Após Snowden: Repensando o Impacto da Vigilância

Didier Bigo, Zygmunt Bauman, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, Robert Walker

Após Snowden: Repensando o Impacto da Vigilância

After Snowden: Rethinking the Impact of Surveillance

Zygmunt Bauman

Um dos mais influentes pensadores sobre a pós-modernidade. Sociólogo polonês radicado na Inglaterra, Bauman é autor de mais de 40 livros publicados, dentre eles, Amor Líquido, Modernidade e Holocausto e Globalização: As Conseqüências Humanas. Professor emérito da Universidades de Leeds.

Didier Bigo

Professor do Departamento de Estudos de Guerra da King's College London e professor pesquisador no Sciences-Po Paris. Também é diretor do Centro de Estudos de Conflitos, Liberdade e Segurança (CCLS) e editor da revista francesa Cultures et Conflits.

Paulo Esteves

Doutor em Ciência Política pelo IUPERJ com pós-doutorado na Universidade de Copenhague. Atualmente é coordenador da Pós-Graduação do Instituto de Relações Internacionais da PUC-Rio e realiza pesquisas sobre a convergência dos campos de segurança internacional, humanitarismo e desenvolvimento.

Elspeth Guild

Ph.D. em Sociologia do Direito pela Radboud University, na Holanda, e pesquisadora sênior associada do Centro de Estudos Políticos Europeus (CEPS), em Bruxelas. Também é professora na Queen Mary, University of London e na Radboud University Nijmegen.

Vivienne Jabri

Professora de Políticas Internacionais na King's College London e coordenadora de pesquisa do Centro de Relações Internacionais. Sua pesquisa tem como foco o desenvolvimento de entendimentos críticos nas relações internacionais, com um interesse particular na guerra e sua relação com a política.

David Lyon

Coordenador do projeto "The New Transparency", diretor do Centro de Estudos sobre Vigilância e professor titular em Sociologia e Direito na Queen"s University. Lyon tem estudado vigilância desde os anos 1980 e é autor de inúmeros livros no tema, incluindo "Vigilância Líquida", com Zygmunt Bauman.

R. B. J. Waker

Doutor pela Queens University (1977) e professor da University of Victoria e do Instituto de Relações Internacionais da PUC-Rio. Atualmente é editor das revistas "Alternatives: Local, Global, Political" e "International Political Sociology".

Tradução:

Joana Negri

Doutoranda do Programa de Pós-Graduação em Comunicação e Cultura da Universidade Federal do Rio de Janeiro, na linha de pesquisa Tecnologias da Comunicação e Estéticas. Mestre em Comunicação e Cultura pelo mesmo Programa (2011) e graduada em Jornalismo pela Pontifícia Universidade Católica do Rio de Janeiro (2007).
E-mail: joananegri@gmail.com.

SUBMETIDO EM: 30/05/2015
ACEITO EM: 10/08/2015

DOSSIÊ

RESUMO

Revelações recentes sobre o PRISM, programa secreto da Agência de Segurança Nacional dos Estados Unidos (NSA), confirmaram a vigilância em larga escala de mensagens eletrônicas e telecomunicações de governos, empresas e cidadãos, inclusive de aliados próximos aos EUA na Europa e na América Latina. As ramificações transnacionais da vigilância pedem a reavaliação das práticas políticas do mundo contemporâneo. O debate não pode se limitar à oposição Estados Unidos e resto do mundo ou vigilância e privacidade; muito mais está em jogo. Este artigo coletivo descreve, brevemente, especificidades da vigilância cibernética em massa, incluindo a combinação de práticas de serviços de inteligência e de empresas privadas ao redor do mundo. Em seguida, investiga o impacto destas práticas em termos de segurança nacional, diplomacia, Direitos Humanos, Democracia, subjetividade e obediência.

PALAVRAS-CHAVE: Vigilância; Democracia; Privacidade; Internet.

ABSTRACT

Current revelations about the secret US-NSA program, PRISM, have confirmed a large-scale mass surveillance of telecommunication and electronic messages of governments, companies, and citizens, including the United States' closest allies in Europe and Latin America. The transnational ramifications of surveillance call for a re-evaluation of contemporary world politics practices. The debate cannot be limited to the United States versus the rest of the world or to surveillance versus privacy; much more is at stake. This collective article briefly describes the specificities of cyber mass surveillance, including its mix of practices of intelligence services and those of private companies providing services around the world. It then investigates the impact of these practices on national security, diplomacy, Human Rights, Democracy, subjectivity and obedience.

KEYWORDS: Surveillance; Democracy; Privacy; Internet.

1. Técnicas de vigilância em larga escala e o alcance global da internet: uma lacuna permanente

Edward Snowden, notoriamente, revelou informações vastas acerca das práticas da Agência de Segurança Nacional dos EUA (NSA) no que diz respeito ao PRISM e outros programas de vigilância norte-americanos - incluindo o *Xkeyscore,* o *Upstream,* o *Quantuminsert,* o *Bullrun* e o *Dishfire* - bem como o envolvimento de serviços em outros Estados - como o GCHQ do Reino Unido e seu Tempora (assim como o seu *Optic Nerve*). Grande parte dessas informações, especialmente sobre a escala, o alcance e a sofisticação técnica dessas práticas, surpreendeu até mesmo observadores experientes e seu significado permanece obscuro. Isto se deve, em parte, à dificuldade de localização dos detalhes extensos acerca dos sistemas complexos expostos, embora muitos deles pareçam ter consequências graves e imediatas. Esses detalhes também parecem sugerir transgressões significativas nos entendimentos estabelecidos sobre o caráter e a legitimidade das instituições envolvidas em operações de segurança e inteligência, estimulando, assim, intensa controvérsia política. E se deve, em parte, e de modo ainda mais desconcertante, ao fato de que algumas revelações parecem confirmar transformações de longo prazo na política dos Estados, nas relações entre eles e nas instituições e normas estabelecidas quanto: aos procedimentos democráticos; ao Estado de Direito; às relações entre Estado e sociedade civil; política pública e interesses econômicos - empresariais ou privados -; à aceitabilidade de normas culturais e, até mesmo quanto a conceitos de subjetividade.

Existe, portanto, uma necessidade urgente de avaliação sistemática da escala, do alcance e do caráter das práticas de vigilância contemporâneas, bem como das justificativas que atraem e das controvérsias que provocam. Precisamos saber se essas práticas marcam uma reconfiguração significativa das relações entre coleta de informações,

vigilância na Internet e outros sistemas de telecomunicações; ou se marcam desafios contínuos aos Direitos Fundamentais na esfera digital. E precisamos estar atentos às implicações de longo prazo de práticas que já suscitaram sérias questões sobre transgressões generalizadas de princípios legais e normas democráticas, de modo a expressarem mudanças históricas no locus e no caráter da autoridade soberana e da legitimidade política.

Os programas da NSA destinam-se, em primeiro lugar, à coleta de dados de cabos (submarinos) da internet (*Upstream, Quantuminsert*) e/ou à interceptação de dados durante o seu trânsito (*Tempora*). Tais programas envolvem a colocação de interceptores nos grandes cabos de fibra óptica que ligam os diferentes centros de Internet. No Reino Unido, informações dão conta de que o programa *Tempora*, do GCHQ[1], teria colocado 200 interceptores em cabos que se estendem das ilhas britânicas à Europa Ocidental e aos Estados Unidos. A DGSE[2] francesa teria, supostamente, colocado interceptores semelhantes em cabos submarinos fora de sua base militar, no *Djibouti.* Dentre outras atividades, foi dito que o BND[3] alemão interceptou diretamente o maior centro de Internet da Europa, o DE-CIX[4], em Frankfurt. O FRA[5] sueco grampeou os cabos submarinos que conectam os países bálticos e a Rússia. Os diferentes serviços de inteligência trabalham razoavelmente juntos e em rede para recolherem informações e as estenderem a um alcance global, abrangendo a Internet. Suas relações tendem à assimetria - às vezes, eles são competitivos e a colaboração diminui no que diz repeito a questões confidenciais – mas, ainda assim, os serviços acreditam que a colaboração é necessária para a produção de uma imagem confiável da Internet global. Eles, invariavelmente, afirmam que não possuem recursos suficientes, necessitando de mais dados e mais trocas de informações - com menos controle e fiscalização - a fim de acelerarem o processo. Não é novidade que tais alegações estimulam a reconvenção de formas de vigilância em massa, como as realizadas pela Stasi, bem como queixas sobre a inversão da presunção de inocência por meio de uma suspeita a priori de que o indivíduo deve, então, rebater através de um comportamento transparente.[6]

As suspeitas também são despertadas por um segundo e mais específico sistema de interceptação, o Xkeyscore, que está ligado à plataforma de integração do programa PRISM, da NSA, e que funciona de forma semelhante à interceptação iniciada pelo programa *Total Information Awareness*, do almirante Poindexter. Esse sistema envolve a aquisição de informações pessoais dos consumidores por meio de pressões exercidas sobre empresas privadas (como Google, Microsoft, Apple ou Skype), que coletam regularmente grandes quantidades de dados para fins comerciais, para entregá-los aos serviços de inteligência sem o conhecimento dos usuários. Acredita-se que a NSA e vários serviços europeus tenham obtido dados extensos e precisos através deste canal. Estas informações não são recolhidas através de cabos de trânsito de dados brutos, mas relacionam-se, principalmente, à disposição dos usuários em utilizar serviços de computação em nuvem - fornecidos, por exemplo, pelas plataformas Microsoft ou

1 British Government Communications Headquarters.
2 The General Directorate for External Security.
3 The Federal Intelligence Service.
4 German Commercial Internet Exchange.
5 The National Defence Radio Establishment.
6 Para atualizações regulares sobre as revelações dos diferentes programas de vigilância, consulte os sites The Guardian e The Christian Science Monitor. Entre os muitos relatórios disponíveis, consulte o US Review Group on Intelligence and Communications Technologies: Liberty And Security in a Changing World, organizado por Richard A. Clarke, em 12 de dezembro de 2013. Veja também o relatório US Independent Privacy Oversight Board, organizado por David Medine, em 23 de janeiro de 2014; o EU Report of the Libe Committee of the EU Parliament, organizado por Claudio Moraes, em 12 de março de 2014; e o Research Study on National Programmes for Mass Surveillance of Personal Data in EU member states and their Compatibility with EU law, CCLS-CEPS, em novembro de 2013 (ver referências).

Dropbox - e a sua ignorância acerca da coleta secreta de seus dados. Este é também o caso das informações provenientes de redes sociais, como as geridas pelo Facebook. Tais dados e metadados permitem um mapeamento das relações entre as pessoas, seus endereços IP, bem como a partilha de conteúdos, localizações e interesses. Portanto, as redes desses diferentes serviços não são apenas transnacionais, mas também híbridas de agentes públicos e privados. Este alargamento, em termos de agentes e alcance, não é um processo fácil; ele também exacerba esforços. Alguns serviços de inteligência, especialmente a NSA e o GCHQ, trabalham em uma escala muito grande e lançam mão de colaborações voluntárias ou involuntárias por meio de prestadores privados (Microsoft, Google, Yahoo, Facebook, Paltalk, YouTube, Skype, AOL, Apple) e empresas de telecomunicações (BT, Vodafone Cable, Verizon Business, a Global Crossing, Nível 3, Viatel e Interroute), a fim de captar pontos e tentar conectá-los utilizando *softwares* de perfis e de visualização. Outros serviços não concordam com esta estratégia e não solicitam dados de fornecedores, preferindo concentrar-se em alvos específicos, trabalhando em pequena escala, mas com maior precisão.

Um terceiro tipo de prática envolve a coleta de chamadas telefônicas, mensagens de texto, comunicações via Skype e diversos sinais de áudio e vídeo transmitidos através de computadores, *smartphones*, comunicações via satélite e telefones fixos tradicionais (como o *Dishfire,* para mensagens de texto). Esta prática atualiza e amplia, de forma eficaz, o tipo de vigilância de telecomunicações que produziu escândalos anteriores envolvendo o sistema *Echelon* para a interceptação de comunicação pessoal e comercial (Schmid, 2001).

Estas diversas práticas de interceptação de comunicação são complexas e interligadas e são projetadas para processamento secreto de dados pessoais que consistem em conteúdo (gravações de chamadas telefônicas, mensagens de texto, imagens de *webcams*, teor das mensagens de e-mail, *logins* no Facebook, histórico de acesso a sites da web do usuário, e assim por diante) e metaconteúdo (registro dos meios de criação dos dados transmitidos, a hora e a data de sua criação, seu criador e o local onde foi criado). Uma vez reunidos, os dados e os metadados são conservados durante um determinado período de tempo (como no *Tempora*) e, em seguida, organizados através de plataformas de integração (tais como o PRISM) para se tornarem inteligíveis por meio da visualização de redes, começando por pessoas ou endereços de Internet que já estão sob suspeita.

O acesso a mais informações sobre estas práticas tem gerado, com razão, considerável polêmica. Mas há o perigo de que tanto o debate popular quanto o erudito sejam reduzidos às narrativas familiares sobre a reformulação das relações entre observadores e observados por meio de desenvolvimentos tecnológicos, ou sobre a concretização das previsões de George Orwell ou Philip K. Dick, ou ainda sobre a transformação das democracias representativas em regimes totalitários em nome da proteção. Tanto a informação que se tornou disponível quanto às muitas tentativas de avaliar o seu significado sugerem que questões mais profundas devem ser discutidas. Uma delas diz respeito à separação conceitual entre, de um lado, disposições e aspirações moldadas pela ideia de um mundo interestadual em que cada Estado tem uma visão clara de sua própria segurança nacional e, de outro, práticas de vigilância realizadas por uma rede de diferentes serviços de inteligência que compartilham algumas informações, enquanto, ao mesmo tempo, atuam contra seus parceiros - desestabilizando, assim, entendimentos tradicionais sobre alianças e comportamento de Estado. A segunda questão diz respeito à utilização destas tecnologias e a materialidade dos cabos de

Internet como fonte de informação cuja geografia específica oferece vantagens políticas para alguns países e pode reconfigurar a política do poder em escala mundial. A terceira questão diz respeito às formas de resistência de múltiplos agentes a estas políticas através de estratégias diplomáticas e legais, bem como o ajustamento do comportamento dos usuários de Internet em suas práticas cotidianas: se, por exemplo, vão continuar a participar de sua própria vigilância, por meio da autoexposição, ou se vão desenvolver novas formas de subjetividade mais reflexivas acerca das consequências de suas próprias ações. A quarta questão diz respeito à origem e à legitimidade das autoridades que afirmam agir em nome da necessidade política e da segurança.

Tais questões nos obrigam a repensar os cânones dos "estudos de vigilância" e os "estudos críticos de segurança" que já criticaram a concepção de vigilância como uma ferramenta a serviço de agentes e interesses mais poderosos. Estudiosos têm suscitado modos promissores de se pensar o caráter complexo e rizomático dos instrumentos de redes de vigilância interconectadas nas quais a autoexposição tem se tornado comum. Mas agora também é preciso analisar a união dos serviços de inteligência com poderosas plataformas de integração, tais como o PRISM.

Parte da dificuldade que existe em repensar essas questões surge do sentimento generalizado de que o que está acontecendo em relação à NSA é moldado por muitas dinâmicas (além da relação entre inovação tecnológica e possibilidade política) que poucos estudiosos e pouquíssimos responsáveis políticos compreendem. Essas dinâmicas abarcam mudanças sociais e culturais que reformulam a aceitabilidade de novas práticas de comunicação, novas formas de conhecimento e rápidas mudanças nos modos de expressão da identidade pessoal. De forma mais significativa, elas incluem a mudança geral para o mercado, em vez da lei estadual como medida final de valor político e ético. De modo mais perplexo, talvez, parece que estamos envolvidos com fenômenos que não são organizados nem na horizontal - na forma de uma matriz internacionalizada de Estados razoavelmente autodeterminados e territorializados - nem na vertical - na forma de uma hierarquia de autoridades superiores e inferiores. Relações, linhas de voo, redes, integrações e desintegrações, contrações espaço-temporais e acelerações, simultaneidades, inversões de interioridade e exterioridade, limites cada vez mais elusivos entre inclusão e exclusão, ou legitimidade e ilegitimidade: crescente familiaridade destas e outras noções semelhantes sugerem uma forte necessidade de novos recursos conceituais e analíticos. Talvez devêssemos reler Leibniz.

2. Uma *banda de Moebius* de segurança nacional e vigilância transnacional

Coleta em massa de dados, segurança nacional, inteligência estrangeira: a distribuição desigual da suspeita

Diz-se que o trabalho de inteligência começa a partir de suspeitas de atos perigosos cometidos por um grupo sob vigilância. Em seguida, procede-se à identificação de pessoas desconhecidas relacionadas com o grupo inicial, dentro de três graus de separação (ou saltos). Isso quer dizer que para uma pessoa suspeita com 100 amigos no primeiro salto, aquele encarregado de vigilância pela NSA - ou um de seus subcontratantes privados - pode colocar sob vigilância, sem mandado, todas as 2.669.556 ligações potenciais no terceiro salto.[7]

7 Barack Obama, seguindo uma das 45 recomendações do Grupo de Revisão em Inteligência e Tecnologias de Comunicação, emitidas em 12 de dezembro de 2013, parece pronto para limitar a busca sem mandado para dois níveis (neste caso 16.340), reduzindo a escala da pesquisa, ao mesmo passo que mantém o princípio vivo. Discurso de 17 de janeiro de 2014, disponível online no The Guardian, http://www.my-rss.co.uk/feeditem.php?feed=0&word=&search=laws&item=263734. (Acesso em 19/03/2014). Para uma pesquisa interativa sobre os níveis, consulte http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-sur-

Dada à magnitude dos dados acumulados desse modo, os analistas não leem todo o conteúdo, mas visualizam o gráfico das relações identificadas e se concentram nos

setores mais significativos que revelam nós específicos de conexões entre os dados. Isto está longe de ser uma leitura completa do conteúdo de tais dados. E também está longe de ser um procedimento científico que talvez garanta reivindicações de certeza e precisão sobre os resultados obtidos. É, antes, parte de um processo de intuição e interpretação que pode variar, consideravelmente, de um analista para outro. Temores sobre o Big Brother são, portanto, em grande parte irrelevantes. A pretensão de verdade, que acompanha essas visualizações, é infundada, contribuindo apenas para transformar suspeitas em formas de conhecimento mais impressivas por meio de previsões acerca das ações dos indivíduos - quando até mesmo a previsão geral sobre tendências futuras é bastante complicada. O que está em jogo, aqui, é menos um casamento entre tecnologia e uma ciência da sociedade e mais entre tecnologia e uma fé especulativa em sistemas projetados para "ler" grandes arquivos de dados.

O campo potencial de suspeita é imenso, no sentido de que ele não tem fim e se espalha através de redes. Mas não é imenso em termos de alcance global ou da vigilância de todos. Este é realmente o principal argumento apresentado pelos diferentes serviços de inteligência. Eles afirmam ter critérios objetivos para restrição de suas pesquisas e que sua cobertura abrange apenas inteligência estrangeira (consultar a Lei de Vigilância de Inteligência Estrangeira [FISA] e a Corte de Vigilância de Inteligência Estrangeira [FISC] norte americanas, os requisitos do GCHQ e as diretivas internas francesas). Portanto, comunicações envolvendo uma extremidade estrangeira seriam examinadas, prioritariamente, em um circuito especial. No entanto, o sistema também pode identificar comportamentos suspeitos no âmbito nacional (e, nesses casos, terá que pedir um mandado nas jurisdições do Reino Unido e dos EUA). A coleta em massa de dados e a visualização através de redes torna impossível distinguir com clareza as comunicações nacionais e estrangeiras. Requisitos de legalidade ameaçam o funcionamento do sistema e presume-se, assim, que a lei deve se ajustar, e não o sistema. Para evitar esse tipo de "complicação", a criação de redes transnacionais entre diferentes serviços permitiu uma diluição dos limites das jurisdições nacionais e estrangeiras. Parece que os diferentes serviços responsáveis pela sua própria segurança nacional, trabalhando através da coleta e troca de informações, solicitam a execução de algumas de suas tarefas a outros serviços de segurança, ignorando limitações de inteligência estrangeira através da utilização de um "comércio da privacidade dos cidadãos" para trocar a vigilância de seu próprio cidadão com outro serviço. Desta forma, o que é nacional e o que é estrangeiro torna-se, em grande parte, irrelevante para operações transnacionais organizadas.

Segurança nacional e a digitalização da Razão de Estado

Essas formas de coleta e partilha de informações têm efeitos paradoxais nos requisitos de segurança nacional. A segurança nacional não é mais nacional em sua aquisição ou mesmo em sua análise de dados, e os diferentes imperativos de segurança nacional dos aliados podem colidir, causando desconfiança. A digitalização cria grandes volumes de dados recolhidos em escala transnacional, diluindo as linhas do que é nacional, bem como as fronteiras entre a aplicação da lei e a inteligência. Estas

veillance-revelations-decoded#section/1. Acesso em 19/03/2014.

tendências incentivam a mudança do quadro jurídico de policiamento criminal para abordagens preventivas, preemptivas e preditivas, e também de um elevado grau de certeza acerca de uma pequena quantidade de dados para um elevado grau de incerteza sobre uma grande quantidade de dados. A hibridação de agentes públicos e privados desestabiliza a socialização por meio dos interesses do Estado nacional e do sigilo, abrindo possibilidades para grandes vazamentos de informações por pessoas com diferentes valores.

Colocando em termos mais teóricos, a mudança e a incerteza em torno das categorias "estrangeiro" e "doméstico" as dispersam através de redes de conexões e convertem a linha soberana que as separava claramente em uma *banda de Moebius* (Bigo, 2001). Ao projetar a segurança nacional de "dentro para fora" - através de uma aliança transnacional de profissionais de segurança nacional e de dados confidenciais, tanto públicos como privados - uma inesperada suspeita de "fora para dentro" é criada acerca de todos os assuntos relacionados à Internet. Muitas das "pessoas em causa" reagem e rejeitam a situação em que todos os usuários da Internet são tratados como suspeitos em potencial, ao invés de inocentes a priori.

As práticas de vigilância em larga escala, realizadas pela NSA e os seus parceiros, devem, portanto, ser compreendidas não como breves escândalos midiáticos, mas como indicadores de uma transformação muito maior que afeta o modo de funcionamento dos limites de segurança nacional. Isto se deve à conjunção de três processos entrelaçados: transnacionalização, digitalização e privatização.

Esta conjunção cria um efeito global de dispersão que desafia a própria ideia de uma razão de Estado conduzida por um "Estado" em que o governo determina os interesses e a segurança nacional, solicitando a seus próprios serviços que operem em conformidade. Mesmo tendo sempre se sustentado em afirmações exageradas sobre autonomia e autodeterminação, o conceito de razão de Estado é agora cada vez menos encapsulado na fórmula de uma segurança nacional executada por serviços de inteligência socializados em sigilo e responsabilidade pública, patriotismo e suspeita de serviços em outras nações. Antes, vemos a transformação da razão de Estado através da emergência de sua versão digitalizada, realizada por um heterogêneo complexo de profissionais e informações confidenciais híbridas de agentes públicos e privados. A natureza transnacional da coleta de informações que atravessa as fronteiras dos Estados dissocia a natureza discursiva e homogênea dos interesses de segurança nacional, enquanto reconstrói um coletivo de profissionais. Esses profissionais trocam informações através de tecnologias digitais, produzem inteligência de acordo com seus próprios interesses, e desprezam a ideia de que os direitos de todos os usuários da Internet possam criar limitações aos seus projetos.

Por conseguinte, estas corporações transnacionais de profissionais estão desafiando diretamente a autoridade dos profissionais de política que, em princípio e pelo menos dentro dos limites de uma ordem internacional, tinham a capacidade e a autoridade para definir o conteúdo dos interesses nacionais e de segurança (Bigo, 2013). Elas também desafiam a autoridade dos cidadãos nacionais, reconfigurando as ideias de privacidade, sigilo de comunicação, presunção de inocência e, até mesmo, de democracia. Não precisamos ir muito longe para sugerir que o que ainda podemos chamar de "segurança nacional" foi colonizado por uma nova nobreza de agências de inteligência que operam em uma arena transnacional cada vez mais autônoma.

Um campo de trocas de informações computadorizadas entre profissionais de dados sensíveis e uma corporação tentando organizá-lo

Se olharmos para o número de agências, o tamanho de suas forças de trabalho e as capacidades tecnológicas dos diferentes serviços de inteligência, torna-se claro que a noção de redes não pode ser empregada para sugerir um regime de reciprocidade e igualdade. Estas redes de relações são assimétricas e hierárquicas, como eram as corporações da Idade Média com seus rituais, códigos e regras de obediência e solidariedade.

A NSA tem oito vezes mais empregados do que o DGSE e o BND, e sete vezes mais do que o GCHQ. Além disso, a NSA emprega empreiteiros privados para executarem parte de seu trabalho, de modo que o número de funcionários pode ser de 12 a 16 vezes maior do que os de qualquer outra agência. Da mesma forma, a NSA tem um orçamento de US$ 10,8 bilhões (7,8 bilhões de euros) por ano, ao passo que o orçamento de 1,2 bilhões do GCHQ europeu está bem abaixo da agência norte-americana - não obstante, é mais do que o dobro do orçamento anual de outras agências, como o BND, a FRA ou o DGSE. É por isso que, talvez, seja mais preciso falar em uma corporação anglo-americana de profissionais estendida a outros serviços de inteligência ocidentais, do que analisar a rede como uma colaboração igualitária entre os EUA e a Europa, ou mesmo uma colaboração transatlântica correlacionada com a OTAN.

A força dessa corporação talvez reflita o considerável grau de solidariedade já criado no final da 2a Guerra Mundial, com a aceitação da hegemonia dos Estados Unidos. A chamada Five Eyes (Estados Unidos, Reino Unido, Canadá, Austrália e Nova Zelândia) é uma rede de serviços de inteligência, recentemente estendida à Suécia - e agora, possivelmente, à França e à Alemanha - que parece ter sido o principal veículo através do qual a NSA alargou a sua vigilância para além de suas próprias habilidades técnicas, a fim de um alcance global (especialmente, através dos cabos submarinos já mencionados). Esta rede de profissionais de segurança e informações confidenciais tem funcionado como um nó para coleta e partilha de dados, transmitindo a impressão de uma forte colaboração recíproca e de um objetivo comum: o antiterrorismo. No entanto, as revelações de Snowden têm mostrado a assimetria estrutural desta relação, em termos de exploração de dados e inteligência. Longe de um fluxo contínuo de informações, são as relações de poder que estruturam o jogo.

Múltiplos focos de resistência

Alguns parceiros da NSA (Alemanha, Polônia, Suécia, Holanda e até mesmo França) abalaram-se com o modo como foram enganados e transformados em instrumentos quando pensavam serem colaboradores. A confiança entre os serviços - que eram limitados, mas todavia existiam em nome da luta contra o terrorismo - desapareceu, em grande parte, quando ficou claro que a espionagem industrial e de políticos, a mineração de dados das informações pessoais de grandes populações - a fim de traçar o perfil de desenvolvimento das escolhas dos consumidores – e, até mesmo as opiniões políticas sobre as futuras eleições têm sido utilizadas por analistas da NSA. Isto inclui a espionagem de populações de países com os quais foram estabelecidas alianças e colaborações na rede *Five Eyes Plus*. Houve, assim, uma compreensão, por parte de alguns parceiros da NSA, de que a colaboração em apoio à segurança nacional dos Estados Unidos tem comprometido, com sua própria cumplicidade "involuntária", a sua segurança e os seus interesses nacionais.

Deste modo, a questão da lealdade foi suscitada, na medida em que os próprios serviços responsáveis pela segurança nacional colocaram nações em perigo, transmitindo informações à NSA. O Reino Unido encontra-se em uma posição especialmente delicada, uma vez que o GCHQ tem participado de comportamentos agressivos contra outros parceiros e instituições da União Europeia[8], mesmo integrando o bloco e tendo assinado o tratado que exige lealdade dos Estados membros. Em contrapartida, as revelações de que a NSA tem levantado arquivos que permaneceram longe do conhecimento britânico - porque eram importantes e prejudicariam os interesses do Reino Unido – causaram mal-estar em alguns serviços de polícia do Reino Unido e um certo sentimento de traição, refletindo a perda da posição privilegiada que mantinha com os Estados Unidos.

Neste sentido, as revelações de Snowden criaram um efeito bola de neve de desconfiança acerca dos resultados positivos da troca de dados com a NSA e impeliram fornecedores privados, como a empresa francesa Orange, a verificarem as suas infraestruturas técnicas. Eles descobriram que a maioria das tecnologias utilizadas pela NSA para reunião de quase todas as informações foram duais: primeiro, por solicitarem a colaboração em questões razoavelmente legítimas (ligadas, principalmente, ao antiterrorismo e ao crime organizado) e segundo por, fraudulentamente, introduzirem ferramentas nos sistemas de seus colaboradores, especialmente aqueles recentemente agregados ao nó principal (França, Alemanha, Suécia, Holanda, e, possivelmente, Brasil).

Políticos destes países viram-se encurralados entre seu apoio oficial à necessidade de reunir informações contra o terrorismo, sua americanofilia, - argumentos para uma aliança comum - e o comportamento agressivo da NSA. Se, por um lado, eles obtiveram grande sucesso em silenciar as reservas expressas por alguns operadores de dentro da rede (magistrados investigativos, por exemplo), o mesmo não aconteceu com todos os prestadores privados e, mais ainda, com a sociedade civil e com as diferentes ONGs. Centenas de ações judiciais, oriundas de diferentes agentes com diferentes motivos, foram lançadas e será impossível bloqueá-las sem uma reforma profunda.

3. Jogos que os Estados jogam ao longo da *banda de Moebius*

A transformação de linhas territoriais em uma *banda de Moebius* rearticula os jogos soberanos habituais dos Estados. Embora a grande coleta de dados dilua categorizações do que é "nacional" e do que é "estrangeiro", a consequente reconfiguração dos limites do Estado soberano em uma *banda de Moebius* tem, por sua vez, tornado-se, por si só, um lugar de lutas políticas, resistências e dissidências. Ao longo da *banda de Moebius*, Estados, movimentos sociais e pesssoas podem desempenhar uma variedade de jogos, reencenando os significados de soberania, cidadania, segurança e liberdade. No caso dos Estados, as reações contra a vigilância em massa têm variado de afirmações de direitos universais à reconstituições de limites territoriais soberanos e da digitalização da segurança à digitalização da geopolítica. Várias dimensões da reação recente do governo brasileiro contra as técnicas de vigilância em massa são exemplares dos diferentes jogos estaduais que têm acontecido ao longo da *banda de Moebius*. Esta seção irá abordar esses jogos e como eles moldam lutas políticas em torno da razão de Estado digitalizada.

8 O GCHQ tem sido acusado de intrusão nos sistemas *Belgacom*, a fim de espionar a Comissão Europeia e o Parlamento - uma operação de codinome Socialista, empreendida através do *Quantuminsert.*

REVISTA ECO PÓS | ISSN 2175-8689 | TECNOPOLÍTICAS E VIGILÂNCIA | V. 18 | N. 2 | 2015 | DOSSIÊ

A exposição das operações de vigilância da NSA no Brasil por Edward Snowden - incluindo o monitoramento do telefone celular da presidente Dilma Rousseff e a coleta de dados da empresa de petróleo do país e, de forma indiscriminada, dos cidadãos brasileiros - desencadeou uma série de ações em várias arenas. Além do adiamento de uma visita oficial aos Estados Unidos, inicialmente prevista para outubro de 2013, a presidente Dilma Rousseff dedicou seu discurso de abertura na Assembleia Geral das Nações Unidas à questão da vigilância em massa ou, em seus termos, à "rede global de espionagem eletrônica". A declaração condenou as práticas da NSA em dois pontos: a violação dos direitos humanos e o "desrespeito à soberania nacional". Em consonância com o discurso de Rousseff, o resultado mais visível foi a inclusão do direito à privacidade na agenda da Comissão de Direitos Humanos da ONU e a introdução de uma resolução na Assembleia Geral das Nações Unidas, com o apoio do governo alemão. Mesmo que a resolução não mencione os Estados Unidos, sua proposta foi uma forma de censurar as práticas de vigilância em massa realizadas por agências norte-americanas. No entanto, contrariamente às muitas acusações de violação da soberania nacional (vocalizadas por muitos governos, incluindo Brasil e Alemanha), o que distingue esta reação foi o palco onde ela ocorreu e o vocabulário através do qual foi articulada. Nas Nações Unidas, os Estados devem empregar um vocabulário universal, permitindo, consequentemente, reivindicações acerca do reconhecimento da privacidade como um direito humano.

A adoção de um vocabulário universal desestabiliza o núcleo das práticas de vigilância em massa, trazendo à tona os meios através dos quais estas constituem o seu principal objeto de preocupação: a "pessoa em causa". A "pessoa em causa" é uma forma condicional de existência cujos direitos são dependentes de seu comportamento nas redes digitais. A observação e análise de comportamentos específicos possibilitam o desenho de perfis genéricos e a identificação de ameaças e alvos. Assim, o grau de separação entre o sujeito e um alvo identificado aciona técnicas de vigilância específicas e define os direitos da "pessoa em causa". Sob o regime da razão de Estado digitalizada, os direitos individuais são condicionados por uma série específica de relacionamentos e pelas posições particulares que a pessoa ocupa dentro dessas redes sem limites. "As pessoas em causa" são constituídas e consultadas com relação à sua posição particular. Seus direitos dependem de quão distantes - ou não - estão de determinados alvos. Esta articulação posicional está em desacordo com os pressupostos cosmopolitas que sustentam a campanha de direitos universais dos governos brasileiro e alemão. As suas tentativas de reconstituição dos direitos individuais e, em última instância, a ideia reguladora de um sujeito autônomo contra a razão de Estado digitalizada podem soar ultrapassadas e, talvez, conservadoras. Neste sentido, os debates políticos sobre as técnicas de vigilância em massa na Assembleia Geral representaram, principalmente, uma luta entre dois modos de existência: a pessoa em causa e o sujeito cosmopolita dos direitos universais. No entanto, a inclinação cosmopolita da resolução da Assembleia Geral foi um meio de reconstituir as promessas da política moderna internacional, não só através da proteção da autonomia do indivíduo mas também através da afirmação da responsabilidade dos Estados em protegê-la. Contra as práticas de vigilância em massa, Estados como o Brasil e a Alemanha tentaram transformar novamente a *banda de Moebius* em linhas territoriais soberanas.

Não obstante, a jogada cosmopolita não foi feita à custa da soberania do Estado, pelo

menos não no caso do governo brasileiro. Dentro deste jogo particular, a adoção de um vocabulário cosmopolita autoriza a ação do Estado a fim de proteger os direitos dos seus cidadãos, incluindo o direito à privacidade e, como será discutido abaixo, à proteção de dados. Portanto, nas Nações Unidas, o jogo das autoridades brasileiras é realmente uma tentativa de conciliar a autonomia individual, a soberania do Estado e os direitos universais. Embora, estrategicamente, este jogo desafie os fundamentos da razão de Estado digitalizada, as técnicas mobilizadas e, eventualmente, implantadas para proteger os direitos dos cidadãos podem, com efeito, reforçá-la. Alegando que a privacidade é um direito humano, as autoridades brasileiras apoiam a criação de um acordo multilateral e multissetorial "capaz de garantir a liberdade de expressão, a privacidade dos indivíduos e o respeito pelos Direitos Humanos" (Rousseff). Contudo, a mesma reivindicação autoriza o governo brasileiro a declarar sua determinação de "fazer tudo ao seu alcance para defender os Direitos Humanos de todos os brasileiros e para proteger os frutos nascidos da engenhosidade dos [seus] trabalhadores e das [suas] empresas" (Rousseff). Ou seja, o que a presidente Dilma Rousseff tem em mente é um conjunto de medidas internas destinadas à criação de capacidades nacionais de proteção à privacidade dos cidadãos brasileiros contra a ameaça da vigilância em massa dos Estados Unidos[9]. Embora a regulação multilateral do ciberespaço e a capacidade nacional de proteção da privacidade dos cidadãos possam se complementar, as perspectivas de desenvolvimento de técnicas de proteção nacional podem desencadear um outro jogo: uma geopolítica digitalizada.

A Razão de Estado digitalizada e sua geopolítica digitalizada

As políticas anunciadas pelo governo brasileiro para controle das ameaças apresentadas pelas técnicas de vigilância em massa dos Estados Unidos incluem o aumento da conectividade internacional na Internet e da produção nacional de conteúdo. De acordo com as autoridades brasileiras, a produção de conteúdo nacional, como um serviço de e-mail ou uma rede social nacionais, permitiria que os cidadãos brasileiros mantivessem seus dados dentro das fronteiras do país. O debate sobre a criação de uma "nuvem de dados europeia" levanta questões semelhantes. De fato, as autoridades brasileiras não estão sozinhas. Seguindo um caminho semelhante, as autoridades holandesas têm tentado manter os dados do governo fora do alcance das empresas americanas, enquanto a União Europeia discute a possibilidade de isolar o armazenamento de dados das técnicas de exploração dos EUA. E o governo alemão tenta manter o tráfego local, alertando os usuários quando o acesso se dá fora do ciberespaço europeu. Isso sem mencionar os casos bem conhecidos do chinês *Great Firewall* ou do iraniano *Internet Halal*. Em todos os casos, os Estados estão engrossando suas fronteiras digitais. Embora não se deva ignorar as diferenças entre o que as autoridades brasileiras ou alemãs estão fazendo para proteção de seus dados e de sua privacidade e o que o governo chinês está fazendo com o seu *firewall*, em cada um destes casos, uma extensa infraestrutura tem que ser construída. Por isso, uma vasta gama de tecnologias, legislações e competências devem ser desenvolvidas e implantadas para proteção de dados, controle de tráfego ou mesmo vigilância. No topo de todos esses investimentos nas capacidades de proteção e vigilância do Estado, os profissionais de segurança e especialistas em inteligência devem ser mobilizados para gestão dos sistemas nacionais.

Ao construírem suas fortalezas nas nuvens, Estados deslocam-se do jogo cosmopolita

9 *Brazil is Beating United States at its own Game*. Disponível em http://america.aljazeera.com/articles/2013/9/20/brazil-internet-dilmarousseffnsa.html. Al Jazeera, 2013. Acesso em 19/03/2014.

para o jogo estratégico. Enquanto o primeiro é baseado em reivindicações de direitos universais, o jogo estratégico baseia-se em reivindicações de afirmação de soberania ou, neste caso, da ciber-soberania. Dentro destes jogos estratégicos, muitas vezes, a

referência aos direitos universais desaparece e acaba substituída por um raciocínio estratégico ancorado na incerteza e no medo. Conceitos como interesse nacional, segurança nacional ou estadual, espionagem e guerra vêm à tona quando os representantes estaduais vão a público para apoiarem políticas e técnicas de proteção de uma dada sociedade. O ciberespaço é, então, descrito como um espaço centralizado pelos EUA, cujo poder cibernético deve, portanto, ser equilibrado através do desenvolvimento de capacidades cibernéticas nacionais ou coligações internacionais.

No caso brasileiro, as tentativas de expansão da conectividade internacional na Internet (dentro do espaço regional mas também em escala global) são consistentes com a ideia de proteção dos dados nacionais bem como de equilíbrio ou competição com a posição norte-americana no ciberespaço. O programa compreende três iniciativas articuladas: a construção de cabos de fibra submarinos intercontinentais (muitos deles ligando os países do Sul); um programa de satélite, com previsão de lançamento do *Satélite Geoestacionário de Defesa e Comunicações Estratégicas*, em 2016; e, finalmente, um cabo de fibra terrestre conectando países da América do Sul. Um dos principais movimentos neste jogo foi o anúncio de um cabo BRICS, conectando todos os países membros independentemente dos Estados Unidos[10]. Cada iniciativa articula diferentes ramos do governo brasileiro às empresas brasileiras ou transnacionais, e cada projeto é transnacional por sua própria natureza[11].

Este novo jogo resulta em uma expansão da razão de Estado digitalizada. Ao invés de uma fuga da *banda de Moebius*, Estados fazem geopolítica em seu interior. A geopolítica digitalizada assume que o ciberespaço é um campo de batalha e que os Estados devem criar suas próprias capacidades cibernéticas a fim de se defenderem e/ou devem se envolver em coalizões internacionais para enfrentarem os desafios da vigilância em massa e da espionagem digital. O efeito paradoxal deste jogo em particular é, em última análise, um reforço do regime da razão de Estado digitalizada por meio da resistência dos Estados contra a vigilância em massa. Reproduzindo a oposição entre segurança e liberdade, enquanto jogam o jogo da geopolítica digitalizada, Estados podem acabar subsumindo direitos e cidadania à lógica posicional da pessoa em causa. Enquanto lutam contra a vigilância em massa, Estados podem criar as condições adequadas para que eles mesmos a pratiquem.

4. Direitos Humanos e privacidade na era da vigilância: o poder da Lei Internacional?

As revelações de Snowden sobre a vigilância em massa não só tiveram substanciais repercussões políticas, em 2013 e 2014, como também suscitaram profundas questões legais. Nesta seção, examinamos algumas destas questões a partir da perspectiva dos movimentos políticos em torno delas. Vamos limitar ao mínimo o detalhe legal, focan-

10 Experts see Potential Perils in Brazil Push to Break with US-centric Internet over NSA Spying. Washington Post, 2013. Disponível em http://www.washingtonpost.com/world/europe/experts-see-potential-perils-in-brazil-push-to-break-withus-centric-internet-over-nsa-spying/2013/09/17/c9093f32-1f4e-11e3-9ad0-96244100e647_print.html. Acesso em 19/03/2014.

11 Empresas de telecomunicações brasileiras estão construindo cabos submarinos com financiamento público ou internacional. Por exemplo, o Expresso Atlântico Sul, cabo que liga o Brasil e a África do Sul, é financiado pelo Banco da China; o satélite é uma joint venture entre a empresa estatal Telebrás e a privada Embraer, com tecnologia fornecida pela empresa franco-italiana Thales Alenia. Brazil is Beating United States at its own Game. Al Jazeera, 2013. Disponível em http://america.aljazeera.com/articles/2013/9/20/brazil-internet-dilmarousseffnsa.html.

do, ao invés disso, em suas implicações para a tempestade de relações internacionais desencadeadas pelas revelações.

Duas questões de Direitos Humanos distintas, porém interligadas, surgem no que diz respeito à vigilância em massa. A primeira - embora seja a mais fundamental é também a mais frequentemente ignorada - é o direito de cada pessoa ao respeito de sua vida privada e familiar. A segunda - geralmente objeto de maior ruído político e midiático - é o dever dos Estados de proteção dos dados pessoais. Agentes políticos que têm interesse em promover a legalidade da vigilância em massa geralmente apresentam dois argumentos. O primeiro é de que a segurança nacional e internacional é sempre uma exceção tanto ao dever de cada Estado de respeitar à privacidade das pessoas quanto ao dever de proteger os dados pessoais. Este é o argumento mais vigorosamente defendido e, quando cai por terra, os agentes que procuram justificar a vigilância em massa encontram-se em frágil terreno legal. O segundo é que a obrigação dos Estados de proteção dos dados pessoais é sujeita a regras e requisitos muito distintos que variam de acordo com as preferências políticas dos diferentes Estados. Deste modo, como não existe um consenso em relação às normas específicas quanto ao que é uma proteção de dados internacionalmente aceitável, os Estados que exercem suas prerrogativas de segurança nacional e internacional só precisam cumprir suas próprias regras nacionais.

O direito ao respeito da privacidade e o direito à proteção de dados

Antes de analisarmos diretamente os argumentos e examinarmos como os agentes políticos insatisfeitos têm a eles respondido, gostaríamos de esclarecer, muito brevemente, a relação entre o direito ao respeito da vida privada e o direito à proteção de dados. O direito ao respeito da privacidade de uma pessoa é o direito humano internacional global. Este pode ser encontrado na Declaração Universal dos Direitos Humanos, de 1948[12], e sua forma jurídica consta no Pacto Internacional sobre os Direitos Civis e Políticos, de 1966[13]. Qualquer interferência na privacidade de uma pessoa deve estar sujeita, em primeiro lugar e acima de tudo, ao consentimento dessa pessoa. O direito de consentir ou recusar a utilização de dados pessoais pertence ao indivíduo, não ao Estado. Além disso, o consentimento só é válido se o indivíduo souber exatamente o que ele ou ela está consentindo. Este aspecto do direito exige uma limitação da finalidade em relação à coleta e ao uso de dados pessoais e proíbe o desvirtuamento da função. Quando o Estado interferir com o direito de coleta e utilização de dados pessoais, constituindo uma invasão à privacidade da pessoa em causa, tal interferência deve ser justificada pelas autoridades estatais. Primeiro, deve ser permitido por lei, e esta deve ser suficientemente clara e pública de modo que todos saibam seu conteúdo e como devem ajustar seu comportamento para conformar-se a ela. Qualquer exceção autorizada por lei a um direito humano deve ser interpretada de forma restritiva. É preciso que exista um objetivo legítimo e a necessidade de tal interferência para atingí-lo unicamente. Não pode haver qualquer alternativa menos intrusiva na vida da pessoa. É necessária a supervisão judicial de qualquer interferência do Estado e a pessoa afetada por tais interferências deve ter acesso à Justiça para contestá-las. Vigilância em massa, por sua própria natureza, não se destina especificamente a qualquer pessoa. Assim, a possibilidade de justificar a interferência à privacidade de qualquer pessoa individualmente é uma tarefa extremamente difícil. Sempre que tais

12 Artigo 12: Ninguém será sujeito a interferências arbitrárias na sua vida privada, família, lar ou correspondência, nem a ataques à sua honra e reputação. Toda pessoa tem direito à proteção da lei contra tais interferências ou ataques.
13 Artigo 17 (1): Ninguém será sujeito a interferências arbitrárias ou ilegais em sua vida privada, família, lar ou correspondência, nem a ofensas ilegais à sua honra e reputação.

técnicas de vigilância em massa pouco definidas foram utilizadas na Europa, o Tribunal de Direitos Humanos descobriu incompatibilidades com o direito à privacidade. Vigilância em massa é, por definição, arbitrária.

O dever dos Estados de proteção de dados surge a partir do direito do cidadão de respeito a sua privacidade. Quando Estados interfirirem na privacidade das pessoas, estes devem cumprir regras estritas para justificar tal interferência. Além disso, os Estados têm o dever de assegurar que os agentes do setor privado não violem a privacidade da pessoa. Assim, eles têm a obrigação de regular a coleta e utilização de dados pessoais pelo setor privado. Isto dá origem à obrigação da proteção de dados. O dever de proteger dados pessoais surge quando estes são utilizados por agentes estatais ou privados e é projetado para garantir que a utilização seja compatível com o direito individual de respeito da vida privada. É por esta razão que há muitos tipos diferentes de regimes de proteção de dados, dependendo do país em questão. Como os Estados procedem a esse respeito é de determinação dos mesmos; o ponto crucial é que os dados pessoais devem ser protegidos porque o indivíduo tem o direito ao respeito de sua vida privada. O conteúdo do direito humano ao respeito da privacidade não é variável.

A posição norte-americana em relação à Lei Internacional de Direitos Humanos e a iniciativa brasileira e alemã

Deslocando-se, então, do Estado de Direitos Humanos à luta política em termos de vigilância em massa, as autoridades norte-americanas confrontam-se, claramente, com um dilema na lei internacional de Direitos Humanos - uma área onde têm sido sempre bastante cautelosas. A abordagem dos anos 1950 em relação à lei internacional de Direitos Humanos sustentava que os instrumentos apenas estabelecem princípios, não são a lei "real" de forma significativa e, certamente, não estão disponíveis para as pessoas como apoio. Esta posição política tem sido minada pelo desenvolvimento de obrigações internacionais muito precisas, pela criação de Comitês de Tratados com competência para receber e decidir sobre queixas de indivíduos que alegarem violações de seus direitos humanos internacionais e pela adoção da lei por parte dos tribunais nacionais. A abordagem original à lei não se sustenta mais; é uma "cobertura" utilizada, ocasionalmente, por Estados que buscam agir de forma arbitrária.

Uma vez que as revelações de Snowden elevaram a escala de questões internacionais, um número de Estados, liderados principalmente por autoridades brasileiras e alemãs, levantaram a questão de como lidar com a vigilância em massa dos EUA e a interceptação da comunicação. Houve muita discussão acerca de negociações bilaterais, ações unilaterais (a construção de novos cabos que evitem território norte-americano, por exemplo) e assim por diante. No entanto, tornou-se rapidamente evidente que as proposições bilaterais e unilaterais não seriam satisfatórias. Na Europa, a vigilância em massa desempenhada pelas autoridades britânicas sobre seus parceiros norte-americanos e outros (os chamados *Five Eyes*) – não só membros do Conselho da Europa mas também da União Europeia - foi apenas um exemplo do problema das proposições unilaterais ou bilaterais. Claramente, para a maioria dos agentes, somente esforços multilaterais seriam capazes de contrabalancear o peso dos Estados Unidos e de alguns de seus colaboradores por meio de uma aliança informal de outros Estados. Tão logo o problema é definido desta forma, o lugar óbvio para se iniciar uma reação é a Assembleia Geral das Nações Unidas e o território de preparação da resposta corresponde àquele das obrigações internacionais dos Direitos Humanos - a

proibição de interferências arbitrárias na privacidade das pessoas.

Este é o caminho que as autoridades brasileiras e alemãs têm seguido. Em agosto de 2013, inciativas estavam em andamento por uma resolução da Assembleia Geral. Cinco organizações não governamentais – Acess, Amnistia Internacional, Fundação Electronic Frontier, Human Rights Watch e Privacy International - estavam intimamente ligadas aos esforços, pressionando por uma resolução assertiva. As autoridades brasileiras e alemãs não estavam sozinhas em seu empenho para chegarem a um acordo acerca de uma resolução da Assembleia Geral das Nações Unidas. Muitos Estados de menor dimensão - mais notadamente Áustria, Hungria, Liechtenstein, Noruega e Suíça mas também outros – apoiaram, fortemente, o trabalho desde o início, até mesmo destacando colaboradores para auxílio na carga de trabalho. A questão foi designada à Terceira Comissão da Assembleia Geral e é lá que as tensas negociações sobre o texto da resolução tiveram lugar. Um texto foi aprovado, em 26 de novembro, na Terceira Comissão e aprovado sem votação na Assembleia Geral das Nações Unidas, em 18 de dezembro de 2013.

A resolução se baseia no direito ao respeito da privacidade, presente na Declaração Universal e no Pacto Internacional sobre Direitos Civis e Políticos de 1966 (PIDCP), com referência específica à proibição de interferência arbitrária. Isso vincula o direito à privacidade ao direito à liberdade de expressão - se as pessoas estão sujeitas a vigilância em massa já não são capazes de se expressar livremente. O chamado efeito inibidor, o preâmbulo da resolução, insiste no impacto negativo que a vigilância e a interceptação de comunicação - incluindo a vigilância e a interceptação extraterritorial em larga escala - têm sobre o exercício e gozo dos Direitos Humanos. A resolução convoca os Estados a respeitarem o direito à privacidade e a impedirem violações, além de examinarem seus procedimentos, práticas e legislações sobre vigilância de comunicações, interceptação e coleta de dados pessoais - incluindo a vigilância em massa, interceptação e coleta, tendo em vista a defesa do direito à privacidade. A determinação também convoca os Estados a assegurarem a plena e efetiva aplicação de todas as obrigações decorrentes da lei internacional dos Direitos Humanos e a estabelecerem ou manterem mecanismos nacionais de supervisão independentes e eficazes, capazes de garantir a transparência e a prestação de contas de suas ações.

Acima de tudo, a resolução ordena ao Alto Comissário das Nações Unidas para os Direitos Humanos que apresente um relatório sobre a proteção e a promoção do direito à privacidade no contexto da vigilância doméstica e extraterritorial e/ou da interceptação de comunicações digitais e coleta de dados pessoais - incluindo em larga escala – ao Conselho de Direitos Humanos, em sua 27 ª sessão (setembro, 2014). A atual alta-comissária, Navi Pillay, uma jurista sul-africana com uma impressionante carreira em Direitos Humanos, foi nomeada para o cargo, em 2008. Ela não é estranha ao problema do direito à privacidade e à vigilância em massa, já tendo se pronunciado sobre o assunto no Conselho, em setembro.

O Conselho de Direitos Humanos das Nações Unidas (composto por 47 membros eleitos pela Assembleia Geral) também já está envolvido com a questão. O assunto constava da agenda da 24ª sessão do Conselho, realizada em setembro de 2013. A alta-comissária observou, nessa reunião, que a ameaça representada pela vigilância em massa é uma das situações mais prementes dos Direitos Humanos globais na a-

tualidade. Muitos deputados de Estado presentes na sessão mencionaram o parecer do Relator Especial da ONU sobre a promoção e proteção do direito à liberdade de opinião e de expressão (Frank La Rue, sobre a liberdade de expressão na era da Internet, em 16 de maio de 2011), que já havia delineado os diversos perigos da vigilância estatal e seu impacto sobre a liberdade de expressão. O surpreendente é que as reuniões de setembro e dezembro de 2013 do Conselho de Direitos Humanos receberam pouquíssima cobertura da imprensa. A reunião teve grande participação de representantes de Estados e as discussões referentes à condenação da vigilância em massa e à interceptação de comunicações foram incendiárias. Muitos representantes estaduais compareceram às reuniões com declarações de condenação à vigilância em massa e à interceptação de comunicações já preparadas e em consonância com os Estados vizinhos em nome dos quais foram ordenados a falar. Embora se pudesse, muito provavalmente, esperar que o representante alemão apresentasse um texto em nome de Áustria, Hungria, Liechtenstein, Noruega e Suíça era, talvez, menos óbvio que o Paquistão, falando em nome de Cuba, Venezuela, Zimbábue, Uganda, Equador, Rússia, Indonésia, Bolívia, Irã e China também apresentasse um texto condenando as práticas. Enquanto o contra-ataque, particularmente em relação a este segundo conjunto de países, é geralmente baseado em suas práticas internas de vigilância e em sugestões e até mesmo acusações de hipocrisia, a intervenção, no entanto, deve ser notada, assim como a possibilidade de um grupo de Estados com sérias discordâncias entre si ter escolhido um denominador comum sobre o assunto.

O próximo passo será a preparação e apresentação de um relatório da alta-comissária de Direitos Humanos ao Conselho de Direitos Humanos, em setembro de 2014. Sem dúvida, sua equipe será presenteada com quantidades substanciais de informações, provas e argumentos legais para auxílio na escrita do relatório.

5. Inteligência, democracia, soberania: que *demos* para que segurança?

Graças à documentação distribuída por Snowden e outros, sabemos agora mais do que sabíamos sobre o caráter e a extensão das práticas de coleta de informações de várias agências encarregadas de aumentar nossa segurança. O que sabemos, precisamente, o que não sabemos e o que isso acrescenta ao nosso limitado conhecimento permanece incerto, de modo a desafiar tanto a análise acadêmica quanto a nossa percepção de como reagir por meio de políticas, procedimentos, instituições e ações coletivas. Pode-se ou não incomodar-se com o que se tornou conhecido, mas certamente o que se tornou conhecido perturba entendimentos convencionais acerca de práticas de segurança - e não unicamente de segurança. Por outro lado, a antiga suspeita de que as agências que afirmam proteger a nossa vida e bem-estar são, muitas vezes, extremamente perigosas mantém sensatez considerável.

É neste contexto que podemos avaliar muitas das respostas iniciais às conseqüências imediatas dos padrões identificados. Privacidade, Direitos Humanos e Estado de Direito tornaram-se princípios profundamente arraigados nas sociedades modernas - mesmo que conquistados de forma imperfeita - especialmente naquelas que afirmam algum tipo de liberalismo. Snowden trouxe evidências consideráveis de que tais conquistas são tratadas com desdém, seja voluntariamente ou até mesmo em tom conspiratório, por ignorância, ingenuidade ou através de processos estruturais que ninguém entende por completo. Além disso, o desdém foi redistribuído aos amigos bem como aos inimigos, aos cidadãos e aos estrangeiros, de forma que generaliza a mácula da suspeita e põe em questão tudo o que pensávamos que sabíamos sobre o

papel da consciência individual, da liberdade de expressão, da inocência e culpa, da liberdade e responsabilidade, do público e privado. Apologistas de meios mais intrusivos e secretos de segurança invocam, frequentemente, narrativas extremistas sobre as ameaças que podemos enfrentar. Mas não é difícil imaginar narrativas igualmente extremas sobre a evisceração das formas de subjetividade moderna e autodeterminação que muito legitimam agências de segurança. O que, afinal de contas, elas supostamente devem proteger?

É improvável que "a democracia" seja a resposta imediata dada por profissionais de segurança, apesar da retórica de muitos políticos. É preferível o Estado ou a nação: a condição de possibilitar um coletivo de cidadãos alicerçados em um local geográfico específico que pode ou não alcançar formas democráticas de governo; ou talvez o sistema internacional, que é a condição possível desta condição de possibilidade; ou, mais precisamente, a frágil e desajeitada interação de Estados dentro de um sistema que nos dá alguma possibilidade de conciliação de nossas reivindicações de cidadanias particulares e nacionalidades com nosso estatuto universal de seres humanos. Concepções tradicionais de segurança podem estar divididas entre campos nacionalistas e internacionalistas, entre a segurança nacional e a segurança coletiva - como a Carta das Nações Unidas coloca. Mas as fraquezas evidentes de ambos os campos só servem para sublinhar a sua dependência mútua enquanto expressões dos princípios concorrentes de autodeterminação e universalidade que moldam a vida política moderna. Uma das principais complicações aqui é que alguns Estados, e atualmente, um Estado age como se fosse particular e universal: não apenas um Estado soberano com um problema de segurança nacional mas também uma hegemonia global responsável por algo mais abrangente. Outras complicações incluem o fato de que os processos econômicos não são sempre subsidiários da ordem política dos Estados internacionalizados.

O que é especialmente interessante, nos padrões identificados nas informações divulgadas por Snowden, é a confirmação potencial das alegações de que agora vivemos em um mundo que não é organizado nem no interior de Estados que atuam dentro de um sistema estadual e nem em uma hierarquia embrionária - como prevista pelos teóricos da globalização, da governança global, e assim por diante. Nem em um novo tipo de império e nem em um conjunto de grandes potências. Além disso, não é sensato supor que esses padrões possam ser interpretados sem alguma compreensão acerca dos deslocamentos contemporâneos rumo a mercados globalizados e à riqueza corporativa como principal medida de valor econômico e até político. Algumas das respostas às revelações de Snowden sugerem que o velho modelo nacional/internacional ainda está vivo. Mas muitas também sugerem que algo menos previsível está ocorrendo. Algumas indicações dessa imprevisibilidade são insinuadas pelos diversos meios através dos quais as práticas das agências de inteligência, como a NSA, desafiam nossas suposições sobre Democracia.

Neste contexto, é importante lembrar que a Democracia, juntamente com outras formas de pluralismo político, é convencionalmente algo que pode ser limitado ou mesmo sacrificado para garantir a ordem primária dos Estados-nações em um sistema como tal. Contudo, o que está especialmente em causa nas revelações recentes não é apenas a questão tradicional de quando é possível a suspensão de normas democráticas, a fim de mobilizar operações de segurança mais eficazes; ou traçar uma linha nítida entre uma arena civil, em que as normas democráticas sejam adequadas, e uma área de segurança, em que a democracia deve ceder - embora muitas narrativas

apologéticas certamente reproduzam esta tradição. É, antes, a aparente rearticulação de ambos os limites entre os Estados e entre o Estado, como a sede da necessidade política, e a sociedade civil, como uma arena de liberdade política e pessoal. E assim, em ambos os casos, entre as exigências de segurança e as possibilidades de liberdade ou autodeterminação. Se isto for realmente parte do padrão que está surgindo, o significado tanto de segurança quanto de Democracia, bem como a relação entre ambas, será radicalmente desestabilizado, e não manisfestamente para melhor.

Além das discussões anteriores sobre privacidade, Estado de Direito e várias tentativas de resistência a pretensões imperiais, outras quatro linhas de análise merecem ênfase a este respeito. Todas se referem aos limites das dicotomias entre nacional e internacional, Estado e sociedade civil, liberdade e segurança, Democracia e conhecimento que são, invariavelmente, reproduzidos em análise convencional e debate público. O estatuto incerto da soberania é evidente em todos os quatro casos (por razões amplamente descritas por Walker, em 2010).

Em primeiro lugar, o nosso mundo político não é nem nacional nem internacional, embora a presunção de que ainda o seja sustente ideais políticos amplamente difundidos. A documentação de Snowden confirma que as incertezas sobre como devemos entender a Democracia, dada à dinâmica que está redefinindo as relações entre os Estados e entre os Estados e as sociedades civis, estão se fundindo rapidamente às incertezas sobre como devemos localizar as ordens políticas que estão sendo estruturadas em relação a novas redes de agências de inteligência e de segurança. Claramente, não estamos falando aqui sobre a imagem clássica dos Estados de segurança nacional. Estas redes são variadamente internacionais e transnacionais, com cartografias que mais parecem circuitos elétricos do que propriedades territoriais. Fronteiras tornaram-se fenômenos indefinidos, de forma que exigem meios desconhecidos de compreensão acerca dos modos de subordinação dos vários subsistemas, das lealdades conflitantes, das cidadanias divididas e dos deslocamentos da estrutura espaço-temporal dentro da qual nós sabemos onde e quando estamos e quem somos. No entanto, embora evasivas, as fronteiras não estão sendo apagadas. É possível que a NSA e outras agências de inteligência funcionem através de redes que escapem a muitas fronteiras, mas as suas próprias razões de existência são precisamente para afirmar limites de inclusão e exclusão, tanto familiares quanto não familiares. Diante das evidências de novos padrões de desigualdade em todo o mundo, devemos, certamente, ter muito cuidado com a perspectiva de novas formas de inclusão e exclusão ordenadas através de novas tecnologias de controle populacional.

Em segundo lugar, uma característica-chave das descrições mais influentes acerca da Democracia, ao longo do século XX, foi a distinção entre Estado e sociedade civil e distinções relacionadas entre público e privado. Estas distinções têm sido, muitas vezes, confusas. No entanto, evidências recentes sugerem um fortalecimento ainda maior da erosão de tais distinções e um direito presumido das agências estatais de penetrarem profundamente nos mundos cotidianos da sociedade civil e da vida privada. Isto não assume a forma de Estados policiais totalizantes da memória recente. Entretanto, é claro que os novos procedimentos de operações de inteligência, coleta de dados, mobilização de suspeitas e identificação de potenciais ameaças - especialmente os que confiam mais em manipulações computacionais de provas que podem ou não ter credibilidade empírica e que dependem de probabilidades estatísticas no âmbito de populações abstraídas para identificar indivíduos em particular - representam perigos às liberdades e direitos estabelecidos que são análogos aos regimes que preferimos

imaginar como definitivamente superados por revoluções, democratizações e modernizações. Aqui, parte da dificuldade analítica surge a partir de uma dinâmica dupla: por um lado, vemos uma complexa interação entre órgãos públicos e privados – sem esquecermos as agências de capital social e de mercado mais do que de cidadania liberal - e, por outro, vemos evidências de complexas redes de agências de inteligência e de segurança que parecem ter alcançado uma considerável autonomia tanto do Estado quanto da sociedade civil ou, em uma linguagem relacionada, tanto da soberania do Estado quanto da soberania popular.

Em terceiro lugar, um número demasiadamente grande de análises políticas e debates inicia-se, atualmente, com o tema da segurança, como se esta fosse um problema, em princípio, capaz de se sustentar em seus próprios termos, ou mesmo o princípio primário que supera todo o resto. A tendência é comum mesmo entre literaturas supostamente "críticas". Embora alguns tenham sustentado esta primazia como um simples fato (sócio-darwinista) da vida, nenhuma discussão sobre Democracia moderna - ou qualquer outro princípio da política moderna - pode se dar ao luxo de cometer um erro tão elementar. Como muitos dos autores canônicos apropriados pelos analistas de segurança do nosso tempo reconheceram (de Maquiavel a Hobbes, passando por Kant, Clausewitz, Schmitt e até mesmo a algumas versões do conceito de segurança nacional), afirmações sobre segurança implicam que há algo a ser protegido. Este algo refere-se, geralmente, a uma comunidade política específica ligada, internamente, a princípios de liberdade e igualdade e com uma capacidade de autodeterminação em relação a outras comunidades semelhantes. Obviamente, no presente contexto, isso gerou tensões de longa data entre reivindicações de liberdade e reivindicações de segurança. Esta é uma tensão que foi eclipsada pela divisão do trabalho intelectual que transformou a segurança em uma especialização autônoma a ser perseguida com pouca consideração ou desdém considerável pelas liberdades do "povo", em nome de quem a segurança é utilizada como um trunfo. O caráter preciso dessa tensão também foi despolitizado por repetidas declarações de que um "equilíbrio" deve ser atingido entre dois valores diferentes.

No entanto, a relação entre liberdade e segurança não pode ser compreendida como um equilíbrio no sentido habitual deste termo. A segurança dita as condições sob as quais o valor principal da liberdade deve atingir os seus limites e sob quais pressupostos normais, injunções éticas e leis deve ser suspenso. Qualquer suspensão do tipo é, classicamente, responsabilidade do Estado soberano e está, portanto, em desacordo com as responsabilidades de um povo soberano. Por conseguinte, a relação entre essas duas compreensões antagônicas de soberania tem que ser negociada. Em algumas influentes leituras (fascistas, autoritárias, totalitárias), negociação significa simplesmente uma decisão soberana de suspensão da norma em nome de um povo ou nação: a soberania do Estado deve triunfar sobre a soberania popular. Tradições democráticas têm sido obrigadas a ajustarem-se às exigências da segurança como condição-limite, geralmente insistindo em um exame minucioso das decisões, divisões de competências institucionais e das condições legais sob as quais as leis podem ser suspensas. Não se trata de escolher produtos em um mercado. Invocações retóricas de equilíbrio simplesmente obscurecem e ameaçam o que está acontecendo no que talvez seja o ponto mais importante, intenso e esquecido da prática democrática moderna. O caminho fica livre, então, para alegações factuais de que as responsabilidades de soberania cabem àqueles responsáveis pela nossa segurança e que o espaço de negociação aberto a todos os supostamente protegidos deve ser reduzido. Considerando tanto a extensão das ameaças plausíveis que confrontam as

sociedades contemporâneas quanto, especialmente, a capacidade de uma variedade de agências de segurança de identificar algumas ameaças ao invés de outras e impulsionar a segurança como o princípio fundamental que rege nossas vidas, o que se entendia, antes, como opções autoritárias, agora parecem desejáveis e, até mesmo, naturais.

Por último, mas não menos importante, a demanda não contida de sigilo por parte das agências de inteligência e de segurança é devastadora. A Democracia sempre foi ligada à qualidade do conhecimento dentro de um demos: da pólis grega ao Iluminismo europeu até o valor mais recentemente dado à educação, ao jornalismo investigativo e à opinião pública, a maioria das concepções de Democracia apoiam-se, em alguma medida, no fato de que as pessoas são capazes de pensar e tomar decisões por si mesmas. O culto do segredo nos leva de volta a uma infinidade de casos históricos em que foram apresentadas alegações de que "o povo" não pode saber o que é bom para ele, enquanto o seu soberano precisa saber o máximo possível acerca do povo cuja soberania alega expressar. Assim, de que autoridade estamos falando aqui? Ou, como Thomas Hobbes colocaria, como a autoridade é agora autorizada?

6. Subjetividade e Vigilância no Ciberespaço

A transformação do cidadão em suspeito não é um fenômeno novo, como Hobbes confirma em seu discurso sobre a subversão e o poder soberano. Onde o mundo de Hobbes é territorialmente confinado, o mundo das agências de segurança modernas recentes é global e transnacional. A distinção entre cidadão e não-cidadão pode ser testemunhada em cada passagem de fronteira onde o não-cidadão é submetido à identificação biométrica, à exposição corporal total e a outros modos de escrutínio; o viajante, enquanto isso, é simplesmente resignado à panóplia de subjetivações humilhantes. Há, neste regime de práticas de segurança, neste terreno de passagem de fronteiras, um processo de aprendizagem que governa o comportamento: o nosso limite de tolerância a tais intervenções e, de muitas maneiras, a nossa agora estabelecida indiferença ou até mesmo cumplicidade com os desconfortos do outro.

É essa indiferença que é posta em questão a partir das revelações de Snowden – a de que todos os cidadãos de qualquer Estado, líderes e liderados, qualquer ser que se comunique, qualquer usuário de modernas tecnologias de comunicação recentes é tornado suspeito. No entanto, o conceito de suspeito é agora completamente transformado, já não somos capazes de confiná-lo ao seu sentido jurídico - que se refere à criminalidade - nem somos capazes de limitar o seu significado a sua interação sócio-política relativa à inimizade ou potencial subversão.

O que está claro é que o tema da vigilância é agora um assunto cujas práticas comunicativas são vistas pelos órgãos de vigilância como dotadas de potencial valor informativo ou utilidade, onde este valor pode relacionar-se com a segurança ou a economia. Portanto, não é que somos todos suspeitos agora, mas sim que nossas entradas de dados e redes podem ser valiosas e entendidas em termos de utilidade, em algum momento no futuro. Enquanto o indivíduo se comunica no ciberespaço, talvez haja alguma consciência de que a rede de comunicação é monitorada, registrada e armazenada de diversas formas. No entanto, existe uma falta de conhecimento acerca da utilidade informativa acumulada por esta comunicação pelas agências de vigilância. O modo como a vigilância em massa das comunicações pode impactar o comportamento é claramente uma questão pertinente. Entretanto, assim como o indivíduo

que viaja adapta-se e conforma-se às normas de viagem, também há, neste caso, um processo de adaptação e criatividade nos modos de autogoverno que prevalece em face de nossa moderna e tardia intensificação de práticas de vigilância.

A complexa interseção entre público e privado aparece de forma mais acentuada no ciberespaço. Há tanto intimidade quanto presença pública aqui. No entanto, é a intimidade que prevalece, independentemente do fato de que o indivíduo das práticas cibercomunicativas está plenamente consciente de que o ciberespaço, como tal, está aberto ao mundo e vulnerável ao olhar estrangeiro - seja o do hacker, o do marqueteiro ou até mesmo o do Estado. "Ser digital" (Negroponte, 1995) é estar ligado e em rede, presente neste terreno distinto de interação social, um espaço desenhado e habilitado por códigos de rede que desconhecem fronteiras, exceto as técnicas. O sujeito cibernético é designado e configurado como um ser que surge e é produzido por formas desencarnadas de performatividades que constituem o ciberespaço (ver, por exemplo, Lucas, 1999). Lucas sugere que o ciberespaço pode ser entendido como uma "estrutura social", onde "novas subjetividades" e formas de agência são produzidas. De maneira mais útil, no entanto, podemos compreender esse terreno como a manifestação de um espaço, a cartografia de uma matriz multitudinal de sobreposições, linhas e nós de interseções que refletem bilhões de comunicações mundo afora. No entanto, no meio destas complexidades em rede, a "consciência prática" do ser digital pressupõe intimidade, apesar das circunstâncias.

O que, muitas vezes, é representado como uma mudança geracional significativa reflete a autorrevelação do indivíduo, não apenas a amigos e familiares, mas potencialmente a todos os "clientes" que utilizam veículos de redes sociais. O pressuposto fundamental de quem se comunica dessa maneira - especialmente aqueles nas sociedades democráticas liberais, mas que, certamente, não se limita a estes - é o controle soberano, a soberania do eu compreendida em termos de liberdade de expressão, comunicação e mobilização em um terreno desterritorializado que pode, potencialmente, desafiar estruturas de poder e dominação. O desafio à distância equipara-se, aqui, de algum modo, ao desafio à autoridade territorialmente delimitada, de forma que mesmo quando tal autoridade visa afirmar presença, o imaginário é uma possibilidade e, até mesmo, uma transgressão. Esta foi a narrativa que alimentou interpretações da chamada Primavera Árabe, das manifestações de Londres, do movimento antiglobalização e outras expressões de protesto e resistência em todo o mundo (ver, por exemplo, Gerbaudo, 2012). Ali estava e, talvez podemos dizer, está a instanciação de uma esfera pública global (Castells, 2008). As práticas comunicacionais que acontecem em seu âmbito, que podem, variadamente, responsabilizar as autoridades, mobilizam fronteiras por dentro e através dos territórios e, ao fazê-lo, constituem outro espaço totalmente diferente, um mundo interconectado cosmopolita, onde o cosmopolitismo é, de uma só vez, da diferença e da homogeneidade.

No entanto, é esta indefinição precisa de fronteiras, este campo ilimitado do possível - em que a diferença pode habitar o familiar, o homogêneo - que suscita e desafia um aparato de segurança que, como Foucault (2007) nos diz, não funciona a partir de um modelo repressivo, mas antes a partir de um modelo produtivo, permissivo e autorizado. Este é o triunfo do liberalismo pois, aqui, qualquer prática repressiva é uma prática regressiva. É uma decepção para todas as suas sofisticadas realizações e todas as suas marcas distintivas – distantes do Zimbábue de Mugabe e da China comunista. O exemplo liberal é o da segurança por meio da liberdade e não o da segurança em detrimento da liberdade. O ciberespaço representa a manifestação tecnológica de uma

liberdade transformadora, em que práticas comunicacionais – sejam políticas, sócio-culturais, pedagógicas ou econômicas – podem ganhar espaço. A questão imposta à autoridade política - e estamos aqui nos concentrando na autoridade política liberal - foi como regular este terreno de comunicação desenfreado e quais tecnologias de controle, não sujeitas aos limites das fronteiras nacionais e da autoridade soberana dos Estados definidos, devem mobilizar. Se tais tecnologias pudessem ser criadas, elas também teriam que funcionar em rede, ser digitalmente definidas em software e não em *hardware*, e ser ocultas e, ainda assim, transnacionais e globais em seu alcance.

A informática é, atualmente, a disciplina de escolha do poder liberal. No entanto, apesar do foco no *software* e dos conhecimentos de codificação processados em formato digital, o hardware também é importante na materialidade das tecnologias destinadas a controlar este espaço ilimitado. Dos discos de armazenamento nos computadores aos cabos submarinos, estes são os elementos e as engenharias tecnológicas de uma maquinaria que serve à liberdade de comunicar e à capacidade de monitoramento e controle. Dentro deste quadro de conhecimento disciplinar - como acontece com todos os sistemas de conhecimento e as formações discursivas que asseguram sua reprodução - o sujeito epistêmico orienta-se por um terreno inseguro, entre política e governo, resistência (podemos pensar em grupos como o *Anonymous* ou o *Hacked-Off*; ver Coleman, 2011) e trabalho, a serviço do mercado digital ou do Estado. A dificuldade é que não há dualismo ou oposição entre esses termos, já que um se baseia no outro. Assim, o mundo do *hacker* resistente, um conhecimento desenvolvido no estudo da intimidade, é baseado e, talvez, aperfeiçoado, a partir de recursos disponíveis para os provedores de serviço ou para o Estado. Raramente, o movimento se dá a partir do mundo do Estado para o indivíduo que resiste. O poder vem a permear o conhecimento e o sujeito produzido nesta complexa matriz já é, sempre, cúmplice e encontra-se envolvido, de alguma forma, em sua reprodução. Rastrear estas conexões e mapear não apenas as redes e seus nós, mas também estes entrelaçamentos intrincados de poder, conhecimentos e subjetividades é a tarefa de qualquer intervenção crítica no ciberespaço, em sua constituição diária por meio de práticas e estruturas de conhecimento e seu poder constitutivo de subjetivação.

Muitos, talvez, sustentem que comunicações virtuais significam o "fim da privacidade" (como previsto em Whitaker, 1998). Este é o pano de fundo para as revelações de Snowden. Independentemente do conhecimento de causa que temos, como usuários do ciberespaço, sobre a possibilidade e mesmo sobre a realidade do perfil como sonho do anunciante em um mercado global digital, o jogo assume uma dinâmica completamente diferente quando o perfil pertence ao Estado e, de modo ainda mais significativo, quando o perfil pode ser de qualquer pessoa ao redor do mundo. Um espaço onde o desafio aos obstáculos técnicos e comunicacionais foi traduzido, em muitos casos, como um desafio ao poder, de repente, e graças a Edward Snowden, revelou-se suscetível à penetração mais intervencionista do sujeito da comunicação por parte de um poder soberano que concebe o mundo dentro de sua esfera de operações. Nessa articulação desterritorializada de poder, os limites parecem irrelevantes; distinções entre amigo e inimigo, nacional e internacional, público e privado parecem se dissolver. Neste mundo "arrastado" pela vigilância, cada instância de comunicação é gravada digitalmente, diversamente armazenada e o triunfo - frequentemente retratado nos documentos vazados da NSA na forma de um sorriso (ver os Arquivos NSA, do The Guardian, acerca dos papéis revelados recentemente na operação denominada *Dishfire*) - é definido como a capacidade de captura de centenas de milhões de comunicações por SMS por dia.

Politicamente, a linguagem vem a ser o terreno sobre o qual e através do qual modos de legitimação e deslegitimação têm lugar. A terminologia preferencial dos defensores da NSA e do GCHQ é "acesso em massa" em oposição à "vigilância em massa"[14]. O último é reminiscente dos tempos da Stasi, na Alemanha Oriental, e qualquer semelhança com as atividades da Stasi é contestada. O termo "acesso em massa" sugere operações que visam à descoberta de "agulhas no palheiro", do indivíduo terrorista ou da célula de terroristas determinada a ordenar uma atrocidade em algum lugar e momento imprevisíveis. De fato, o secretário britânico de Relações Exteriores, William Hague, sugeriu isso quando afirmou: "se você não tem nada a esconder, não tem nada com o que se preocupar." A operação de vigilância é aqui considerada uma operação de peneiramento, onde a "massa" passa despercebida e livre pela peneira, enquanto a comunicação anormal e singular é capturada e, por meio dela, o potencial autor de um ato de violência terrorista. Quando comunicações de líderes mundiais e de empresas petrolíferas também são apreendidas no "arrastão", estes são exemplos infelizes e colaterais que uma operação de acesso em massa pode involuntariamente capturar.

No entanto, se insistirmos no termo "vigilância em massa", o foco é sobre a "vigilância" da "massa", onde a massa pode ser entendida não como o terreno biopolítico da população, mas, mais radicalmente, como uma "multidão" de comunicações singulares e em rede sujeitas à vigilância, ainda que "dados" apareçam digitalmente em um perfil de rede revelado por "metadados" ou mesmo por "conteúdo." O sujeito da vigilância não é, portanto, simplesmente parte de uma população - embora possa-se considerar o "perfil" como veículo de populações particulares – mas, acima de tudo, o sujeito individual da comunicação. É neste sentido que o espaço da intimidade é, sabemos agora, absolutamente penetrado por estas agências, de modo que um perfil é construído a partir dos rastros digitais deixados pelo sujeito interativo e da comunicação.

Os rastros serão deixados em toda sua intimidade e com o pleno conhecimento de que esta não é mais privada e que as agências envolvidas na vigilância têm acesso. A fórmula "liberdade por meio da segurança", quando compreendida normativamente, não prevê limites para tal acessibilidade. No entanto, a concepção positiva dos direitos estipula – e esta é a grande brecha – o limite reconhecido na lei, como indicado em outras partes deste artigo, onde é conferido à privacidade valor cultural e também jurídico.

7. Convivendo com a vigilância: resignação, perplexidade e resistência

Quaisquer que sejam as respostas específicas às revelações de Edward Snowden sobre a vigilância em massa e a NSA, é evidente que a opinião pública despertou e muitos ao redor do mundo estão discutindo as descobertas progressivas feitas acerca das agências de segurança e da inteligência nacional. É igualmente claro que membros do sistema têm se movimentado rapidamente para sublinhar a necessidade de tal vigilância em nome da "segurança nacional" ou da "ordem pública". A resposta oficial do presidente Obama para as revelações de Snowden, declarada em janeiro de 2014, reforça alegações de que a vigilância em massa do governo é necessária e chama atenção para a vigilância das empresas do setor privado, exigindo mais fiscalização (Podesta, 2014).

14 O termo "acesso em massa" foi utilizado por Sir David Omand, ex-Director do GCHQ do Reino Unido, como a forma mais apropriada para descrever as atividades da NSA e do GCHQ. Consulte M*ass Electronic Surveillance and Liberal Democracy, do Research Centre in International Relations, do Department of War Studies, King's College London*, 21/01/2014.

Mas o que dizer dos cidadãos comuns e dos consumidores, discorrendo sobre suas vidas cotidianas, com um crescente sentimento de que talvez suas atividades e suas comunicações estejam sendo rastreadas e monitoradas mais do que eles têm conhecimento? É claro que não há nada direto ou descarado como um *Big Brother* em uma tele gritante, mas um mal-estar mais kafkiano de que os metadados ostensivamente inocentes (localização, duração e destinatários das chamadas, por exemplo) têm de fato consequências. Mas tudo parece muito fluido, escorregadio e difícil de entender. De fato, parece corresponder à própria qualidade das relações que caracterizam uma cultura orientada pelo consumo – fissípara, mutante e flutuando por meio de canais e veículos em constante mudança. Isso tem sido chamado de "vigilância líquida" (Bauman e Lyon, 2013).

Compreender a opinião pública é notoriamente difícil mas, ao se abordar a questão a partir de vários ângulos, talvez seja possível uma leitura sobre o que está acontecendo e como as pessoas têm respondido às revelações. Há medidas diretas - como pesquisas ou entrevistas menos superficiais e etnografias - e abordagens indiretas, situando a questão em um contexto cultural e histórico, em uma tentativa de discernir os sinais dos tempos. Cada uma tem um próposito e podemos, ao menos, dar os primeiros passos, não obstante reconhecendo tanto as dificuldades decorrentes do fato de que apenas alguns meses se passaram, desde que Snowden iniciou seu programa, em junho de 2013, e do fato de que as experiências variam, amplamente, entre regiões e países afetados pela vigilância dos Estados Unidos.

Uma pesquisa global da Angus Reid, realizada no final do ano passado (Reid, 2013), mostrou que o que se pensa sobre Snowden depende, em parte, de onde se está. Assim, 51% dos americanos consideram Snowden um herói por "deixar o público saber que os nossos governos estão executando programas de vigilância eletrônica que ameaçam a privacidade das pessoas", enquanto 49% o consideram um traidor que "ameaça as operações de inteligência ocidentais." No entanto, 60% dizem que a difusão da vigilância em massa do governo é inaceitável. Contudo, em outros países, o apoio à Snowden é mais elevado: 67% dos canadenses e 60% dos britânicos veem sua denúncia de irregularidades como positiva. Apenas 5% dos entrevistados no Canadá confiam no governo para proteção de seus dados e essa porcentagem só aumenta para 7% nos Estados Unidos. Seja nos Estados Unidos, no Canadá ou no Reino Unido, é evidente, a partir destes resultados, que uma proporção substancial da população está preocupada com a vigilância do governo e que há um alto grau de cinismo sobre o que os governos fazem com esses dados.

Considerando que o caso Snowden é tão recente, há pouca análise aprofundada sobre a visão das pessoas sobre a vigilância em massa conduzida pelo governo, tampouco etnografias pós-Snowden de como estão agora organizando suas vidas diárias em relação a seus dados online. Diante disso, temos que recorrer a análises mais amplas e de longo prazo acerca dos comportamentos. O trabalho de Snowden revelou evidências de até que ponto a NSA e as agências relacionadas dependem de empresas de Internet e plataformas de mídia social, como o Facebook, para o acesso a dados transacionais e interacionais. Mas, para a maioria dos usuários de mídias sociais, a vigilância como poder hierárquico parece ter pouca importância, a não ser para aqueles que vivem em zonas de conflito ou em países com repressão política aberta. É muito mais provável que se sintam atraídos pela vigilância social (Marwick, 2012) em que, nas capilaridades do poder, de acordo com Foucault, os diferenciais de poder das interações cotidianas são mais urgentemente significativos do que qualquer coisa que

a NSA e suas agências correlacionadas estejam fazendo. Isso não equivale dizer que a conscientização não vá aumentar, particularmente em relação a eventos globais, como a coordenada resistência online, *the-day-we-fight-back*, em 11 de fevereiro de 2014.

O contexto mais amplo das revelações de Snowden não é meramente o declínio da participação política dentro dos Estados democráticos liberais mas também, como Agamben sugeriu, o colapso da própria política. Agamben insiste que, sob o signo da segurança, os Estados de hoje transitaram da política ao policiamento e do governo ao gerenciamento – utilizando sistemas de vigilância habilitados eletronicamente - pondo em questão, assim, a própria possibilidade de política (Agamben, 2013). O fato disto ocorrer simultaneamente junto ao crescimento de todos os tipos de vigilância, e não apenas daqueles associados a comunicações e transações, é um mau presságio no tocante às chances de uma política renovada, especialmente quando, em um nível mundano, as culturas de vigilância parecem tão inócuas.

Três tipos de fatores, provavelmente, ajudam a indicar porque todas as formas de vigilância ainda parecem publicamente aceitáveis para muitos, embora também se deva notar que tais fatores podem se sobrepor para reforçar ou enfraquecer um ao outro em contextos específicos.

O primeiro é a familiaridade. A vigilância é hoje tão difundida e tem tantas dimensões que, simplesmente, tornou-se parte da vida cotidiana. A vigilância em torno de nós dá-se em muitos contextos, não apenas o óbvio (ou, hoje, não tão óbvio, porque eles são miniaturizados): câmeras de vídeo na rua, shoppings, escolas, procedimentos de segurança nos aeroportos e também nos próprios edifícios, veículos e dispositivos que usamos no dia a dia. A vigilância é incorporada em carros (GPS, Internet, gravadores de dados e câmeras de alta resolução) e edifícios (sistemas de cartão de acesso, sensores). Assim, muitos destes procedimentos são simplesmente aceitos; eles são domesticados, normais, despercebidos. Muitos já não os notam e certamente não pensam sobre as suas capacidades de vigilância (New Transparency, 2014).

O segundo é o medo que, muitos argumentam, tornou-se mais significativo desde 9/11 (Lyon, 2003; Bauman, 2005). Governos, empresas de segurança e a mídia jogam, cinicamente, com o fator medo, que tem efeito inibidor bem como efeitos diretos. O medo funciona para empresas que tentam vender novos equipamentos; para governos que veem como tarefa permitir mais controle por parte das forças de mercado e manutenção da segurança; e para a mídia que depende da polarização "mocinhos contra bandidos", especialmente se o "mal" pode ser pensado em termos "muçulmanos" (Kurzman, 2011). Os efeitos de inibição ocorrem, por exemplo, quando políticos ou jornalistas não distinguem claramente entre aqueles que são realmente terroristas e outros que podem ser manifestantes legais (contra a degradação ambiental, abusos de Direitos Humanos ou exploração indígena) ou imigrantes em situação irregular. Os níveis de medo superam amplamente as estatísticas reais da atividade terrorista e, sem dúvida, incentivam uma aceitação da vigilância intensificada.

O fenômeno da "diversão" é o terceiro fator crítico a fomentar a vigilância intensificada. Isto pode soar um tanto trivial no contexto dos temores pós-11 de setembro, mas não é insignificante que a mídia social também tenha se expandido exponencialmente durante a última década, através de meios que se apoiam mutuamente. A chave para se entender a mídia social é a sua premissa básica, a do "conteúdo gerado

pelo usuário". Na chamada Web 2.0, a informação não é fornecida apenas por grandes organizações - antes, todos participam.

A Wikipedia foi talvez o primeiro modelo popular. As mídias sociais, no entanto, funcionam não só através das entradas do usuário mas, fundamentalmente, por meio de relações entre diferentes usuários - sendo o Facebook, ainda, o exemplo mais óbvio e generalizado. Além disso, as pessoas participam do Facebook e de outras mídias sociais usando suas identidades reais, conectando-se com outros de visão semelhante. Esta "vigilância social" (Marwick, 2013; também chamada de "vigilância entre pares" ou "vigilância lateral") é, decididamente, agradável para os participantes. A reunião de grupos que gostam das mesmas músicas, filmes ou esportes é realizada pelos próprios usuários, antes que o trabalho (de empresas de *marketing* de Internet) de dividí-los através de algoritmos comece. Meios de comunicação social continuam extremamente populares e, enquanto podem ser um potente meio de formação da opinião política e protesto, eles também fornecem a matéria-prima de dados tanto para corporações quanto, como Snowden tem nos mostrado, para a polícia e as agências de inteligência.

"Tudo parece tão fluido, escorregadio e difícil de entender" para os "cidadãos comuns e para os consumidores." A pessoa sente e sabe que está sendo vigiada, mas não sabe (e não tem muito cuidado) por quem e com que finalidade. Câmeras de TV são, hoje em dia, talvez a visão mais corriqueira em todas as esquinas – em ruas igualmente movimentadas e despovoadas. Elas são tão comuns que não são mais notadas - "escondidas na luz", ou melhor, em sua familiaridade. De fato, elas nada escondem - elas anunciam a sua presença, descaradamente e com orgulho. E há algo mais que as diferencia da câmera escondida na tela da televisão do quarto de solteiro de Winston Smith: elas não te observam para mantê-lo na linha e dentro do esquema previsto; elas não transmitem comandos; elas não roubam a sua livre vontade, escolha e capacidade de definir suas próprias preferências. Elas estão onde estão (ou seja, em todos os lugares) a fim de manter você e as liberdades que tanto aprecia em segurança.

Apesar da plena consciência da onipresença da espionagem (renomeada, no jargão politicamente correto, de "coleta de dados") e da extensão dos "bancos de dados" produzidos (tendo deixado para trás tudo o que as CIAs, KGBs e Stasi nunca conseguiram acumular no passado, com todas as suas incontáveis legiões de informantes pagos), a profundidade e a dimensão da equanimidade com a qual as revelações de Snowden foram recebidas pelos "cidadãos comuns e pelos consumidores" foi surpreendente. Se esperavam elevados índices de audiência e vendas de jornais, os profissionais dos meios de comunicação se enganaram. Apesar de suas sérias tentativas, as revelações de Snowden causaram pouquíssimos tremores, onde se esperavam terremotos.

Suspeita-se que parte significativa desta reação (ou melhor, ausência de reação) foi impulsionada pela satisfação consciente ou inconsciente sentida por bilhões de usuários da Internet que se dedicam, com entusiasmo, à auto-espionagem 24/7. Afinal, uma das principais atrações da Internet é a liberdade de acesso constante à "esfera pública" (versão online), antes aberta exclusivamente a poucos escolhidos, como as grandes estações de rádio, TV ou imprensa, severamente vigiando o acesso. Para incontáveis milhões, assombrados pelo espectro da solidão e do abandono, a Internet oferece uma oportunidade sem precedentes de saída/salvação do anonimato, da negligência e do esquecimento. Um efeito colateral das revelações de Snowden foi tornar os usuários da Internet conscientes de quão grande e recheada de pessoas importantes,

"pessoas que realmente importam", a esfera pública está. As revelações de Snowden forneceram, repentinamente, à sua semiconsciente esperança uma feição muito mais realista, provendo a prova retumbante - se uma prova era necessária - do quão sólido é o investimento de tempo e energia em amigos virtuais e na arena pública virtual. Se pudermos esperar alguma mudança, o efeito mais profundo e duradouro do caso será outro grande impulso à dedicação e ao entusiasmo da espionagem *Do It Yourself* (DIY) - voluntária e não remunerada - para alegria e conforto dos consumidores e dos mercados de segurança.

Assumindo que os fatores aqui mencionados estejam corretos, o perigo de responsabilizar grandes agências e a participação democrática em novos protocolos de informação é que, do ponto de vista dos usuários cotidianos da Internet e da mídia social, isso não representará nada de novo. Isto é proveitosamente combatido pelo efeito homeopático das revelações de Snowden. Parece que cada revelação é calculada para tocar em diferentes dimensões da vigilância, orquestrada por agências do governo mas viabilizada através da cooperação das empresas de Internet. Manter questões perante os olhos do público durante um período de tempo mais longo do que o habitual breve interesse que a mídia permite é conquista de alguma sagaz denúncia de irregularidade. O que realmente irá produzir algum envolvimento público mais sério ainda está para se ver.

Referências bibliográficas

AGAMBEN, Giorgio. **From the State of Control to the Praxis of Destituent Power.** Palestra pública em Atenas, 16 de novembro de 2013. Disponível em http://roarmag.org/2014/02/agamben-destituent-power-democracy. Acesso em: 12 mar. 2014.

BAUMAN, Zygmunt. **Liquid Fear.** Cambridge: Polity, 2005.

_____; LYON, David. **Liquid Surveillance: A Conversation.** Cambridge: Polity, 2013.

BIGO, Didier. **The Mobius Ribbon of Internal and External Security(ies).** IN: MATHIAS, A.; JACOBSON, A.; LAPID, Y. (eds.). Identities, Borders, Orders. Rethinking International Relations Theory, Vol. 18. Minneapolis: University of Minnesota Press, 2001.

BIGO, Didier. **The Transnational Field of Computerised Exchange of Information in Police Matters and Its European Guilds.** IN: KAUPPI, N.; MADSEN, M. R. (eds.). Transnational Power Elites: The New Professionals of Governance, Law and Security. Londres: Routledge, 2013.

CASTELLS, Manuel. **The New Public Sphere: Global Civil Society. Communication Networks, and Global Governance.** The Annals of the American Academy of Political and Social Science 616 (1): 78–93. 2008.

Christian Science Monitor. Disponível em http://www.csmonitor.com/USA/2013/1016/NSArevelations-A-timeline-of-what-s-come-out-since-Snowden-leaks-began/June-5-8-2013 . Acesso em 12 mar. 2014.

CLARKE, Richard A.; MORELL, Michael J; STONE, Geoffrey R.; SUNSTEIN, Cass R; SWIRE, Peter. **Relatório Final do Review Group on Intelligence and Communications Technologies: Liberty and Security in a Changing World**, 12 de dez. 2013.

COLEMAN, Georges. **Hacker Politics and Publics.** Public Culture 23 (3): 511–516. 2011.

PARLAMENTO EUROPEU. **Relatório da Comissão de Liberdades Civis (Libe) do Parlamento Europeu**, presidido por Claudio Moraes em 12/03/2014, intitulado US NSA Surveillance Programme, Surveillance Bodies in Various Member States and their Impact on EU citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs. A7-0139/2014. 2014.
Disponível em http://www.europarl.europa.eu/committees/en/studies.html#studies. Acesso em 12 mar. 2014.

_____. Pesquisa realizada por CCLS-CEPS, Didier Bigo, Sergio Carrera, Nicholas Hernanz, Julien Jeandesboz, Joanna Parkin, Francesco Ragazzi, Amandine Scherrer intitulada **National Programmes for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU law**. 2013-PE 493.032. Disponível em http://www.ccls.eu e também em http://www.ceps.eu/book/mass-surveillance-personal-data-eu-member-states-and-its-compatibility-eu-law . Acesso em 12/03/2014.

FOUCAULT, Michel. **Security, Territory, Population.** London: Palgrave, 2007.

GERBAUDO, Paolo. **Tweets and Streets: Social Media and Contemporary Activism**. Londres: Pluto

Press, 2012.
GUARDIAN.COM. Disponível em http://www.theguardian.com/world/interactive/2013/nov/01/snowdennsa-files-surveillance-
revelations-decoded . Acesso em 12 mar. 2014.
KURZMAN, Charles. **Where Are All the Islamic Terrorists? Chronicle of Higher Education,** 2011. Disponível em https://chronicle.com/article/Where-Are-All-the-Islamic/128443/. Acesso em 12 mar. 2014.
LUKE, Timothy W. **Simulated Sovereignty, Telematic Territoriality: The Political Economy of Cyberspace.** IN: LASH, S.; FEATHERSTONE, M. (eds.). Spaces of Culture: City-Nation-World. Londres: Sage, 1999.
LYON, David. **Surveillance After September 11.** Cambridge: Polity, 2003.
MARWICK, Alice. **The Public Domain: Surveillance in Everyday Life. Surveillance and Society 9 (4)**, 2012. Disponível em http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/viewFile/pub_dom/pub_dom/ . Acesso em 12 mar. 2014.
MARWICK, Alice. **Status Update: Celebrity, Publicity and Branding in the Social Media Age.** New Haven, CT: Yale University Press, 2013.
MEDINE, David; BRAND, Rachel; COOK, Elisabeth Collins; DEMPSEY, James; WALD, Patricia. **Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court. Privacy and Civil Liberties Oversight Board,** 23 de janeiro de 2014. Disponível em http://www.fas.org/irp/offdocs/pclob-215.pdf/. Acesso em 12 mar. 2014.
NEGROPONTE, Nicholas. **Being Digital.** New York: Vintage, 1995.
NEW TRANSPARENCY. **Transparent Lives: Surveillance in Canada/Vivre à nu: La surveillance au Canada.** Edmonton, Alberta: Athabasca University Press, 2014.
PODESTA, John. **Big Data and the Future of Privacy. 2014.** Disponível em http://www.whitehouse.gov/blog/2014/01/23/big-data-and-future-privacy/. Acesso em 12 mar. 2014.
REID, Angus. **Pesquisa Global da Angus Reid. The Huffington Post**, 30 de outubro de 2013. Disponível em http://www.huffingtonpost.com/2013/10/30/edward-snowden poll_n_4175089.html/. Acesso em 12 mar. 2014.
SCHMID, Gerhard. **Report on the Existence of a Global System for the Interception of Private and Commercial Communications** (ECHELON Interception System) (2001/2098(INI)). 2001.
WALKER, R. B. J. **After the Globe, Before the World.** London: Routledge, 2010.
WHITAKER, Reg. **The End of Privacy: How Total Surveillance Is Becoming a Reality**. New York: New Press, 1998.