modernista por poder, participação e democracia ainda tem seu valor e, dessa forma, raça, gênero, classe social e outros mecanismos de hierarquização são produzidos e reproduzidos nas redes digitais. O alinhamento das corporações na área de tecnologia, juntamente com as elites governamentais e os atores da sociedade civil, além da anuência passiva do público apontam para uma propensão coletiva que remete a um totalitarismo. Este *ethos* político está baseado no consenso tácito e na prescrição secreta de transparência individual e coletiva. Dessa forma, consideramos que seja importante rever categorias ideológicas e políticas tradicionais que têm dado a diretriz aos complexos de vigilância nos Estados Unidos, Inglaterra e no ocidente em geral, assim como em países onde arranjos sociopolíticos alternativos podem estar em curso. O termo quase-totalitarismo que usamos aqui se inscreve num *continuum* genealógico em debates históricos e políticos na academia, que tentaram lidar com várias formas de autoritarismo e despotismo (Facismo, Nazismo, os regimes soviéticos, ditaduras semiperiféricas na América Latina e a região MENA (médio Oriente e norte da África), pós-totalitarismo e assim por diante), tanto à direita quanto à esquerda.

describing their experiences in terms of 'play', 'excitement', and as 'identity affirming', rather than 'oppression' or 'coercion'."

O princípio totalitário é o seguinte: o estado exerce controle total sobre seus membros. Isso não significa dizer um controle meramente performativo, mas também cognitivo. Tanto os feitos quanto os pensamentos dos cidadãos são determinados pelo poder estatal. O termo, cunhado por Carl Schmitt, em *The Concept of the Political*, corresponde a um estado que, ao abraçar todos os domínios da vida social, gera em última análise uma indistinção entre Estado e sociedade. Num Estado desse tipo, de acordo com Schmitt (1996, p. 22), “tudo é, em princípio, político”. A interpenetração entre o Estado e a sociedade – a hiperpolitização do social – é a característica mais proeminente do totalitarismo. O totalitarismo não é meramente uma forma de autoritarismo em que o poder é exercido de cima para baixo sobre o tecido social. Nesse sentido, Schmitt (1996, p. 24) indica que “um Estado que se posiciona acima da sociedade pode ser chamado de universal, mas não total”⁷.

A permeabilidade mútua dos campos político e social resulta que, no totalitarismo, o *motus politicus* tende a tornar-se – sem nunca ser totalmente – indistinto do *motus socialis*. Os membros de uma sociedade tornam-se individualmente agentes das demandas políticas do Estado e o Estado, por sua vez, torna-se o lugar para a promoção das demandas sociais do coletivo de indivíduos. É importante observar que essa ideia relaciona-se com a ocupação do espaço privado que em todas as formas de totalitarismo está submetida ao escrutínio político e coletivo.

Nesse sentido, o atual alinhamento das redes de segurança e o consentimento dos sujeitos envolvidos aproximam-se das marcas da interpermeabilidade do agenciamento político e social encontrado no totalitarismo. No intento de prever uma atividade terrorista ou criminal perpetrada por organizações ou indivíduos, prevendo práticas mercadológicas ou modificando práticas socioculturais mudando atitudes subjacentes, os governos, as corporações e os atores da

7 Do original: “A state standing above society could be called universal but not total”.

sociedade civil se associam numa explícita e implícita normatização de uma valoração moral da transparência.

Autores como Arendt (1951) e Popper (1971) demonstraram que uma agenda utópica é uma marca indicativa dos totalitarismos. Popper (1971, p. 157) entende os totalitarismos como práticas instrumentais orientadas para a realização do que ele entende como “Estado Ideal”. Totalitarismo é, para ele, um projeto de engenharia utópico baseado na noção de que a vida da pólis é a implementação instrumental de normas orientadas para a concretização do auge da doação política. Para Popper, no limite, o totalitarismo está intimamente relacionado à política entendida como uma soteriologia.

No entanto, as massas – como Arendt (1951) denomina o contingente de indivíduos de quem líderes totalitários esperam uma deposição de fé política – não aderem naturalmente a teologias políticas, mesmo que muito frequentemente o façam. Processos totalitários recrutam e implantam o pensamento de um estado político final que já pode ser encontrado em algum lugar na própria população. Por esse motivo, o agente totalitário faz uso de mecanismos de inculcação. A propaganda é central para a construção do imaginário político de um público (ARENDR, 1951). Mecanismos de inculcação são centrais para Estados totalitários e devem ser amplamente compreendidos como processos longitudinais de controle cognitivo. A propaganda não mira o que os indivíduos fazem, mas o que esses indivíduos pensam e sentem. A propaganda é preparada para introduzir nas massas um compromisso de fé com o “Estado Ideal”. Por fim, então, a vigilância de ações de comunicação não é uma mera forma de sondagem, de predição e prevenção de certos atos, mas é sim uma maneira de testar a eficiência da propaganda na medida em que ela avalia o conteúdo de pensamentos e sentimentos. Dessa forma, o totalitarismo de Friedrich e Brzezinski (1956) inclui os seguintes aspectos principais: ideologia do perfeito estado final da humanidade, um único partido massivo hierarquizado, controle monopolizador da área militar e das comunicações, controle policial terrorista, controle central e direcionamento da economia. Em Deleuze e Guattari (1983)

é a máquina estatal que captura os fluxos sociais decompondo suas conexões horizontais ao longo do caminho.

O consenso de nossas três redes de segurança, com a anuência tácita dos usuários lembra muitos aspectos dos mecanismos totalitários que descrevemos. Por exemplo, na maior parte das comunidades políticas a emergência de um amplo consenso político indica a emergência de um *status quo* que demarca o centro gravitacional dessa mesma política. Na verdade, o consenso tácito conta com a subjacente fusão do *motus politicus* com o *motus socialis*. Enquanto o século XX assistiu a esse tipo de junção em propostas de pureza nacional e de exclusividade etnocultural, sob os quais procuraram construir o “Estado Ideal”, no descenso do século XX e início do século XXI, correntes neoliberais e social-democratas transformaram-se nos direcionadores do “Estado Ideal”, que têm permeado todos os aspectos do tecido social. Desde meados no século XX, mesmo nos Estados mais despóticos, a construção ideológica do “Estado Ideal” vem se apresentando em variações desses dois imaginários sociopolíticos. O novo e estranho animal político é algo entre as linhas de uma versão neoliberal do totalitarismo: um quase-totalitarismo.

Quase-totalitarismo e a opressão do consenso tácito

Os centros de planejamento digital e de redes de vigilância estão embebidos numa ideologia que apresenta aspectos marcadamente totalitários, mas que não são instantaneamente reconhecíveis como parte de eventos históricos, regimes e práticas políticas que, ao longo do século XX, foram construídos em cima da politização total da vida cotidiana.

Há duas importantes variantes. O quase-totalitarismo *não depende da formação de um* “Estado Ideal”, embora as justificativas para as medidas políticas criadas e implantadas nas redes sejam apresentadas como instrumentos destinados a um fim crítico: segurança, crescimento ou melhoria nos hábitos socioculturais. No entanto, um impedimento está em operação no

alinhamento entre as três redes, numa ampla medida, é a sociedade civil que sistematicamente recorre a um discurso de “Estado Ideal” para promover suas próprias pautas. Dificilmente encontraremos usuários que sinceramente optam por uma abordagem maniqueísta para a esfera da vida digital. O que é mais provável é que os atores do setor público insistam em retratar a esfera digital ou como um sonho utópico ou como um pesadelo distópico.

A segunda maneira pela qual o quase-totalitarismo se difere de seu antecessor diz respeito à direção da construção de um consenso ideológico. Com exceção da sociedade civil, as “redes de segurança” não estão envolvidas no negócio de barganhar uma narrativa de um “Estado Ideal” futuro. As corporações, como instituições privadas, querem simplesmente promover seus produtos e serviços além de sustentar as condições que as levaram à prevalência comercial. Agências governamentais operando nas sombras não precisam de consentimento das massas. Trata-se mais da estratégia de consenso político do centro totalizador que arma os esquemas planejadores das redes.

É a emergência do consenso central entre os atores da sociedade civil que parece ditar a construção ideológica do poder e não o contrário. Nesse sentido, o quase-totalitarismo recruta e implanta alguns dos mecanismos inerentes aos processos democráticos. De certa maneira, as regras são do povo. E ainda assim, como no totalitarismo, há um movimento em direção à interpenetração do social e do político. Talvez o mecanismo mais esclarecedor que deve ser ressaltado é o reforço banal das políticas que ajudam a propagar o consenso sociopolítico do centro.

A repetição banal das tarefas que são designadas pelas redes de segurança parecem ter pouca ou mesmo nenhuma conexão com a determinação das práticas políticas – abrir o *laptop* de alguém, fazer *login* numa rede, enviar uma mensagem pelo celular etc. – está aí a acumulação de ações que os indivíduos realizam de maneira não efetiva para sustentar um *status quo* e seu mecanismo de coesão sociopolítica. A preservação e promoção do *status quo* significa também a apresentação e promoção do centro. Nas práticas da esfera

digital esse híbrido ideológico é vendido pelo amplo e coletivo centro na forma de redes centralizadas que negociam suas respectivas necessidades de vigiar, lucrar e talvez, curiosamente, também atua em nome de uma liberdade putativa dos usuários.

Formas de associação no quase-totalitarismo

A diferença entre o papel ideológico que o “Estado Ideal” possui no modelo totalitário e no modelo quase-totalitário pode ser melhor explicada pelas duas abordagens de Michael Oakeshott sobre projetos políticos em *On human conduct*. Para Oakeshott (1975), a questão está numa noção aristotélica da comunhão na pólis, em que podemos ver melhor como a relação entre pares sustenta uma associação política impermeável à instrumentalidade. Em oposição a uma entidade empresarial que se reúne para garantir a realização de um lucro, conquistar produção etc. – a comunhão em torno da civilidade pode se sustentar sem a necessidade de um objetivo comum. De acordo com Oakeshott, a associação civil (a comunhão pela civilidade) está baseada na coerência interna do reconhecimento mútuo e na completude por um ser membro do grupo do outro (1975, p. 110).

Cada uma dessas redes de segurança emerge da junção de grupos que têm propósitos substanciais manifestos e externados. O grupo corporativo remonta a um “pacto pelo descarte”. Isso significa dizer que há um agrupamento instrumental dos agentes. O governo é uma reunião de associações cujo projeto é deter a administração (ecônomos) enquanto os atores da sociedade civil são essencialmente associações ligadas a projetos políticos – no sentido vulgar do termo. Ao mesmo tempo, a ideia de preservação de uma comunidade de reconhecimento mútuo e de pertencimento que – ao menos em teoria – supõe-se que as redes destinam-se a preservar e promover. É a ideia integrativa do centro que preenche nessas redes o papel da justificativa que antes era do “Estado Ideal”. Mas nesse “Estado Ideal”, para além de ser extrínseco –

relacionado a um futuro utópico – ele está num sentimento que já foi atingido e deve ser preservado.

A ideia integrativa do centro justifica então uma grande quantidade de suspensões dos instrumentos legais e políticos batalhados a duras penas e que vêm sendo empregados justamente para garantir a civilidade do consenso do centro. As redes de segurança justificam a violação supostamente intermitente da privacidade, a livre associação, a liberdade de expressão através da afirmação da necessidade instrumental de aquisição de dados estruturais, da vigilância, de infringir as redes digitais, somado à disrupção da segurança computacional e da encriptação.

No contexto de sociedades intensamente ligadas em rede, esse dados não têm sido suficientes para reunir argumentos em relação ao constitucionalismo e aos princípios democráticos e contra o controle de *big data* e das infraestruturas das redes digitais pelo Estado, pelos atores corporativos e pelos atores da sociedade civil que colaboram em ações de governança. Parece-nos óbvio que a máquina das redes digitais está enredada nos ambientes de rede controlados pelo Estado e pelas corporações em conjunto com as redes da sociedade civil, que certificam seu comportamento oferecendo algo como um controle com qualidade política. Nesse sentido, a associação na esfera pública digital está sendo realizada em grande parte dentro do confinamento das plataformas corporativas (orientadas por seu projeto), mesmo quando essa associação inclui funções civis, como a participação política e o diálogo, como é o caso dos atores da sociedade civil.

A recuperação das histórias de um vasto catálogo de violações legais que têm inundado a esfera pública, como resultado do vazamento feito por Snowden, mostra que os princípios legais sobre os quais a vida democrática foi constituída *não* vêm sendo suficientemente protegidos das motivações secundárias das três redes reunidas. Dentro do contexto desse debate, o termo quase-totalitarismo explica a similaridade com as práticas de coleta total de informações por parte dos governos e dos atores corporativos com as práticas do passado sem tornar trivial as experiências históricas de totalitarismo.

Ademais, em outro nível, o quase-totalitarismo do centro, aponta para o “centro” do espectro político. Tradicionalmente, o centro tem sido ocupado por liberais e social-democratas de algum tipo ou ainda por outros sistemas democráticos. No entanto, o centro ideológico em Estados não democráticos é, por sua vez, o centro ideológico no espectro específico da cultura política nos contextos específicos do país. O quase-totalitarismo do centro refere-se aqui, então, a uma segunda camada na relação com as organizações hierarquicamente centralizadas, mesmo se elas estiverem ligadas em rede, porque a lógica sociopolítica permanece hierarquizada independentemente do uso das comunicações em rede. Os centros para o planejamento do digital e as rede de vigilância são quase-totalitárias por essência.

Esse é justamente o motivo pelo qual liberais e social-democratas, parlamentares e outros personagens do centro ideológico ocidental entendem como absurda a sugestão de que uma vigilância ubíqua (o controle dos planejadores do digital sobre as redes globais) seja uma prática totalitária. Essa versão do totalitarismo adquire seu conteúdo ideológico a partir do centro do sistema político. Nesse sentido, complexos de vigilância são a descendência genealógica direta e retratam uma ideologia política dominante em qualquer sistema político.

No entanto, o paradoxo presente nesse cenário é que nem o neoliberalismo nem a social-democracia, que são as duas ideologias dominantes nos Estados democráticos contemporâneos, são as ideologias pelas quais o controle digital é *exercido* na prática. Quem pode esquecer Chris Hune, secretário de Estado para Energia e Mudança Climática entre 2010 e 2012 e sua exasperação por não ter ideia das atividades realizadas pela GCHQ? “Cabinet não foi informado de nada sobre isso” (HOPKINS; TAYLOR, 2013). O quase-totalitarismo baseia-se num projeto de associação específico para florescer, diferente de associações civis, que até pouco tempo era o tipo ideal mais comum de associação na política representativa tradicional e jogava a favor ou contra o totalitarismo de esquerda, de direita e contra as variações liberais e social-democratas do passado.

Associações civis, como uma forma de autenticação da prática entre as práticas, que não têm um propósito corporativo agregado, a não ser manter uma política aberta e dar sequência à discussão, podem servir tanto como uma resposta à crítica apresentada aqui quanto uma nova visão poderosa para a coisa pública em rede, que atualmente está dominada por uma conduta humana direcionada principalmente em relação a formas de associação empresarial.

O conflito é explicitado brevemente por Noel O'Sullivan (2012, p. 310) que sublinha a existência de uma "tensão entre a regra da lei à qual a associação civil está atrelada e sua subordinação aos poderes administrativos de governos inclinados a impor concepções de uma boa sociedade"⁸. É importante frisar o fato de que o princípio de civilidade que está implicado nas afirmações políticas e nas proposições do centro é sempre, senão regularmente, cooptado por associações empresariais que apresentam seus próprios objetivos como necessidades instrumentais para a preservação das associações civis.

Assim, num certo sentido, a tarefa que temos nas mãos para a radicalização de um modelo democrático é acabar com a usurpação das associações civis que estão nas mãos de corporações. Em outras palavras, o trabalho consiste em resistir articulação da comunhão pela civilidade como um modelo que está em perigo e cuja guarda pode ser muito rapidamente confundida com um "Estado Ideal". A comunhão pela civilidade não é um estado de realização como o da obtenção de lucro ou o fim de um conflito. Ela é, de outro modo, uma forma de atuação política e dessa forma não pode ser aprisionada num "Estado Ideal" sem que se negue sua natureza não instrumental.

Na verdade, como Noel O'Sullivan aponta, uma leitura dedicada das noções de civilidade em Oakeshott em face de uma instrumentalização do político pode servir bem para a rearticulação de uma comunhão democrática contra o impacto

8 Do original: "a tension between the rule of law to which civil association is committed and the subordination of it to the administrative powers of governments bent on imposing substantive conceptions of the good society".

e a usurpação da civilidade pela intrusão política de associações empresariais. O autor (O’SULLIVAN, 2012, p. 306) diz:

Chantal Mouffe, um crítico simpático a Oakeshott, sugere que a preocupação muito estreitamente elaborada do autor em relação a associações civis pode ser superada realocando o modelo civil por um quadro democrático radical que encorajaria uma participação ativa na política e dessa forma removeria a confiança de Oakeshott no que pode provar ser um consenso minoritário sobre tais formas e procedimentos⁹.

De maneira significativa, o perigo de não se reconhecer a transformação da sociedade civil num Estado empresarial é um problema crucial na política contemporânea.

Ainda que a transformação de um Estado civil em empresarial possa ser aceitável ocasionalmente, na medida em que se faz necessário defender ou manter a associação civil em si mesma, o preço a ser pago deve ser reconhecido claramente: ele está em que a regra da lei cessa de ser o laço entre os cidadãos e assim o estado, nessa condição, não é mais livre¹⁰. (O’SULLIVAN, 2012, p. 296)

A conduta de Snowden como associação civil

Edward Snowden vazou centenas de milhares de documentos da Agência de Segurança Nacional (NSA) americana e posiciona-se contrário à associação empresarial. Sem desconsiderar o tom conspiratório, a resposta do coletivo Anonymous à tentativa de Snowden em colocar o tema da vigilância para o debate

9 Do original: “Chantal Mouffe, a sympathetic critic, has suggested that Oakeshott’s narrowly conceived concern with civil association might be overcome by *relocating the civil model within a radical democratic framework* that would encourage active participation in politics, thereby removing Oakeshott’s reliance on what may prove to be a minority consensus about forms and procedures”.

10 Do original: “Even though the transformation of a civil into an enterprise state may be acceptable on occasion, insofar as it is necessary to defend or maintain civil association itself, the price to be paid must be clearly recognized: it is that the rule of law ceases to be the bond of citizens, and thus the state, for the time being, is no longer a free one”.

público mostra muito dolorosamente a reação a revelações pelos movimentos que, instintivamente, se opõem aos modelos quase-totalitários da esfera pública digital:

Sua privacidade e liberdade estão sendo lentamente tiradas de vocês, em encontro a portas fechadas, em leis enterradas em cartas legais, as pessoas que supostamente deveriam estar te protegendo [...] Faça o download desses documentos, compartilhem, reflitam sobre eles, não deixem que eles façam-nos desaparecer. Espalhem amplamente e para longe. Deixem que essas pessoas saibam, que nós não seremos silenciados, que não irão tirar vantagem de nós e que não estamos satisfeitos com essa espionagem sem garantias, desnecessária, sem ética de nossas vidas privadas para o ganho monetário de 1%¹¹ (ANONYMOUS..., 2013).

Neste comunicado, Anonymous sempre retrata a si mesmo como o garantidor de valores da sociedade civil, como protetor da comunhão pela civilidade. É compreensível que a articulação de compromisso com essas redes não seguras está avançando em termos morais, e muito frequentemente eles se apresentam como um novo ator clandestino que se dispõe como a vigilância política global com o objetivo de fazer resistência contra a vigilância, a censura, perseguir injustiças e a corrupção e em solidariedade com os movimentos que lutam contra governos repressivos e autoritários. Anonymous e Snowden servem para demarcar um espaço de resistência em relação aos mecanismos ocultos da corrente penetração política do social e ao fazer isso desvendam mecanismos totalitários a que ambos dizem resistir.

De acordo com o jornal *The Guardian* (HUET, 2013), uma das principais organizações de mídia com a qual Snowden colaborou, o programa Prism da NSA é o maior gerador individual de relatórios de inteligência que o americano vazou. Prism era um programa menor, o que significa que a Agência coletou dados do Google, Facebook, Apple, Yahoo e outros gigantes americanos. Um dos slides mostrava que

11 Do original: "Your privacy and freedoms are slowly being taken from you, in closed door meetings, in laws buried in bills, and by people who are supposed to be protecting you [...] Download these documents, share them, mirror them, don't allow them to make them disappear. Spread them wide and far. Let these people know, that we will not be silenced, that we will not be taken advantage of, and that we are not happy about this unwarranted, unnecessary, unethical spying of our private lives, for the monetary gain of the 1%".

a Agência tinha acesso direto aos servidores dessas empresas. Essa informação tem sido, contudo, altamente questionada pelas gigantes da tecnologia, que afirmam que apenas cumpriram com determinações legais ao pedirem dados de usuários. Os documentos também revelam a existência do Tempora, um programa iniciado em 2011 pelo GCHQ inglês. Esse programa reúne dados massivos de tráfego de dados por celular e internet recolhidos de cabos de fibra óptica. GCHQ compartilhava a maior parte das informações coletadas com a NSA.

Os documentos, classificados como altamente secretos, emergiram juntamente com outras revelações de alta monta atribuídas a Snowden a partir do momento que ele inicia sua colaboração com o *Guardian* através de artigos que começam a ser publicados em 6 de junho de 2013. O governo dos Estados Unidos tem, desde então, enquadrado Snowden no *Espionage Act*, que o forçou a pedir asilo para não menos que 20 nações. Ironicamente, ao fim, foi Putin quem concedeu e ofereceu asilo.

O relacionamento entre a NSA e as gigantes da tecnologia é realmente complicado. De acordo com o *The Guardian*, a partir de julho de 2010, dados do Yahoo foram responsáveis por gerar o maior número de relatórios da inteligência da NSA. Na sequência são citadas a Microsoft e depois o Google. Todas as três companhias estão em batalhas legais para revelar números mais precisos em relação aos pedidos de dados que receberam por parte das agências de inteligência dos Estados Unidos. A Agência está autorizada a caminhar “três passos” de distância em relação ao seu alvo – que poderia ser pessoas “que falam com pessoas que falam com pessoas que falam com você”. No Facebook, em que o típico usuário tem 190 amigos, os níveis de separação entre eles dão ao usuário acesso a uma população do tamanho do estado do Colorado (aproximadamente 5.260.000 pessoas).

De acordo com documentos internos citados pelos jornalistas, a Microsoft “desenvolveu uma capacidade de vigilância” que foi iniciada para “lidar” com as autoridades federais que se mostravam preocupadas com o fato de que não poderiam grampear mensagens encriptadas enviadas pela *web* em tempo

real. A reposta do vice-presidente da Microsoft, John Frank foi: "Nós seguimos acreditando que nos é permitido publicar o que é necessário para ajudar a comunidade a entender e debater essas questões" (RT, 2013).

Dois grupos franceses ligados aos direitos humanos deram entrada a uma queixa legal contra a Agência de Segurança Nacional americana, contra o FBI e contra sete empresas de tecnologia que eles acusam de terem ajudado os Estados Unidos a bisbilhotar os e-mails e as ligações telefônicas de cidadãos franceses. A queixa relaciona os métodos de espionagem americanos, como foram revelados por Snowden, e se dirige a "pessoas desconhecidas", mas menciona Microsoft, Yahoo, Google, Paltalk, Facebook, AOL e Apple "como cúmplices em potencial" da NSA e do FBI. A Federação Internacional de Direitos Humanos (FIDH) e a Liga Francesa pelos Direitos Humanos (LDH) defendem que "essa flagrante intrusão nas vidas dos indivíduos representa uma séria ameaça às liberdades individuais e se não for detida pode levar ao fim de determinações legais" (HUET, 2013).

Os relatórios apontam ainda para "alianças feitas com mais de 80 grandes corporações globais que apoiam a missão de ambos". No jargão da NSA, "missão de ambos" refere-se à defesa das redes nos Estados Unidos, por um lado, e ao monitoramento das redes pelo mundo, por outro lado. As empresas envolvidas no caso são empresas de telecomunicações, produtoras da infraestrutura das mesmas redes, produtoras de softwares e empresas de segurança (POITRAS et al., 2013).

Mark Zuckerberg, presidente do Facebook, e Marisa Meyer, presidente do Yahoo, defendem suas empresas contra as críticas que implicam as companhias de tecnologia de se interporem muito pouco contra a vigilância perpetrada pela NSA. Meyer diz que os executivos estariam ameaçados de prisão se revelassem segredos governamentais. O Yahoo processou a corte da vigilância de inteligência internacional (FISA) sem sucesso, o que fornece um precedente legal para a vigilância realizada pela NSA. Em 2007, o Yahoo pediu permissão para publicar detalhes dos pedidos recebidos pela agência de espionagem. Meyer declarou que "quando você perde não pode ir em frente, é traição. Nós acreditamos que faz mais sentido trabalhar no interior do sistema"; enquanto Zuckerberg por sua vez disse que o governo havia

feito um “trabalho ruim” entre balancear a privacidade das pessoas e cumprir seu dever de protegê-las com uma frase que agora já se tornou famosa: “Francamente eu acredito que o governo ferrou tudo” (RUSHE, 2013).

A escalada das tensões entre as corporações e os governos, seja ela verdadeira ou fabricada para o consumo do público, aponta para processos de tomada de decisão que claramente estão para além dos métodos e princípios de governança democrática. Elas envolveram negociações ocultas entre os Estados e as elites corporativas sob um véu de sigilo garantido por provisões legais que impediram a divulgação de informações mesmo sobre a existência dos próprios pedidos feitos pela NSA. Isso seria traição, como Meyer justifica.

A campanha “*Stop watching us*” (Pare de nos espionar) e a campanha global de 11 de fevereiro contra a vigilância, além dos grupos pela privacidade, como Electronic Privacy Information Center e Electronic Frontier Foundation entraram com processo que resultaram na abertura de centenas de páginas da seção 215 de intimações da FISA, que desde 1988 deu autorização ao governo – com aprovação prévia das cortes – para obter os registros de investigações de inteligência em curso pelo mundo. A vigilância da GCHQ e da NSA está enfrentando hoje um desafio legal diante da Corte Europeia de Direitos Humanos, Big Brother Watch, English PEN e o Open Rights Group. O Google, a Microsoft e a Yahoo estão sofrendo retaliação por parte de seus usuários nos Estados Unidos e pelo mundo contra a vigilância em massa e estão lutando para terem permissão de serem mais transparentes sobre seus entraves com as agências de inteligência. Essas empresas, juntamente com o Facebook, a Apple e a AOL também se reportaram ao Senado numa carta aberta exigindo uma reforma do sistema. De fato, uma revisão feita pelo governo Obama foi conduzida como uma resposta, mas satisfaz pouco as críticas em curso.

Governos de democracias liberais operam sob estatutos que proíbem a espionagem conduzida sobre suas próprias populações. No entanto, como indicado no estudo de larga escala realizado pelo Center for European Policy Studies, publicado em novembro de 2013, a solidez das provisões e a eficiência

dos mecanismos de varredura para garantir a lei varia de país para país. Referindo-se a um artigo publicado no *The Guardian* em agosto do mesmo ano, o estudo indica:

Isso aponta para um potencial cenário de compra da privacidade das pessoas pelos serviços que exploram regimes com uma proteção/varredura mais fraca ou com as maiores brechas legais. Esse cenário é até certo ponto refletido nos relatórios que indicam que a GCHQ fez propaganda de si própria para a NSA com base no fraco regime regulatório e de varredura existente no Reino Unido. (BIGO et al., 2013, p. 17)

É vedado aos governos espionarem suas própria populações, mas eles podem espionar estrangeiros. Os Estados Unidos entendemos que são parceiros do Reino Unido, da Austrália, do Canadá e da Nova Zelândia (The Five Eyes) e outros países como Alemanha, França, sobre os quais ele pode espionar. Isso acabou por incluir a União Europeia e o telefone celular de Ângela Merkel:

Num dia normal a NSA monitorou cerca de 20 milhões de conexões telefônicas alemãs e 10 milhões de pacotes de dados de internet, subindo para 60 milhões de conexões telefônicas num dia cheio, diz o relatório. [...] Na França, o Der Spiegel reportou que os Estados Unidos têm acesso a 2 milhões de conexões de dados por dia. Somente o Canadá, a Austrália, a Grã-Bretanha e a Nova Zelândia foram explicitamente poupadas de ataques de espionagem¹². (REUTERS, 2013)

Ainda assim, a reação nas capitais europeias em relação às atividades de espionagem dos Estados Unidos e do Reino Unido tem sido menor que o esperado. O presidente francês François Hollande condenou a prática dizendo que “Não podemos aceitar esse tipo de comportamento vindo de parceiros e aliados” e que hackear não era necessário pensando em esforços contra o terrorismo. “Eu não acho que haja uma preocupação em nossas embaixadas

12 Do original: “On an average day, the NSA monitored about 20 million German phone connections and 10 million internet data sets, rising to 60 million phone connections on busy days, the report said. ... In France, Der Spiegel reported, the United States taps about 2 million connection data a day. Only Canada, Australia, Britain and New Zealand were explicitly exempted from spy attacks”.

ou da União Europeia em geral de que esse risco exista” (SCHOW, 2013). Os alemães ficaram assistindo enquanto a Chanceler praticamente nem protestava contra as revelações. Num artigo publicado pelo *Der Spiegel*, “A Chanceler e a NSA: Merkel abandonou os alemães”, o autor defende que

trata-se da nossa lealdade à América. Ou de terrorismo internacional. Ou mesmo do papel dos serviços de inteligência. Todos temos uma opinião sobre o fato. Trata-se de nossos direitos sendo violados sem que tenhamos chance de resistir. Paramos de ser cidadãos para sermos assunto¹³. (AUGSTEIN, 2013)

Um segundo mecanismo que parece ter sido utilizado para criar essas matrizes de vigilância, além da explicação de brechas legais por um feudo da inteligência supranacional foi o favorecimento econômico entre as próprias agências:

A agência de inteligência GCHQ britânica pode espionar todos menos cidadãos britânicos, a NSA pode conduzir vigilância sobre qualquer um menos em americanos e a BND alemã pode espionar a todos menos alemães. É dessa forma que uma matriz foi criada atingindo uma vigilância sem fronteira pela qual cada parceiro opera numa divisão de trabalho¹⁴. (POITRAS, et al., 2013)

Num sentido mais amplo, a lógica da vigilância liderada pelo governo americano e executada dentro dessa matriz de feudos da inteligência internacional é uma lógica de guerra de inteligência. É razoável, então, que o órgão central que implementa a estratégia de vigilância, a NSA, teria de ser uma unidade de inteligência militar. Tanto o sistema como seus atores que levaram o programa da NSA adiante eram, não surpreendentemente, pessoas que vieram da guerra

13 Do original: “and this about our loyalty to America. Or international terrorism. Or even the role of intelligence services. Everyone has their own opinion about that. This is about our rights being violated without us being able to resist it. We stop being citizens and turn into subjects”.

14 Do original: “Britain’s GCHQ intelligence agency can spy on anyone but British nationals, the NSA can conduct surveillance on anyone but Americans, and Germany’s BND foreign intelligence agency can spy on anyone but Germans. That’s how a matrix is created of boundless surveillance in which each partner aids in a division of roles.”

do Iraque. Greenwald, um dos jornalistas que trouxe a história de Snowden para a visibilidade pública discute o perfil do ex-diretor da NSA, General Keith B. Alexander no *Washington Post*:

O *Post* esclarece como Alexander assumiu uma abordagem de “coleta total” para as operações de vigilância que eram originalmente direcionadas aos iraquianos no meio de uma guerra e que foi posteriormente transferida e é hoje direcionada à população civil dos próprios Estados Unidos e também ao mundo em geral: [...] E, como ele fez no Iraque, Alexander forçou a barra para ter tudo o que podia: ferramentas, recursos e apoio legal para coletar e armazenar vastas quantidades de informação *não trabalhada em relação às* comunicações nos Estados Unidos e fora dele¹⁵.

A subversão da lei, a perversão da regra democrática e a suspensão da cultura deliberativa não foram meramente apontadas por pesquisadores, por europeus e por formadores de opinião. Rendendo-se à pressão dos atores da sociedade civil, que sentiram o cheiro de sangue e se prepararam para um frenesi de embate político, e às corporações tentando resgatar suas reputações e a lealdade de seu público, Obama realizou uma das declarações mais notáveis de arrependimento não arrependido da história política:

Pedi uma revisão dos nossos programas de vigilância. Infelizmente mais do que um processo ordenado e legal para debater essas questões e chegar às reformas apropriadas, repetidos vazamentos de informações sigilosas deram início ao debate de uma forma muito apaixonada, mas nem sempre compactamente informada. [...] Estou também ciente de que essas questões estão sendo observadas para além do nosso território porque a liderança americana no mundo depende de um exemplo de democracia americana e de abertura americana, isso é o que nos difere em relação a outros países, não somente nossa habilidade de assegurar nossa nação. É a maneira como fazemos, com um debate aberto e num

15 Do original: “the *Post* explains how Alexander took a “collect it all” surveillance approach originally directed at Iraqis in the middle of a war, and thereafter transferred it so that it is now directed at the US domestic population as well as the global one.... nd, as he did in Iraq, Alexander has pushed hard for everything he can get: tools, resources and the legal authority to collect and store vast quantities of raw information on American and foreign communications.”

processo democrático¹⁶. (FRIEDERSDORF, 2013)

Temos todas as evidências do contrário. Os programas de inteligência militar empregados contra civis internamente e pelo mundo foram completamente faltosos em relação a um debate aberto e um respeito pelos procedimentos regulamentares que subjazem ao exercício democrático.

A legalidade putativa dos programas mostrou simplesmente que a estrutura da jurisprudência dos Estados Unidos simplesmente se mostrava repleta de brechas e de subterfúgios que erigiram um estado de exceção justificado pela chamada guerra contra o terror, dando cobertura legal para as práticas e policiamento que haviam sido inteiramente desconsideradas, como a tortura, o desaparecimento e a prisão escondida e que agora estavam novamente sendo empregadas para justificar o maior sistema de violação de privacidade que o mundo jamais tinha visto.

A terceira rede: as ONGs

Beneficiárias desse desastre são os atores da sociedade civil que, como no caso do resultado final do terremoto catastrófico que destruiu o Haiti, agora também estavam perfeitamente posicionadas para tirar vantagem da oportunidade momentânea. Sob a rubrica de serem entidades das sociedades civis, tais grupos, que são na maioria das vezes associados a uma rede semicoberta de entidades americanas e europeias, dispensam o dinheiro de qualquer ator corporativo rico, projetando a si mesmas como uma voz certa das associações civis e da comunhão para a civilidade. O alcance político desses grupos pode ser avaliado com base na elaboração de instituições que são diretamente dependentes do suporte financeiro e organizacional das outras duas redes mencionadas.

16 Do original: "I called for a review of our surveillance programs. Unfortunately, rather than an orderly and lawful process to debate these issues and come up with appropriate reforms, repeated leaks of classified information have initiated the debate in a very passionate but not always fully informed way. ... I'm also mindful of how these issues are viewed overseas because American leadership around the world depends upon the example of American democracy and American openness, because what makes us different from other countries is not simply our ability to secure our nation. It's the way we do it, with open debate and democratic process".

Por exemplo, Hivos, fundador de ONGs que trabalham na área de cibersegurança, entre outras questões, tem financiamento regular vindo do governo holandês. O Departamento de Estado tem uma longa lista de iniciativas e de linhas de financiamento para grupos que promovam os princípios democráticos e os direitos humanos. A Fundação Ökotárs, que dispensa verba do governo norueguês foi acusada pelo governo de Fidez, na Hungria, de participar da licitação de governos de outros países. Esses dados, além da queda de ONGs em países como Rússia, Egito e Azerbaijão mostra que, longe de serem entendidas como membros da sociedade civil de seus respectivos países, esses grupos são vistos como agentes estatais e corporativos por governos não amistosos.

Talvez um dos casos mais interessantes de usurpação e ocultamento dos interesses corporativos e governamentais sob a fachada da associação civil seja o caso da ascensão súbita de Pierre Omidyar ao parnaso dos financiamentos parapolíticos. Tendo começado suas atividades filantrópicas no fim da década de 1990, quando chega a 2014, Omidyar já tinha doado um bilhão de dólares para todo tipo de organizações e projetos. Só em 2013, suas organizações doaram 225 milhões de dólares. Para as doações pessoais, o financiamento é feito através de três organizações: Omidyar Network Fund, HopeLabs, e Humanity United. Michael Gentilucci (2014) da Inside Philanthropy aponta que “estamos lidando com um arquipélago nesse caso, não com terra firme, e a entidade que se sobressai é The Omidyar Group”. Tal grupo é uma organização sem fins lucrativos.

Entre as organizações fundadas por Omidyar temos Change.org; Center on Democracy, Development, and the Rule of Law; Global Integrity; Fundacion Ciudadano Inteligente; Global Voices; Media Development Investment Fund; The Open Data Institute; Open Government Partnership; Project on Government Oversight (POGO); Sunlight Foundation; The Transparency and Accountability Initiative; The Foundation for Ecological Security; Endeavor Foundation e a Ashoka.

Omidyar – cujo registro de atividade nos Estados Unidos inclui contribuições para a campanha presidencial de Wesley Clark e um coinvestimento na CIA, como forma de capital de risco, na IN-Q-TEL e com Booze Allen Hamilton (subcontratado

pela NSA e antigo empregador de Edward Snowden) – tornou-se o guardião dos documentos de Snowden. Com um capital inicial de 250 milhões de dólares, Omidyar começou a erigir ele mesmo uma rede de mídia, em 2013, intitulada First Look Media. Os três primeiros profissionais que ele contratou foram Glenn Greenwald, Laura Poitras e Jeremy Scahill. Seguindo o padrão organizacional de seu trabalho filantrópico, a First Look Media gerou, em cerca de apenas alguns meses, uma estrutura de mídia secundária sob o nome de The Intercept, que foi lançada em 2014. A publicação on-line destinava-se a publicar os documentos de Snowden e produzir “jornalismo destemido e de oposição passando por uma grande variedade de temas” (RICE, 2014).

Enquanto a questão da legitimidade da intervenção política das fundações e das ONGs tem sido uma questão permanente nos debates sobre atores não governamentais e fundações, a peculiaridade desse novo cenário mostra que são precisamente as ONGs armadas com poderio financeiro de partidos políticos que agora exercem poder consultivo sob o disfarce de legitimar os representantes da sociedade civil. Dessa forma, elas prestam um serviço valioso a corporações e agentes governamentais interessados em contornar princípios democráticos de governança e de administração pública.

Considerações finais

A fotografia dos servidores destruídos (Figura 1) que guardavam os papéis da NSA nos porões do *The Guardian* nos parece totalmente incompatível com os princípios e processos de um Estado democrático. Ele mais parece algum dos piores aspectos dos mecanismos de controle do século XX utilizados por regimes totalitários. A destruição dos canais de informação – cartas, livros, gravações etc. – foram instrumentos críticos para o controle das interpretações políticas. Na verdade, é o próprio Edward Snowden quem melhor explicou o espectro político dessa empreitada e o objetivo dessa conduta e de um inimigo ideológico confesso:

No dia 12 de julho de 2013 Edward Snowden encontrou-se com um grupo de organizações de direitos humanos em seu refúgio temporário

no aeroporto internacional de Sheremetievo, em Moscou. Alguns dos argumentos que ele usou foram os seguintes: "Através dessa conexão de trabalho com a Agência de Segurança Nacional, Snowden descobriu que 'tinha a possibilidade de, sem nenhuma restrição de pesquisar, capturar e ler comunicações. As mensagens de qualquer um em qualquer momento. Esse é o poder de mudar o destino das pessoas. Snowden também chegou à conclusão de que o uso diário dessa capacidade por parte da NSA era 'uma séria violação da lei'. A Quarta e Quinta Emendas da Constituição do meu país, o Artigo 12 da Declaração Universal dos Direitos Humanos e diversos estatutos e tratados proíbem tais sistemas massivos, invasivos de vigilância". "Meu governo [dos Estados Unidos] defende que normas sigilosas da corte, que o mundo não está autorizado a conhecer, de alguma forma legitimam esse caso ilegal [...] O que é imoral não pode ser transformado em algo legal através do uso de uma lei sigilosa". Consternado com essa situação, Snowden apoiou-se no princípio de Nuremberg, de 1945, que diz 'Os indivíduos têm deveres internacionais que transcendem as obrigações de obediência nacional. Dessa maneira, cidadãos têm o dever de violar as leis domésticas com o intuito de evitar crimes contra a paz e a humanidade'. Concluindo que o real e potencial acesso sigiloso da NSA nas comunicações de praticamente a totalidade dos americanos e sobre um grande número de não cidadãos era criminosa por natureza (talvez um totalitarismo sendo articulado), ele vazou informações sigilosas que trariam as atividades da NSA ao conhecimento público. "Essa decisão moral de trazer a público sobre uma espionagem que afeta a todos nós tem sido custosa, mas foi a coisa certa a ser feita e eu não me arrependo"¹⁷. (DAVIDSON, 2016)

Os mecanismos de vigilância, controle e coação expostos com o caso Snowden apontam precisamente para uma estrutura que de muitas formas se

17 Do original: "On 12 July 2013 Edward Snowden met with a number of human rights organizations at his temporary refuge in Moscow's Sheremetyevo International Airport. Here are a few of the points he made: 'Through his working connection to the National Security Agency, Snowden found that he "had the capability without any warrant to search for, seize, and read your communications. Anyone's communications at any time. That is the power to change people's fates'. Snowden also concluded that the daily use of this capacity by the NSA was a 'serious violation of the law. The 4th and 5th Amendments to the Constitution of my country, Article 12 of the Universal Declaration of Human Rights, and numerous statutes and treaties forbid such systems of massive, pervasive surveillance'. 'My government [U.S.] argues that secret court rulings, which the world is not permitted to see, somehow legitimize an illegal affair. . . .The immoral cannot be made moral through the use of secret law'. Appalled by this situation, Snowden took to heart the 1945 Nuremberg principle that says, 'Individuals have international duties which transcend the national obligations of obedience. Therefore individual citizens have the duty to violate domestic laws to prevent crimes against peace and humanity from occurring'. Having concluded that the NSA's real and potential secret access to the communications of almost every American, and a growing number of non-citizens, was criminal in nature (perhaps totalitarianism in the making), he leaked the classified information that would bring the NSA's activities into public view. 'That moral decision to tell the public about spying that affects all of us has been costly, but it was the right thing to do and I have no regrets'."

assemelha aos mecanismos de regimes totalitários. A ideologia subjacente que foi traduzida na forma de “Estados Ideais” nos Estados totalitários tradicionais nos parece ausente na aliança das redes de segurança. Ainda, os preceitos ideológicos que guiam a preservação da saúde do sistema econômico e político estão presentes e evidentes. Eles pertencem essencialmente a um discurso de consenso para o centro, o que significa coroar as ideias de associações civis e a constituição de uma comunhão para a civilidade. Mas essa comunhão não é sempre amigável de acordo com as intenções e suposições das entidades empresariais, então é precisamente esse o papel da máquina da sociedade civil, a terceira e mais recente rede de segurança a assumir o lugar como ator civil e no acompanhamento das ações dos outros dois grupos.

As distintas características do atual alinhamento de forças e de atores incluem: (a) o papel das ONGs na sociedade civil como forma de contornar processos democráticos; (b) as políticas de associação entre empresas que assegurem o duplo objetivo do Estado (segurança) e do capital (lucro); (c) a dimensão inigualável na estrutura total de aquisição de dados pelas matrizes da inteligência ocidental; (d) a perseguição e o julgamento de jornalistas, denunciadores e atores pela transparência fora da esfera dos grupos da sociedade civil; (e) a significativa, porém insuficiente, contestação, por parte do público, em relação à infração contra às liberdades civis.

Por fim, as práticas quase-totalitárias das entidades empresariais conduzidas por essas redes de segurança globais são lideradas pelos Estados Unidos e precisam ser urgentemente reconsideradas, assim como novos métodos de desafiá-las. Sem uma solução estrutural para a ocupação do espaço político em ambientes digitais pelas três redes, o cidadão é deixado numa situação de precariedade política, legal e possivelmente até mesmo existencial, em que sua única opção é hackear a reunião de redes autoritárias para reafirmar seus próprios direitos e as obrigações éticas das redes.

Referências

AL JAZEERA. Egypt NGOs 'robbed of independence'. *Al Jazeera*, Doha, 22 set. 2014. Disponível em: <<http://www.aljazeera.com/news/middleeast/2014/09/egypt-ngo-law-crackdown-2014913121624569527.html>>. Acesso em: 17 jan. 2017.

ANONYMOUS releases NSA docs related to global spy network. *Common Dreams*, Portland, 7 jun 2013. Disponível em: <<http://bit.ly/2jUPVai>>. Acesso em: 6 fev 2017.

ARENDT, H. *The origins of totalitarianism*. New York: Harcourt, Brace and Co, 1951.

ASSOCIATED PRESS-NORC CENTER FOR PUBLIC AFFAIRS RESEARCH. *Balancing act: the public's take on civil liberties and security a trend study*. 2013. Disponível em: <<http://bit.ly/2kxAr88>>. Acesso em: 13 jan. 2017.

AUGSTEIN, J. The Chancellor and the NSA: Merkel has abandoned the Germans. *Spiegel Online*, Hamburgo, 16 jul. 2013. Disponível em: <<http://www.spiegel.de/international/germany/editorial-merkel-has-left-germans-high-and-dry-a-911425.html#spLeserKommentare>>. Acesso em: 17 jan. 2017.

BALOGH, E. The Hungarian government turns up the heat on the NGOs. *Hungarian Spectrum*, Bethany, 23 out. 2014. Disponível em: <<https://hungarianspectrum.wordpress.com/2014/10/23/the-hungarian-government-turns-up-the-heat-on-the-ngos/>>. Acesso em: 17 jan. 2017.

BARHAIM, G. *Public-private relations in the totalitarian states*. New Brunswick; London: Transaction, 2011.

BIGO, D. et al. Mass surveillance of personal data by EU member states and its compatibility with EU law. *CEPS*, Brussels, 6 nov. 2013. Disponível em: <<http://www.ceps.eu/book/mass-surveillance-personal-data-eu-member-states-and-its-compatibility-eu-law>>. Acesso em: 17 jan. 2017.

BORGER, J. NSA files: why The Guardian in London destroyed hard drives of leaked files. *The Guardian*, London, 20 ago. 2013. Disponível em: <<https://www.theguardian.com/world/2013/aug/20/nsa-snowden-files-drives-destroyed-london>>. Acesso em: 13 jan. 2017.

CASTELLS, M. *Networks of outrage and hope: social movements in the Internet Age*. Cambridge, UK: Polity, 2012.

DAVIDSON, L. A national debate about government spying? *The New York Times Examiner*, New York, 16 jul. 2016. Disponível em: <<http://www.nytxaminer.com/2013/07/anational-debate-about-government-spying>>. Acesso em: 17 jan. 2017.

DELEUZE, G.; GUATTARI, F. *Anti-Oedipus: capitalism and schizophrenia*. London: Athlone, 1983.

FARCHY, J. Concern grows over NGO crackdown in Azerbaijan. *Financial Times*, London, 22 set. 2014. Disponível em: <<http://www.ft.com/intl/cms/s/0/aec6a9b2-4247-11e4-a9f4-00144feabdc0.html#axzz3KZgToDG9>>. Acesso em: 17 jan. 2017.

FOUCAULT, M. *Discipline and punish: the birth of the prison*. New York: Random House, 1975.

FRIEDERSDORF, C. The surveillance speech: a low point in Barack Obama's presidency. *The Atlantic*, Washington, 12 ago. 2013. Disponível em: <<http://www.theatlantic.com/politics/archive/2013/08/the-surveillance-speech-a-lowpoint-in-barack-obamas-presidency/278565/>>. Acesso em: 17 jan. 2017.

FRIEDRICH, C.; BRZEZINSKI, Z. K. *Totalitarian dictatorship and autocracy*. Cambridge, MA: Harvard University, 1956.

FUCHS, C. *Foundations of critical media and information studies*. London: Routledge, 2011.

GENTILUCCI, M. Can't get a grip on Omidyar philanthropy? You're not alone, so take this guided tour. *Inside Philanthropy*, Santa Monica, 27 mar. 2014. Disponível em: <<http://www.insidephilanthropy.com/tech-philanthropy/2014/3/27/cant-get-a-grip-on-omidyar-philanthropy-youre-not-alone-so-t.html>>. Acesso em: 17 jan. 2017.

GREENWALD, G. The crux of the NSA story in one phrase: 'collect it all'. *The Guardian*, London, 15 jul. 2013. Disponível em: <<http://www.theguardian.com/commentisfree/2013/jul/15/crux-nsa-collect-it-all>>. Acesso em: 17 jan. 2017.

HARVEY, D. *Rebel cities: from the right to the city to the urban revolution*. New York: Verso, 2012.

HAYEK, F. A. *The road to serfdom: text and documents – the definitive edition*. Chicago: University of Chicago, 2007.

HOPKINS, N.; TAYLOR, M. Cabinet was told nothing about GCHQ spying programmes, says Chris Huhne. *The Guardian*, London, 6 out. 2013. Disponível em: <<http://www.theguardian.com/uk-news/2013/oct/06/cabinet-gchq-surveillance-spying-huhne>>. Acesso em: 17 jan. 2017.

HUET, N. French lawsuit targets NSA, FBI, tech firms over Prism. *Reuters*, London, 11 jul. 2013. Disponível em: <<http://www.reuters.com/article/2013/07/11/ususa-security-france-idUSBRE96A00F20130711>>. Acesso em: 17 jan. 2017.

IHRFG – International Human Rights Funders Group. *Hivos institutional profile*. 2015. Disponível em: <<https://www.ihrfg.org/funder-directory/hivos>>. Acesso em: 17 jan. 2017.

KARATZOGIANNI, A. (Ed.). *Cyber-conflict and global politics*. London: Routledge, 2008.

_____. *The politics of cyberconflict*. London: Routledge, 2006.

KARATZOGIANNI, A.; KUNSTMAN, A. (Ed.). *Digital cultures and the politics of emotion*. Basingstoke: Palgrave Macmillan, 2012.

KARATZOGIANNI, A.; ROBINSON, A. *Power, resistance, and conflict in the contemporary world: social movements, networks and hierarchies*. London: Routledge, 2010.

KARATZOGIANNI, A.; ROBINSON, A. *Schizorevolutions vs. microfascisms: the fear of anarchy in state securitization*. 2016. Disponível em: <http://works.bepress.com/athina_karatzogianni/19>. Acesso em: 17 jan. 2017.

LOVINK, G. *Networks without a cause: a critique of social media*. Cambridge, UK: Polity, 2012.

MACASKILL, E.; DANCE, G. NSA files decoded: what the revelations mean for you. *The Guardian*, London, 1 nov. 2013. Disponível em: <<http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded>>. Acesso em: 17 jan. 2017.

MCCAHERILL, M.; FINN, R. L. *Surveillance, capital and resistance: theorizing the surveillance subject*. London: Routledge, 2014.

MOORE, C. This is not Blitz Britain. We sure as hell can't lick terrorism on our own. *The Telegraph*, London, 11 out. 2014. Disponível em: <<http://bit.ly/1spTykQ>>. Acesso em: 13 jan. 2017.

MOROZOV, E. *The net delusion: how not to liberate the world*. London: Allen Lane, 2011.

O'SULLIVAN, N. Oakeshott on civil association. In: FRANCO, P.; MARSH, L. (Ed.). *A companion to Michael Oakeshott*. University Park: Pennsylvania State University, 2012.

OAKESHOTT, M. *On human conduct*. Oxford: Clarendon, 1975.

POITRAS, L. et al. How the NSA targets Germany and Europe. *Spiegel Online*, Hamburgo, 1 jul. 2013. Disponível em: <<http://bit.ly/2k5DgjF>>. Acesso em: 17 jan. 2017.

POPPER, K. *The open society and its enemies*. Princeton: Princeton University, 1971.

RADIO FREE EUROPE – RADIO LIBERTY. The crackdown on NGOs in Russia. *RFE/FL*, Praga, 1 dez. 2014. Disponível em: <<http://www.rferl.org/a/russia-persecution-ngos/25009129.html>>. Acesso em: 17 jan. 2017.

REUTERS. U. S. taps half-billion German phone, internet links in month-report. *Reuters*, London, 30 jun. 2013. Disponível em: <<http://uk.reuters.com/article/uk-usa-germany-spying-idUKBRE95T04I20130630>>. Acesso em: 24 jan. 2017.

RICE, A. The Pierre Omidyar Insurgency. *New York Magazine*, New York, 2 nov. 2014. Disponível em: <<http://nymag.com/daily/intelligencer/2014/10/pierre-omidyar-first-look-media.html>>. Acesso em: 17 jan. 2017.

RT. Microsoft helped the NSA bypass encryption, new Snowden leak reveals. *RT*, Moscow, 11 jul. 2013. Disponível em: <<http://rt.com/usa/microsoft-nsa-snowden-leak-971/>>. Acesso em: 17 jan. 2017.

RUPNIK, J. Totalitarianism revisited. In: KEANE, J. (Ed.). *Civil society and the state: new European perspectives*. London: University of Westminster, 1988. p. 263-290.

RUSHE, D. Zuckerberg: US government “blew it” on NSA surveillance’. *The Guardian*, London, 12 set. 2013. Disponível em: <<http://www.theguardian.com/technology/2013/sep/11/yahoo-ceo-mayer-jail-nsa-surveillance>>. Acesso em: 17 jan. 2017.

SCHIMITT, C. *The concept of the political*. Chicago: University of Chicago, 1996.

SCHOW, A. US government declares hacking an act of war, then hacks allies. *Washington Examiner*, Washington, 1 jul. 2013. Disponível em: <<http://washingtonexaminer.com/article/2532594>>. Acesso em: 17 jan. 2017.

SHIRKY, C. The political power of social media: technology, the public sphere, and political change. *Foreign Affairs*, Tampa, v. 90, n. 1, p. 28-41, jan.-fev. 2011.

SIEGEL, A. Introduction: the changing fortunes of the totalitarian paradigm in communist studies. In: _____. (Ed.). *The totalitarian paradigm after the end of Communism: towards a theoretical reassessment*. Amsterdam: Radopi, 1998. p. 9-35.

TALMON, J. L. *The origins of totalitarian democracy*. London: Mercury Books, 1961.

THE UNITED STATES OF AMERICA. U.S. Department of State. *Funding opportunities*. 2016. Disponível em: <<http://www.state.gov/j/prm/funding/>>. Acesso em: 17 jan. 2017.

YAR, M. *The cultural imaginary of the Internet: virtual utopias and dystopias*. Basingstoke: Palgrave, 2014.

ZIZEK, S. Introduction: on ideological antioxidants. In: _____. *Did somebody say totalitarianism? Five interventions in the (mis)use of a notion*. London: Verso, 2011.

submetido em: 18 ago. 2016 | aprovado em: 20 set. 2016