Governança da Internet e suas Implicações para as Políticas Públicas

Glenn Greenwald (2014), *No Place to Hide*, New York, NY: Metropolitan Books, 259 pp.

Laura DeNardis (2014), *The Global War for Internet Governance*, New Haven: Yale University Press, 287 pp.

Milton Mueller (2010), *Networks and States: The Global Politics of Internet Governance*, Cambridge: The MIT Press, 313

Fernanda Rosa e Diego Vicentin
American University e Universidade Estadual de Campinas

A governança da internet é um território de estudo que vem sendo reconhecido como estratégico, dada a centralidade social e econômica que a internet tem alcançado e a expansão contínua de sua abrangência. A produção acadêmica sobre o tema tem forte preponderância de países de economias desenvolvidas, em especial os Estados Unidos, sendo a participação latino-americana ainda restrita, e o estudo da governança da internet como objeto de política pública na região ainda bastante limitado. Pretendemos, aqui, fortalecer o debate na região e ampliar o enfoque sobre as políticas públicas nessa área a partir da revisão de três livros fundamentais no campo. Milton Mueller (2010) e Laura DeNardis (2014) são autores-chave na constituição desse território que emerge com a internet – o de sua governança, revelando as disputas que caracterizam sua infraestrutura e seu modo de funcionamento. Os autores tentam fundar e estabelecer os limites do campo, bem como elucidar o que está em jogo nessa área de conhecimento em formação. São leituras essenciais e que, espera-se, sejam em breve traduzidas para o português e o espanhol.

Em "Networks and States" (2010), Mueller assume as perspectivas da Ciência Política e das Relações Internacionais, e trata do tema da governança da internet a partir da problemática do Estado-Nação. Não por menos, busca diferenciar governo e governança. A última seria mais "fraca" e "denota a coordenação e a regulação de atores independentes sem a presença de uma autoridade política ampla" (2010: 8). Para o autor, a governança é menos impositiva que o governo, mesmo que, de algum modo, ela compreenda suas funções, como, por exemplo, planejar e implementar políticas públicas. Assim: "a governança da internet é o rótulo mais simples, direto e inclusivo para o conjunto de disputas e deliberações sobre como a internet é coordenada, gerida e informada para refletir políticas"[1] (2010: 9).

1 "[...] Internet governance is the simplest, most direct and inclusive label for the ongoing sets of disputes and deliberations over how the Internet is coordinated, managed, and shaped to reflect policies".

Laura DeNardis, por sua vez, em seu livro "The Global War for Internet Governance" opta por um conceito mais descritivo e aplicado de governança da internet: "A principal tarefa da Governança da Internet envolve a concepção e a administração das tecnologias necessárias para manter a internet operacional e para a adoção de política substantiva em torno dessas tecnologias"[2] (DeNardis 2014: 6). Com base nos Estudos de Ciência e Tecnologia (Science and Technology Studies), seu argumento central defende que uma infraestrutura técnica sempre implica questões políticas, de interesse público, ainda que as decisões sobre seu *design* e evolução sejam comumente restritas a grupos de especialistas e técnicos. Esse é um dos pontos fortes do livro de DeNardis: lançar luz sobre camadas pouco visíveis da arquitetura da rede, explicando em detalhes e de maneira original aspectos tecnológicos que concretizam problemas técnicos e políticos de primeira ordem.

DeNardis e Mueller permitem entender que a arquitetura da internet e seus conflitos têm implicações diretas no acesso ao conhecimento, no ritmo da inovação da rede e na possibilidade de garantia (ou violação) de direitos individuais, como privacidade e liberdade de expressão. Eles mostram que, no campo da governança da internet, técnica e política têm uma conexão intrínseca, não sendo possível compreender uma sem a outra. O desafio, então, é tornar as tecnologias e as disputas de poder que envolvem as diferentes camadas da rede mais familiares para que as políticas públicas sejam mais efetivamente endereçadas. Ambas as obras são leituras muito apropriadas a formuladores de políticas públicas, tomadores de decisão e pesquisadores acadêmicos. Por sua abordagem descritiva sobre o funcionamento das tecnologias da rede, DeNardis (2014) se estende também a um público mais geral, interessado em compreender como opera a internet.

A tecnopolítica ganha concretude no último livro de nossa tríade. "Sem lugar para se esconder" (2014), de Glenn Greenwald, que é o registro em primeira pessoa de um acontecimento que define o momento na história da internet a partir do qual não é mais possível alegar ignorância em relação ao controle e à vigilância que ela possibilita e concretiza. No livro, Greenwald narra de forma exclusiva, tanto para um público não-especializado como para leitores envolvidos com os temas de internet e cibersegurança, o processo a partir do qual ele se tornou o principal jornalista a receber e publicar os documentos minuciosamente coletados e compartilhados por Edward Snowden, ex-funcionário da Agência de Segurança Nacional Americana (NSA), sobre a política de vigilância massiva colocada em prática pelo governo dos Estados Unidos (EUA).

Com poderes quase incontestáveis imputados pelo pretexto de combate ao terrorismo, a NSA implantou um esquema em que coletava, ainda em 2012, dados de cerca de 20 bilhões de comunicações

2 "The primary task of Internet governance involves the design and administration of the Technologies necessary to keep the Internet operational and the enactment of substantive policy around these technologies".

por dia (Greenwald 2014: 98). A estratégia de "coletar tudo" (desde comunicações telefônicas até o conteúdo de e-mails) transforma a internet no maior aparato de vigilância que jamais existiu, uma ferramenta de repressão a direitos fundamentais. É a própria liberdade política que está em jogo quando Estados e corporações detêm capacidade de vigilância em massa.

Este artigo é um experimento que busca discutir a tecnopolítica da governança da internet a partir das obras acima. O texto é introdutório, e, além de oferecer um breve panorama sobre o tema, pretende apontar para questões atuais e urgentes, para conflitos que ainda não encontraram seu termo.

Em 2005, o grupo de trabalho sobre governança da internet, criado pela Organização das Nações Unidas (ONU) no contexto da Cúpula da Sociedade da Informação (World Summit on the Information Society, WSIS), identificava em seu escopo desde aspectos técnicos da infraestrutura de telecomunicações até temas como liberdade de expressão, cibersegurança, privacidade, acessibilidade e propriedade intelectual (Mueller 2010). Hoje, mais de dez anos passados desde a primeira fase do WSIS, em Genebra (2003), ainda é um desafio descrever e definir quais são as operações básicas (técnicas e institucionais) envolvidas no funcionamento da internet e, sobretudo, fazer ver suas implicações em termos de políticas públicas. Nessa seção, vamos realizar esse exercício a partir da seleção de alguns dos principais conflitos discutidos pelos autores e derivados de algum tipo de concentração de poder sobre a rede. Isso inclui acesso e gestão dos recursos críticos (e a consequente disputa entre modelos de governança); bem como a definição de padrões técnicos, que é movida majoritariamente por interesses de mercado, e ainda questões de cibersegurança e vigilância na rede. Utilizaremos uma abordagem descritivo-analítica das tecnologias e suas disputas, de modo a afirmar a indissociação entre técnica e política na governança da internet tal qual discutida pelos autores.

A expressão "recursos críticos da internet" tornou-se comum juntamente com o termo governança. Ela aparece em documentos oficiais da ONU e inclui certamente (mas não só) o sistema de nomes de domínio (Domain Name System, DNS), os servidores raiz, e o conjunto de endereços IP (protocolo de internet). DeNardis indica que esses recursos são críticos para o funcionamento da internet porque apresentam algum tipo de escassez, que pode ser inclusive de natureza lógica. O exemplo mais evidente diz respeito ao esgotamento do número de endereços IP e a transição entre os padrões IPv4 e IPv6. O endereço IP é o protocolo mais básico de funcionamento da internet e serve como "identificador único" que permite, a partir de um sistema globalmente coordenado, localizar os dispositivos conectados à internet e os websites. Por exemplo, apesar de digitarmos www.exemplo.com em um navegador, ele é convertido em

um endereço IP, numérico, para que se estabeleça a comunicação com o servidor que hospeda o conteúdo daquele site. Portanto, ele é essencial para o acesso e transmissão de informação na internet.

O sistema de endereços IP, tal como foi formulado ainda na década de 1980 (IPv4), permite uma quantidade máxima de 4 bilhões de endereços, insuficiente para a contínua expansão da rede (DeNardis 2014: 39). O problema de sua escassez pode ser solucionado a partir da adoção progressiva da versão mais atual do protocolo, conhecida como IPv6, que provê um número impronunciável de endereços IP.[3] Por um lado, essa quantidade desfará as barreiras para a conexão de mais dispositivos à rede, viabilizando cada vez mais a internet das coisas. Por outro, ultrapassando o fórum técnico, tais definições podem trazer consequências para a gestão da proteção da privacidade na rede, uma vez que o número potencialmente ilimitado de endereços abre a possibilidade de que cada aparelho receba um número de IP fixo, que combinado com outras informações, deverá facilitar a identificação dos usuários.

O controle e a distribuição dos endereços IP são parte das "funções IANA" (Internet Assigned Numbers Authority)[4]. A IANA é um departamento da ICANN (Internet Corporation for Assigned Names and Numbers)[5], uma organização de direito privado subordinada formalmente à NTIA (National Telecommunications & Information Administration)[6] que, por sua vez, responde ao Departamento de Comércio do governo dos EUA. Podemos dizer que os recursos críticos são assim nomeados também porque provocam disputas de dimensão global em torno de algumas operações da internet que são desempenhadas de forma centralizada.

Tomemos como exemplo a função IANA de manutenção-atualização dos servidores raiz, responsáveis por armazenar o arquivo que faz a correspondência entre números de IP e endereços da web (www.exemplo.com). Como já adiantamos, cada endereço da web precisa ser traduzido em endereço IP, a fim de que se estabeleça a conexão do usuário com os servidores da página web que ele deseja acessar. É preciso lembrar que o IP é a identidade numérica de um nodo da rede e guarda informações sobre sua localização. Assim, ao digitar o endereço de uma página web qualquer na barra de localização do navegador, o software dispara uma série de procedimentos para descobrir qual é o endereço IP que corresponde àquela página para, assim, disponibilizar a visualização do seu conteúdo.

A tradução entre endereços web (ou nomes de domínios) e números IP faz parte do "sistema de nomes de domínio"

3 O número total de endereços disponíveis no IPv6 é de 3,4x1038 (cf. DeNardis 2014: 40).

4 Autoridade para Atribuição de Números da Internet.

5 Corporação da Internet para Atribuição de Nomes e Números.

6 Administração Nacional de Telecomunicações e Informações.

(Domain Name System, ou DNS). Sua arquitetura aponta para treze servidores raiz que distribuem a informação de maneira hierarquizada para os servidores espelho, os quais mantêm cópias das informações para aumentar a robustez da rede e evitar falhas. Atualmente, dez dos treze servidores raiz estão localizados nos EUA.[7]

Todos os servidores armazenam o arquivo que faz a correspondência de um número IP ao nome de domínio desejado; o arquivo precisa se manter único globalmente para garantir a correspondência correta. Hoje, a responsabilidade de atualização e distribuição do arquivo recai sobre uma empresa privada chamada Verisign, que é contratada pelo departamento de comércio dos EUA (Denardis 2014: 49; Mueller 2010: 63). Esse é um dos pontos de concentração de poder na arquitetura da rede, na medida em que aquele que controla o arquivo raiz (*root zone file*), tem domínio sobre parte primordial do sistema de endereçamento da internet e pode, por exemplo, agir como censor de conteúdo, negando o acesso a determinadas páginas.

Além dos endereços IP, vale ressaltar que faz parte das funções IANA controlar e distribuir os ASNs (Autonomous System Numbers)8 que identificam, com um número único, toda organização operadora da rede, ou em outras palavras, todo sistema autônomo. O ASN assegura, assim, que uma empresa, universidade etc, desempenhe uma função infraestrutural na arquitetura da internet. A internet é comumente chamada de "rede das redes" porque é resultado da interconexão entre diversos sistemas autônomos que interoperam a partir da utilização padrões técnicos comuns.

Mueller define a fundação da ICANN (1998) e a realização do WSIS (2003-2005) como os principais marcos na formação institucional da governança da internet. A fundação da ICANN instituiu um modelo que se pretendia não-governamental para tomadas de decisão sobre os recursos críticos da rede; o WSIS, por sua vez, é o momento em que esse discurso é desafiado no plano global, dada a oposição de alguns governos à supremacia de um Estado-Nação, os Estados Unidos, sobre esses recursos. Desde então, tal debate tem apenas se intensificado e é um dos principais motivos para a transição, iniciada em 2015, das funções IANA da ICANN para uma organização internacional.9

As disputas que se desenvolvem na coordenação dos recursos críticos explicitam a tensão entre dois modelos de governança: multilateralismo e multisetorialismo. Na sua origem, o primeiro defende a governança centrada no poder estatal, seguindo o formato da Assembleia Geral das Nações Unidas onde cada Estado-nação participa de

7 Cf. https://www.iana.org/domains/root/servers (último acesso: 22/03/2016).

8 Sistema Autônomo de Numeração

9 Cf. https://www.icann.org/stewardship (último acesso: 22/03/2016).

processos decisórios. Já o segundo modelo visa distribuir o poder decisório entre os diferentes atores interessados (*stakeholders*) não-exclusivos à esfera estatal, como empresas privadas, grupos da sociedade civil.

Para DeNardis e Mueller, a questão que se coloca de fundo a tais modelos é a legitimidade, ou "[...] *quem deve definir política pública para a internet como um todo*?"[10] (Mueller 2010: 65). Esse autor ainda lembra que, no WSIS de 2005, o Brasil liderou a articulação entre países críticos à hegemonia dos EUA. O país latino-americano defendeu o processo de governança mais tradicional, baseado no mecanismo de eleições, legislação em nível nacional e negociações multilaterais (Mueller 2010: 64). Naquele momento, mesmo a União Europeia (tradicional parceira dos EUA nas questões internacionais) também emitiu um documento crítico à posição dos EUA, requerendo maior internacionalização da governança da internet e maior participação dos Estados. A resposta do governo dos EUA foi imediata, seu congresso definiu que a ICANN deveria continuar com suas responsabilidades relativas à administração da internet, inclusive sobre as funções IANA. Como aponta Mueller: "os Estados Unidos basearam seu apelo, ironicamente, na manutenção da internet livre de governos"[11] (2010: 75), afirmando que o modelo multilateral de governança daria demasiado poder aos países não democráticos e causaria prejuízos à liberdade na rede.

A tensão entre os modelos multilateral e multissetorial é, em grande parte, resultado da disputa pelo controle sobre os recursos críticos da internet, seja por sua escassez, ou por sua gestão centralizada. De todo modo, sabemos que a governança da internet se estende por uma gama bem mais ampla de tópicos, como a definição de padrões técnicos, a coordenação da interconexão entre redes (sistemas autônomos), disputas de propriedade intelectual, sistemas de intermediação de informação e algoritmos, cibersegurança, entre outros. Em cada um deles, redes de relações entre diferentes atores, em sua maioria privados, se estabelecem ao redor de funções específicas necessárias para o funcionamento da rede.

Os vários espaços de tomada de decisão nessa arquitetura distribuída expõem os desafios de simplificar a oposição entre multilateralismo e multissetorialismo. Mais recentemente, no encontro multissetorial NETMundial (2014) e no 10º Fórum de Governança da Internet (2015), ambos ocorridos no Brasil, o governo brasileiro defendeu a complementaridade dos dois modelos, expressando que o ponto de discórdia é ter, atualmente, "arranjos multissetoriais sujeitos à supervisão de um ou de poucos Estados".[12] A discussão sobre modelos de governança é latente.

Mueller (2010) e DeNardis (2014) concordam que a governança da internet

10 "[...] *who should define public policy for the entire internet*?" (Ênfase em itálico no original).

11 "The United States based its appeal, ironically, on keeping the Internet free of governments".

12 Cf. http://bit.ly/1VuaUwi (último acesso: 22/03/2016).

tomou suas primeiras formas de maneira espontânea, mudando na medida da evolução da tecnologia e do crescimento da rede em direção à sua atual configuração formal e institucional. DeNardis (2014: 18) lembra que as estruturas de governança da internet eram originalmente baseadas na confiança e na familiaridade tanto quanto no conhecimento técnico. A legitimidade desses atores advêm do acúmulo de conhecimento e experiência, mas isso não ocorre sem tensão.

Parte do conflito toma forma no desenvolvimento dos padrões técnicos que definem as operações básicas do funcionamento da internet. Os padrões são um conjunto de regras, protocolos, ou especificações cujo objetivo é produzir interoperabilidade. Para que diferentes aparelhos operem em conjunto é preciso que se estabeleça essa dimensão comum e compartilhada. Como afirma DeNardis: "os protocolos de internet são a Internet"[13] (2014: 66). Uma infraestrutura como a da internet depende do funcionamento de inúmeros padrões, que são simultaneamente técnicos e políticos não apenas porque tratam da interoperabilidade da rede, de ação conjunta, mas também porque podem ser projetados para refletir decisões políticas, defender valores, assegurar ou minar direitos dos usuários. Ora, mas como são definidos os padrões da internet?

Hoje os padrões são desenvolvidos por diversas comunidades técnicas, consórcios industriais e organizações de padronização. O protocolo IP é, por exemplo, um padrão mantido pelo Internet Engineering Task Force (IETF)[14], uma comunidade técnica formada em 1986 que prima pelo desenvolvimento de padrões abertos, que não exigem pagamento de licença para o seu uso. No IETF os padrões são documentos de acesso público e gratuito e a comunidade se pretende aberta à participação. O trabalho de padronização pode ser acompanhado através das listas de e-mail, ou de reuniões presenciais. Na prática, existem grandes barreiras à participação, como o alto nível de conhecimento especializado e o suporte financeiro que seja suficiente para garantir o tempo de trabalho necessário à qualquer contribuição que seja decisiva no funcionamento de um padrão (DeNardis 2014: 71).

Não por menos, em sua imensa maioria, os participantes que contribuem nos trabalhos do IETF e de outras organizações de padronização, como o Institute of Electrical and Electronics Engineers (IEEE)[15], a Internet Society (ISOC) e o World Wide Web Consortium (W3C)[16], representam os interesses de grandes empresas, seja como meio de investimento em inovação ou simplesmente para assegurar uma posição no mercado. Esse é um aspecto importante na privatização da

13 "Internet protocols are the Internet"

14 Força-tarefa de Engenharia da Internet.

15 Instituto de Engenheiros Eletricistas e Eletrônicos.

16 Consórcio World Wide Web.

governança da internet: majoritariamente movidos por questões de mercado, atores privados tomam decisões técnicas que têm implicação de política pública (DeNardis 2014: 83). Fóruns de padronização como o IETF, o IEEE, a ISOC e o W3C também são pontos privilegiados na rede de atores e instituições que coloca em prática a governança da internet, ou seja, que a mantém funcional. Esses fóruns concentram parte importante do poder de decisão sobre aspectos básicos de arquitetura da rede, e são um ponto estratégico de ação política.

Em 2013, após anos de trabalho terceirizado na NSA, o analista de infraestrutura Edward Snowden revelou ao mundo alguns dos mecanismos de vigilância e espionagem do governo americano, contribuindo para compreensão dos riscos de negligenciar valores como transparência e *accountability* na governança da internet. Os documentos sigilosos compartilhados por Snowden, e tornados públicos por Glenn Greenwald, mostram como opera a coleta de dados massiva da NSA de metadados das comunicações, como tempo de ligação e localização, e também de seu conteúdo, como mensagens de voz, texto e e-mails de cidadãos americanos e de outras partes do mundo, sem justificativa baseada em denúncias ou ordens judiciais.

A invasão de redes privadas e o acesso não autorizado a dados pessoais é uma das ameaças que se enquadram na ampla temática de cibersegurança. Outras são vírus e *worms*, ataques à infraestrutura crítica da rede como roteamento e endereçamento, entre outros (DeNardis 2014: 89; Mueller: 159-160). A responsabilidade de prevenir e combater tais ataques é distribuída, mas o setor privado tem um papel central (idem). Como exemplo, empresas são responsáveis por disponibilizar avisos e atualizações de hardware e software quando identificam vulnerabilidades em seus produtos (DeNardis 2014: 92); e autoridades de certificação (Certificate Authorities, ou CA), também privadas, garantem a autenticidade entre as partes numa transação online. Por outro lado, centros de respostas como os Computer Emergency Response Teams (CERT)[17], em alguns países também sob coordenação de atores privados, são referências nacionais sobre o tema.

Os detalhes providos pelos documentos revelados por Snowden, de todo modo, questionam a suficiência e integridade desse modelo e a confiança nos sistemas de intermediação de informação como redes sociais, aplicativos de chamada telefônica, de e-mail etc. Na descrição da operação FAIRVIEW realizada para obter acesso a informações de cidadãos de outros países, são expostas as relações existentes entre empresas americanas e o governo:

> "Parceiro corporativo desde 1985, com o acesso a cabos, roteadores, switches int. [internacionais]. O parceiro opera nos EUA, mas tem acesso à informação

17 Equipe de Resposta a Incidentes em Computadores.

> que transita na nação e, por meio de suas relações corporativas, fornece acessos únicos a outras empresas de telecomunicações e ISPs [provedores de serviços de internet]."[18] (Greenwald 2014: 105)

Já nos documentos sobre a operação STORMBREW é descrita uma parceria da NSA com o Departamento Federal de Investigação americano (FBI) e com as empresas operadoras de telecomunicação a fim de interceptar os tráficos da internet e de telefonia que passam por solo americano seja por "pontos de estrangulamento" da rede (*choke points*) seja por cabos submarinos nas costas leste e oeste do país. Como discutido por DeNardis, tais pontos de centralização de informação sujeitos à vigilância existem dado o desenho da arquitetura da internet, que tem os Estados Unidos como ator central na história de seu desenvolvimento.

O programa PRISM evidencia a estratégia do governo americano via NSA de coletar dados diretamente dos servidores de empresas de internet sem nenhuma justificativa ou mandado judicial. AOL, Apple, Facebook, Google, Microsoft, PalTalk, Skype, Yahoo!, Youtube são as empresas citadas nos documentos. Produtos como Hotmail, Gmail, áudio e informações de conversas são alguns dos focos da operação. Em um relato detalhado, nota-se a anuência da Microsoft com a operação:

> "MS [Microsoft], trabalhando com o FBI, desenvolveu uma capacidade de vigilância para lidar com a nova SSL (Camada de Soquete Seguro ou Secure Socket Layer). Estas soluções foram testadas com sucesso e foram ao ar em 12 de dezembro de 2012"[19] (2014: 115).

A instalação de *malware* em computadores privados também é uma prática revelada pelos documentos. É recorrente que a NSA implante ferramentas de vigilância conhecidas como *backdoors* (porta dos fundos) em servidores e outros componentes de rede de computadores exportados dos EUA, dando acesso ao governo americano a várias redes e a dados de seus usuários ao redor do mundo. Como precaução a atividades similares vindas de outros países, representantes do governo americano defenderam que hardware de empresas chinesas como Huawei e ZTE fossem combatidos no mercado americano.

O Brasil é citado como alvo em vários momentos. Na operação OAKSTAR, relações entre o governo americano e empresas foram estabelecidas para coleta de dados do Brasil e da Colômbia (2014: 106). Outro exemplo é a operação canadense OLYMPIA de espionagem sobre o Ministério de Minas e Energia do Brasil de ciência do governo americano

18 "Corp partner since 1985 with access to int. cables, routers, switches. The partner operates in the U.S., but has access to information that transits the nation and through its corporate relationships provide unique accesses to other telecoms and ISPs. Aggressively involved in shaping traffic to run signals of interest past our monitors".

19 "MS, working with the FBI, developed a surveillance capability to deal with the new SSL. These solutions were successfully tested and went live 12 Dec 2012".

(2014: 119). Juntamente com México e outros países, o Brasil circula numa lista confidencial cujo título é "Amigos, inimigos ou problemas?" (2014: 141). A Venezuela também é citada como alvo de espionagem na América Latina, além de interceptação direta de políticos, como o então candidato e depois presidente do México Enrique Peña, e a presidenta do Brasil, Dilma Rousseff.

Greenwald denuncia o cenário descrito como a construção de um estado de vigilância instaurado com o objetivo de "coletar, armazenar, monitorar e analisar a comunicação de todas as pessoas ao redor do mundo" (Greenwald 2014: 94). Trata-se de uma ação unidirecional onde "o governo dos EUA vê o que todos no mundo fazem, incluindo a sua própria população, enquanto ninguém vê suas próprias ações" (2014: 169). Importante destacar que existe colaboração com outros países como a aliança Five Eyes composta também por Reino Unido, Canadá, Austrália e Nova Zelândia. A cooperação internacional, com essas e outras nações, por vezes envolve pagamento, treinamentos, recursos para ampliar suas ações de vigilância nacional.

A estratégia de "coletar tudo", via ações de interceptação sobre a arquitetura na rede até então pouco claras, mostra que o trabalho da NSA não se restringe à segurança nacional ou ao combate a atos terroristas. O conteúdo dos documentos vazados evidencia que a quebra da privacidade global serve a ações de espionagem diplomática e também econômica, onde a "gigante de petróleo brasileira Petrobrás" (2014: 134) aparece como um dos focos de interesse na América Latina.

Entre as reações da América Latina às ações de espionagem está a aprovação, em 2014, do Marco Civil da Internet – lei federal brasileira, em discussão desde 2007 – que estabelece princípios, direitos e obrigações para o uso da internet no Brasil e define parâmetros para temas sensíveis como privacidade, liberdade de expressão e neutralidade da rede. O Marco Civil coíbe o acesso a informações pessoais sem mandado judicial, ainda que, controversamente, requeira que tais dados sejam armazenados por um período mínimo, a depender de sua natureza. De todo modo, a capacidade de monitorar o cumprimento de tais regulações é o grande desafio de nossa era, visto que a internet tem uma arquitetura não restrita por fronteiras nacionais, e seu controle tecnológico é também uma forma de regulação (cf. Lessig 1999), embora não transparente e não sujeita à fiscalização.

A problemática colocada em 2013 pelas revelações de Snowden deve ressoar por muito tempo no campo da governança da internet e questiona não apenas a ação dos EUA, mas de qualquer governo com domínio sobre a rede. A possibilidade de rastreamento, vigilância e controle é também fruto de decisões tomadas no âmbito da arquitetura da internet. A concretização de um desenho que privilegie a descentralização, o anonimato e a liberdade de expressão depende de

decisões tomadas no território de sua governança, sendo urgente esse debate.

Diante dos evidentes desafios para a construção de uma internet que garanta a privacidade, a liberdade de expressão e outros direitos fundamentais dos cidadãos de todas as nações num mundo de informação globalizada, muito se discute a respeito de como implementar uma governança da internet cujo desenho institucional seja coerente com tais direitos. Uma das soluções comumente reivindicadas é a regulação via legislação. Porém, como as revelações de Snowden mostram, decisões estatais com finalidades altamente controversas podem ignorar ou impor interpretações escusas sobre legislações existentes de proteção à privacidade. A exigência de fiscalização, comum às políticas públicas, torna-se mais complexa quando se está tratando da arquitetura distribuída da internet e a necessidade de aplicar arranjos tecnológicos que impeçam a interceptação de informações sensíveis.

Um outro aspecto latente dessa discussão é a necessidade de ampliar o letramento digital da sociedade para tornar possível maior agência e autonomia dos cidadãos frente a situações de afronta à liberdade de expressão e à privacidade. O entendimento público de tecnologia e das consequências de estar às voltas por dispositivos de vigilância são essenciais não apenas a cidadãos comuns, como a tomadores de decisão, de forma a garantir o cumprimento de direitos básicos que têm sido desrespeitados recorrentemente.

Por fim, faz-se urgente uma maior compreensão da governança da internet como área de política pública, onde disputas cruciais relativas à democracia, o papel do Estado e o fortalecimento da esfera pública têm sido estabelecidas com a participação limitada de agentes locais latino-americanos e de outras regiões. As disputas elucidadas pelos autores aqui apresentados tornam fundamentais a intensificação da produção de conhecimento na região e a entrada de novos atores guiados por interesses públicos em fóruns onde se discute a arquitetura da internet, a fim de propor soluções técnicas e políticas de desconcentração de poder que garantam a integridade da rede e a sua expansão como meio de comunicação livre e global.

Bibiliografia

Lessig, Lawrence (1999): "The Law of the Horse: What Cyberlaw Might Teach", in: *Harvard Law Review*, 113, 501-546.