O DISCURSO DE SEGURANÇA E A PRIVACIDADE NO MARCO CIVIL DA INTERNET

Resumo: A discussão sobre segurança, no âmbito do combate aos cibercrimes, foi um dos pontos de conflito ao longo da elaboração do Marco Civil da Internet. A proposta deste artigo foi desenvolver uma análise das notas da Câmara dos Deputados brasileira a fim de entender como se travaram os embates no âmbito da segurança, do cibercrime e da vigilância. Com o intuito de se preservar a garantia pela guarda de dados de conexão e aplicação no projeto de lei, deputados da frente parlamentar contra crimes cibernéticos fizeram forte apelo pelo estabelecimento de um prazo de 12 meses para guarda de registros de conexão e aplicação, favorecendo o trabalho de investigação criminal. No entanto, a guarda de dados por um longo tempo era vista como uma ameaça à privacidade. Neste trabalho, será possível refletir sobre os embates e enfrentamentos em torno do discurso de segurança, pensando nos impactos que ele oferece à privacidade dos usuários da Internet.

Palavras-chave: Privacidade, Vigilância, Internet, Segurança

El discurso de la seguridad y la privacidad en el Marco Civil da Internet

Resumen: La discusión sur la seguridad en la lucha contra el delito cibernético fue uno de los puntos de conflicto en relación a la elaboración del Marco Civil de Internet en Brasil. El propósito del trabajo es la análisis de las notas del Congreso Nacional con la finalidad de comprender cómo los conflictos ocurren en el campo de la seguridad, de la delincuencia informática y la vigilancia. Con el fin de preservar la garantía de mantener los datos de conexión y aplicación en el proyecto de ley, los diputados de la Frente Parlamentario contra el delito cibernético hicieron fuerte presión para el establecimiento de un período de 12 meses para asegurar la guarda de los registros de conexión y de aplicación, favoreciendo los procedimientos de investigación criminal. Sin embargo, la guardia de datos durante mucho tiempo fuera vista como una amenaza a la privacidad. En este trabajo reflexionamos respecto de los conflictos y enfrentamientos en todo el discurso de la seguridad, pensando en el impacto que la cuestión ofrece a la privacidad de los usuarios de Internet.

Palabras clave: Privacidad, Vigilancia, Internet, Seguridad

The security speech and privacy on the Marco Civil da Internet

Abstract: The discussion of security in context of the fight against cybercrime was one of the points of conflict over the drafting of the Marco Civil da Internet on Brazil. The purpose of this paper is develop an analysis of the Chamber of Brazilian Deputies' notes in order to understand how conflicts were waged in the field of security, cybercrime and surveillance. In order to preserve the guarantee of keeping connection data and application in the bill, members of parliamentary group against cybercrime made strong appeal to establish a period of 12 months to guard connection and application records, favoring criminal investigations by police. However, the data guard for a long time was seen as a threat to privacy. In this work, we reflect on the conflicts and confrontations around the security discourse, thinking of the impact that it offers to the privacy of internet users.

Keywords: Privacy, Surveillance, Internet, Security

PAULO EDUARDO ASSIS MAIA
MARTA DE ARAÚJO PINHEIRO
GUSTAVO FERNANDES PARAVIZO MIRA

Um dos grandes pontos de conflito que se estabeleceu durante a tramitação do Marco Civil da Internet, lei brasileira que estabelece diretrizes para o uso e a operacionalização da rede, se refere à questão da segurança. O embate entre forças policiais, representadas por órgãos de segurança pública como a Polícia Federal e a associação dos peritos e forças políticas, como os deputados, o Governo e os movimentos sociais, se consolidou na Câmara dos Deputados quando a matéria foi apreciada pelos parlamentares, alguns deles reforçando a caracterização de usuários da rede como suspeitos, e defendendo a criação de ferramentas de punição.

A princípio, o texto do projeto de lei determinava aos provedores de conexão (teles, operadoras e empresas que comercializam o acesso à internet) a guarda de registros de acesso e facultava aos provedores de aplicação (Google, Facebook, navegadores, desenvolvedores de aplicativos) este armazenamento. O ponto gerou divergências entre os atores em questão, uma vez que a preocupação pela guarda de dados por empresas como o Facebook, Google, Microsoft poderia se configurar, na visão de alguns, a violação da privacidade. No entanto, deputados que representavam órgãos policiais, bem como entidades representativas desse segmento, defendiam a obrigatoriedade de guarda de logs por um período pré-estabelecido, de maneira a contribuir com o exercício da investigação de cibercrimes ou mesmo a chegar até hackers que tivessem colocado em xeque a própria segurança de autoridades, violando suas privacidades.

Este artigo propõe uma análise das disputas que se estabeleceram no âmbito da discussão sobre a guarda de dados, enfocando a preocupação com a segurança e os confrontos gerados por posicionamentos divergentes entre órgãos policiais e movimentos sociais. Para isso, buscou-se pensar nas seguintes questões: de que forma o discurso que classifica o usuário da rede como um suspeito se estabeleceu no processo de elaboração do Marco Civil e como as soluções de combate ao cibercrime implicam em um prejuízo à privacidade dos usuários, a partir de um modelo de vigilância que passa a ser institucionalizada? Inicialmente, será feita uma contextualização do caso, apresentando os principais atores em debate. Em um segundo momento, uma revisão teórica sobre a vigilância na sociedade de controle, os efeitos do monitoramento dos indivíduos pelo Estado e a questão da segurança a partir do risco. Na terceira parte deste artigo, serão apresentados os conflitos ocorridos no debate sobre o Marco Civil.

A pesquisa desenvolvida levou em conta um escopo de 89 discursos registrados pelo Departamento de Taquigrafia e Revisão da Câmara dos Deputados ao longo das sessões de discussão do Marco Civil da Internet, enfocando a questão privacidade como um dos tópicos da elaboração do texto. As falas foram proferidas por 27 oradores, sendo eles deputados, representantes de entidades de classe, acadêmicos, lideranças de movimentos sociais e membros do Governo federal. Tendo em vista o grande embate gerado em relação à obrigatoriedade da guarda de dados por provedores de aplicação, inicialmente sendo facultativa, observa-se que 63% dos oradores abordaram o tema da guarda de dados em uma de suas falas, seja empunhando-o como uma bandeira a ser defendida na discussão do Marco Civil, cuja preocupação com a segurança se sobressaía, seja simplesmente a título de menção como tópico importante que o projeto abrangia. Os posicionamentos mais incisivos, considerando o termo, vieram da frente parlamentar contra

crimes cibernéticos, que se predispôs a defender um período maior para a guarda de registros tanto para provedores de conexão quanto para provedores de aplicação.

GARANTIA DA AÇÃO POLICIAL E O COMBATE À PEDOFILIA E À PORNOGRAFIA

Atuando de forma incisiva nas discussões do projeto, a frente parlamentar era composta por alguns deputados como Fernando Francischini (SDD) e Sandro Alex (PPS), os quais defendiam que o prazo para a guarda de dados dos usuários por provedores de aplicação fosse aumentado, a fim de garantir a ação policial. Esse processo passou a ser visto por movimentos sociais e acadêmicos como uma institucionalização da vigilância, sendo duramente criticado. A argumentação dos parlamentares insistiu muito no combate a pedofilia e a pornografia na internet. Tal posicionamento não está restrito ao quadro nacional, pois, segundo Jacob Appelbaum (apud Assange, 2012), os órgãos de inteligência, em geral, elaboram um discurso com os "Quatro Cavaleiros do Infoapocalipse: pornografia infantil, terrorismo, lavagem de dinheiro e a guerra contra certas drogas", a fim de convencer às pessoas sobre a necessidade de se empregar medidas restritivas na Internet.

Na tentativa de emplacar a obrigatoriedade da guarda desses dados, esses deputados e representantes de entidades ligadas à investigação diziam que o projeto poderia tornar o país um paraíso para pedófilos e para a pornografia infantil, uma vez que, por preocupação com os custos de provedores, as investigações ficariam mais difíceis. Eles também questionavam o prazo estabelecido, tendo em vista que muitas vítimas tomam conhecimento do ilícito somente tempos depois de que ele tenha sido praticado, sendo 12 meses já insuficientes para a ação policial. O discurso usado pelos parlamentares remete à iniciativa tradicional de atrelar aguarda de informações como forma de garantir a segurança, assemelhando-se ao discurso sustentado por órgãos de inteligência estatal como a própria NSA, nos Estados Unidos, ou o Serpro, no Brasil, que avaliavam serem essas medidas necessárias para sustentar medidas de segurança, tornando-se uma justificativa aceitável para que a população consinta com a guarda de suas informações pessoais.

Outro ponto importante da discussão sobre a guarda de dados, segundo Silveira (2014), é que, ao buscarem facilitar o seu trabalho, policiais batalharam pela obrigatoriedade da guarda de registros de conexão de todas as pessoas, inocentes ou suspeitas, uma vez que a maioria das pessoas não usa IPs fixos. O autor lembra que neste embate político travado pela guarda de dados, o resultado foi positivo, mas as forças vigilantistas conseguiram aprovar alguns pontos "extremamente nefastos ao espírito original da lei" (Silveira, 2014). Com o prazo de seis meses para que os provedores de aplicação fizessem a guarda dos dados, estabelecidos no artigo 15, tal ponto é considerado uma violação à privacidade, por expandir o armazenamento de nossas informações. A abordagem se dá principalmente pelos termos técnicos empregados na lei, que classificam as aplicações de internet como "conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet". Assim, qualquer empresa de conteúdo, como

Facebook, Twitter e Google, poderá armazenar esses dados para processá-los, analisá-los, agrupá-los com a finalidade de entender o comportamento de seus usuários (Silveira, 2014).

Promovendo um discurso que estimula uma adesão envolta pelo temor da insegurança e do medo, como será demonstrado abaixo, as forças policiais inseriram na lei um dispositivo que permitirá que as informações de usuários estejam vulneráveis ao acesso dos governos e das grandes corporações, reforçando aspectos de controle.

VIGILÂNCIA E A SOCIEDADE DE CONTROLE

O monitoramento de informações em bancos de dados está atrelado à compreensão sobre a nossa sociedade atual que, para muitos analistas e teóricos, se caracteriza como a "sociedade de controle". As denúncias de Edward Snowden, em 2013, trazem à tona uma discussão sobre a forma pela qual a vigilância se estabelece nas interações entre os indivíduos. Quando se propõe a analisar a vigilância no cenário posterior a estas revelações, Lyon (2015) entende que essa não pode ser definida apenas como uma sistemática atenção de rotina às informações pessoais para uma finalidade definida. Segundo ele, a intenção prática da vigilância pode ser tanto proteção, inteligência, cuidado, segurança, direito de posse, gerenciamento ou influência individual ou grupal. O autor analisa a prática de monitoramento exercida pelo Estado, que existe há muito tempo, ressaltando o Big Brother, de George Orwell, para descrever a compreensão sobre o tema durante o século XX. No entanto, observa que, com os atentados ao World Trade Center, em 11 de setembro de 2001, houve uma intensificação da cultura da vigilância com o aumento da coleta de informações pessoais. Tal ação era justificada por um discurso que reforçava a segurança contra ataques terroristas, já que esses poderiam se utilizar de ferramentas tecnológicas.

Com as revelações de Snowden, aumenta o monitoramento estatal de informações pessoais contida nos posts no Facebook, feeds do Twitter,*cloudservices* como o Google Docs, além de dados de GPS instalados em smartphones. Esses dispositivos digitais se transformaram em "sensores em nossos bolsos, que nos rastreiam a qualquer lugar que formos" (Lyon, 2015). Dessa forma, participamos "como nunca" da cultura da vigilância.

A identificação de endereços de IP, identidade de contato, a localização de chamadas ou mensagens e a duração do contato são chamados de "metadados". Segundo Lyon, talvez essa tenha sido a palavra mais recorrente durante o caso Snowden. Quando se trata dos tipos de atividades da NSA, trata-se de monitoramento de conteúdo de telefonemas e mensagens de texto, bem como o armazenamento em grande escala e análise dos metadados, os quais tiveram sua importância minimizada pelo governo norte-americano posteriormente.

O aspecto crucial dessa realidade é o leque de alvos desse sistema de monitoramento por ele alcançado, entre eles, jornalistas, ativistas e ambientalistas. O primeiro objetivo explícito são terroristas, no entanto, é cada vez mais claro aos pesquisadores do tema que ativistas ou pessoas

que discordem da política governamental são também alvos potenciais.

De forma não menos importante, a atividade de monitoramento de redes sociais também propicia a criação do "estado de vigilância", em que indivíduos são monitorados de maneira frequente, e aparatos de vigilância são cada vez mais vultosos, tanto para sustentar este modelo de controle quanto para prover o armazenamento de dados (Lyon, 2014: 6).

A análise da vigilância contemporânea é compreendida por Bruno (2003) para além dos modelos historicamente conhecidos, pensando em processos que estão distribuídos entre múltiplos agentes, técnicas, funções, propósitos, etc. A pesquisadora afirma que a vigilância comporta três circuitos capazes de gerar uma significação subjetiva e plural, reunindo aspectos de segurança, cuidado, temor, suspeição, prazer, entretenimento, entre outros. São eles: os circuitos de segurança e controle; os circuitos de visibilidade midiática; os circuitos de eficácia informacional, que dão um caráter multifacetado à vigilância, com registros de legitimação superpostos (Bruno, 2003: 21).

Trata-se do dispositivo de vigilância distribuída, vigente na contemporaneidade, que abrange jogos de poder e formações específicas de saber que vêm se constituindo a partir do monitoramento de dados pessoais, principalmente no ciberespaço. Essa ação se difere, em parte, da vigilância no âmbito da modernidade, centrada especificamente na ação disciplinar dos indivíduos monitorados. Num passado recente, as práticas de vigilância envolviam grupo específicos, enquanto no mundo contemporâneo se torna uma vigilância para todos.

A SEGURANÇA E O RISCO

Ao se pensar a questão da segurança, entende-se que os aspectos de temor e risco emergem como um forte argumento a fim de estimular a aceitação de mecanismos de vigilância. É necessário pensar, portanto, como a gestão do risco se torna um instrumento defendido para combater, principalmente, os ataques terroristas, abrindo brechas para o monitoramento de indivíduos. Bennet e outros autores (2014) abordam a perspectiva dos riscos analisando a expansão da vigilância no Canadá e seus resultados com base na gestão de risco e de segurança. A preocupação com a segurança se expande para além da questão dos atentados de 11 de setembro e do discurso antiterrorismo, sendo identificadas antes desses acontecimentos. Tal discussão aborda uma vigilância nova e mais intensa, a qual cria riscos para a privacidade, a justiça e a liberdade. Ela surge a partir dos anos 1980 com a gestão de riscos, a qual está relacionada com previsões sobre o comportamento humano.

Com o aumento desta vigilância gerada por uma fome de dados para cálculos de riscos, há um enfraquecimento das normas de privacidade, uma vez que, em muitos casos, não se pede permissão antes de se coletar informações pessoais sobre usuários da internet, por exemplo. Um segundo ponto se refere à vigilância usada para monitorar pessoas uma vez que os riscos sejam identificados, garantindo que estas pessoas não se comportem de uma maneira arriscada,

além de gerir as consequências quando cometem algum ato.

De modo irônico, o grande foco na segurança pode gerar ainda mais insegurança, uma vez que a própria discussão do tema e os esforços para controlar os riscos levam a sociedade a um clima de dúvida e medo. Cria-se um ciclo vicioso que passa a reforçar a justificativa da vigilância como necessária para a busca da segurança. A maior consciência sobre o risco, embora estejamos mais seguros do que antes, tende a gerar um gasto de energia maior para deter aqueles riscos que ainda permanecem. Contribuem para este cenário as rápidas mudanças que implicam na quebra de certezas e instituições tradicionais, como a família. "A vida é vivida como mais individualizada; há uma sensação de que os indivíduos estão sozinhos para se defenderem sozinhos em um mundo arriscado" (Bennet, 2014: 43).

Neste sistema da gestão de riscos, o molde que ela estabelece em torno dos medos favorece cada vez mais o emprego de mecanismos de vigilância. As pessoas tendem a se concentrar em certos riscos devido à sua "natureza terrível", mesmo que eles sejam improváveis. Os riscos são apontados por especialistas mais na sua natureza dramática do que realmente em sua probabilidade, de forma que algo que possa ocorrer, ainda que improvável, não possa ser descartado. Essa estratégia, por outro lado, é muito mais eficaz, uma vez que as pessoas assimilam mais as impressões e sentimentos em relação a um risco que lhes é colocado, do que por probabilidades numéricas. A mídia exerce um papel fundamental neste caso, especialmente por abordar de forma mais aterrorizante tais riscos, ampliando seus efeitos.

> A vigilância torna-se uma resposta adequada a um sentimento generalizado de insegurança. Tendências psicológicas, a mídia e os políticos contribuem para um ambiente em que as medidas de vigilância são muitas vezes introduzidas com base em um incidente dramático e terrível, mas estatisticamente improvável que recebe uma grande quantidade de meios de comunicação social, política e atenção do público (Bennet, 2014: 45).

Esta intolerância crescente ao risco torna-se mais importante do que a verdadeira natureza e o nível dos riscos. Um exemplo disso é a introdução de medidas de lei e ordem radicais e dispendiosas pelo governo do Canadá em 2012, considerando a violência da criminalidade, agiu na contramão dos dados estatísticos, os quais apontavam uma baixa na criminalidade em quarenta anos. O risco de que algo ruim poderia acontecer introduzia a justificativa de mais medidas de segurança.

Por outro lado, Bennet (2014) argumenta que a evolução das mudanças tecnológicas também gerou a produção de novos riscos, de consequências inesperadas. Ao mesmo tempo em que a gestão da informação facilitou a ação de governos e negócios, também levanta questões acerca da vigilância e da privacidade, especialmente pelo avanço em áreas como câmeras de vigilância, biometria, localização e rastreamento de sistemas, sistemas de telecomunicações. Tais artifícios têm facilitado a coleta e o processamento de informações, fazendo com que a regulamentação esteja muito aquém da implantação dessas novas tecnologias. O número de dados gerados pelos dispositivos tem se transformado em um grandioso aparato que coloca em xeque a segurança de tais informações.

O CASO BRASILEIRO

Diante dos conceitos de vigilância e controle e da questão dos riscos, busca-se agora analisar a forma como esses pontos permearam o debate do Marco Civil. O tema da segurança contra o cibercrime pode ser verificado na questão da responsabilização dos provedores pelo armazenamento de dados, a fim de se identificar usuários e de se contribuir com investigações criminais. Como já ressaltado neste artigo, a discussão sobre segurança entre agentes da Polícia Federal, peritos, delegados e advogados ligados ao Direito digital era sobre a possibilidade de detectarem dificuldades nas suas atividades de investigação, como o chamado "apagão da perícia", ou seja, dos rastros deixados pelos usuários em seus logins nos aplicativos móveis e de navegação. Eles chegaram a usar inúmeros exemplos para convencer parlamentares acerca da importância desses dados no caminho das investigações e confiaram na pessoa do relator Alessandro Molon a mudança da redação do artigo de modo a atendê-los.

A visão desses representantes se assemelhava às propostas que já haviam sido apresentadas por deputados federais em anos anteriores, que traziam instrumentos capazes de futuramente criminalizar usuários de forma errônea ou mesmo cercear a liberdade no uso da rede. Uma delas foi o famoso projeto de lei 84/1999, apresentado pelo deputado Eduardo Azeredo (PSDB), denominado AI-5 Digital, que visava criminalizar o usuário, permitindo o acesso a dados pessoais pela polícia e o Ministério Público sem o aval judicial.

No âmbito do Marco Civil, o maior ponto de conflito estava na possibilidade de facultar aos provedores de aplicação, ou seja, às empresas que fornecem o aplicativo como Skype, Facebook, Twitter, Microsoft, Apple, a guarda dos dados. Essas corporações passariam a não ter que armazenar os logs de acesso dos usuários em suas aplicações: o usuário quando entra em sua conta no Facebook, digita ali o seu e-mail e sua senha. Nesse momento, o próprio sistema registra o horário que foi feito o login, de qual IP foi realizado o login, sua localização e possivelmente as páginas acessadas ou curtidas, os contatos feitos, a duração da conversa. Ainda que a empresa garanta que este tipo de informação não significa a guarda de conteúdo das mensagens ali trocadas, mas sim dos chamados logs, ela não seria obrigada a armazená-los.

Em resposta às reivindicações, o relator da matéria explicou que impor a retenção desse material a pequenos provedores de aplicação poderia incidir em custos enormes para o pequeno empresário, citando, por exemplo, sites que teriam de registrar quaisquer tipos de informação em uma simples pesquisa realizada por seu cliente. Seguindo essa informação, defensores da garantia da privacidade se manifestaram a fim de proibir ao provedor de aplicações essa guarda, uma vez que isso poderia implicar no armazenamento, sem consentimento, de informações sigilosas dos usuários. Também alertavam sobre a possível vulnerabilidade à qual se submeteria o grande volume desses dados, uma vez que uma ação hacker poderia inclusive acessá-los, filtrá-los, distribuí-los, criar perfis de consumo e vendê-los. Tal ação poderia gerar consequências graves para o usuário, tendo em vista que informações pessoais estariam ali armazenadas, consentidas ou não, sendo elas fruto do mecanismo de rastreamento de sistemas que possibilitaria o seu

armazenamento.

Diante desse cenário, acadêmicos chegaram a sugerir que se fizesse a guarda dessas informações "no menor tempo possível", a fim de evitar a retenção exagerada dessas informações por bancos de dados "amplos e desregulados demais". Um dos criadores do texto base do Marco Civil da Internet, o professor da Fundação Getúlio Vargas, Luiz Fernando Marrey Moncau, já havia defendido a Internet Livre em comissão de discussão da matéria, sem a intervenção do estado ou empresas. Ele considerou que o texto do projeto de lei, que ainda estava em tramitação, seria uma importante ferramenta para assegurar a privacidade, incluindo a vedação à prática de empresas que "bisbilhotam" as comunicações entre os usuários.

Os deputados ligados à bancada da segurança, como Sandro Alex (PPS-PR) e Fernando Francischini (SDD-PR), que chegaram a apresentar emendas parlamentares para guarda de dados de aplicação pelo prazo de 12 meses, citavam como exemplo o caso de investigações em que a Polícia Federal necessitou do uso dessas informações para chegar até o autor do ato ilícito. Eles criticavam o estabelecimento de 12 meses apenas para a guarda de registro de conexão por provedores de conexão, ou seja, do horário, localização e IP em que o usuário teve acesso à internet, mas sem o mesmo prazo para a guarda de informações pelos aplicativos que o usuário teria acessado. Na argumentação, afirmavam sobre o risco de que a investigação criminal pudesse ser interrompida, uma vez que tais provedores poderiam apenas alegar que não teriam armazenado os dados, já que a lei não os obriga, o que possivelmente geraria um vácuo para o investigador. Na tentativa de coibir a facultação dessa guarda, o deputado Mendonça Filho (DEM) também chegou a apresentar uma emenda para inserir a obrigatoriedade desse armazenamento.

O deputado Alessandro Molon, relator da matéria, chegou a mencionar a necessidade de um "equilíbrio fino" em relação aos dados e à segurança. Informou que a nova lei garante a presunção de inocência na internet, respeitando preceitos constitucionais. Os posicionamentos do Ministério da Justiça e do Instituto Brasileiro de Defesa do Consumidor (IDEC) também levantaram uma importante questão acerca da garantia da presunção da inocência, mas alimentavam uma pergunta: até que ponto vale colocar em xeque a inocência do usuário, quebrando sua privacidade, para se consolidar a ação de mecanismos de segurança? Assumindo um caráter de estabelecer princípios, como defendeu o relator da matéria, e deixando para lei específica as situações envolvendo crimes na rede, como reforçou o presidente da comissão, João Arruda, o Marco Civil pensaria mais em termos de disciplina e garantia de direitos aos usuários e menos em criminalização, ponto esse que foi um dos de maior conflito.

Buscando estabelecer o consenso entre as partes e garantir uma redação ao texto de forma que atendesse as partes em disputa, e sem risco de prejuízo ao projeto de lei por causa desse embate, o relator Alessandro Molon (PT) inseriu no texto a obrigatoriedade por um período menor, de seis meses para a guarda de aplicações, delimitando que os dados fossem armazenados em local seguro. Outra ponderação foi a de que os provedores de conexão (como teles, operadoras, empresas que fornecem internet) não tivessem acesso a estes dados de aplicação, uma vez que

eles têm consigo dados cadastrais de usuários da internet, como RG e CPF, informados no ato da contratação, o que poderia ocasionar uma compreensão global acerca de gostos e preferências de indivíduos, prejudicando sua privacidade.

Molon afirmou que a proibição de guardar dados ao provedor de conexão seria uma importante forma de vedar o monitoramento ou a análise do conteúdo postado pelos usuários na rede. Em seu relatório, destacou os princípios de liberdade e controle como pilares da internet, inclusive mencionando os protocolos que sustentam a comunicação interativa. O deputado citou os rastros digitais deixados pelos usuários, explicando que é muito mais fácil monitorar as pessoas na internet do que na vida real. E, dessa forma, o monitoramento é realizado de forma indevida, e deve ser coibido para que a liberdade de expressão e a privacidade não sejam tolhidas. Destaca ainda que foram feitas alterações no texto do projeto para garantir maior proteção à privacidade dos internautas, sem que isso prejudique a inovação ou os modelos de negócio.

O respeito à legislação brasileira na coleta de dados também foi um dos pontos inserido pelo relator no texto, considerado como um instrumento "para proteger ainda mais a privacidade e o sigilo dos dados pessoais, das comunicações privadas e dos registros". A medida abrange qualquer empresa sediada no exterior, desde que pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil, "de modo que a simples localização de dados em bancos de dados no exterior não exclua a aplicabilidade da legislação brasileira, quando pelo menos uma empresa integrante do mesmo grupo econômico tiver estabelecimento no Brasil", aponta o relator.

CONSIDERAÇÕES FINAIS

A forma como se revela o anseio pela segurança em um debate acerca da regulamentação da Internet torna-se um fator preocupante diante do cenário de controle e ampliação do investimento em ferramentas de monitoramento e prospecção de informações. Criando um modelo de institucionalização da vigilância, provocado por amparo legal que autoriza o armazenamento de informações, percebe-se que o discurso do medo e da insegurança se tornam argumentos para favorecer os trabalhos de investigação e ação de órgãos vigilantistas. Pode-se constatar, portanto, que aspectos de natureza conservadora tomam o debate sobre a regulamentação da rede, principalmente pelos deputados e órgãos que representam o segmento policial. São discursos que buscam ampliar a sensação de insegurança, irrompendo os princípios da presunção da inocência e classificando os usuários da internet como suspeitos. A privacidade entra como o fator chave justamente pelas ações de monitoramento e comercialização de dados que poderiam se estabelecer com a guarda de dados de aplicações por muito tempo. O equilíbrio buscado pelo relator Alessandro Molon acabou se consolidando com a estipulação de um prazo menor do que os registros de conexão, sendo esse de apenas seis meses.

Um aspecto que se pode observar é o lugar em que o Governo brasileiro se posiciona em toda a discussão sobre o armazenamento de dados. Diferentemente do discurso norte-americano,

de se fortalecer as ações de combate ao terrorismo monitorando indivíduos, o governo, pelo menos na esfera do Marco Civil, atua inicialmente de modo a facultar aos provedores de aplicação a guarda desses registros. Cabe aos deputados de oposição ao Governo Dilma a fala mais veemente para estabelecer a obrigatoriedade, inclusive ameaçando derrubar o projeto de lei no caso de não se garantir o período de guarda.

Outro ponto que permite maior discussão é a questão da jurisdição, a qual, embora pertença a uma questão específica do Direito digital, merece aqui um destaque especialmente pela preocupação mundial em torno da efetividade das políticas que possam ser desenvolvidas, tendo em vista o advento da comunicação em rede. O respeito à legislação brasileira na coleta de dados foi um aspecto inserido pelo relator no texto, considerando-o um instrumento "para proteger ainda mais a privacidade e o sigilo dos dados pessoais, das comunicações privadas e dos registros", nas palavras do relator. A medida abrange qualquer empresa sediada no exterior, desde que pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil. Na tentativa de se preservar mecanismos jurídicos que remetam ao território, ou seja, que responsabilize empresas por atos cometidos em âmbito nacional, o crime cometido em um ambiente que não se estabelece sobre o "território", mas em cabos ópticos, a quem cabe julgar o ilícito? A questão demonstra como a organização transfronteiras do mundo em rede provocou uma mudança em todo o sistema, permitindo refletir não somente sobre as ações dos indivíduos neste cenário, mas as possíveis implicações que essas ações possam gerar, sem que haja respostas imediatamente claras.

REFERÊNCIAS

Assange, J. (2013).*Cypherpunks: liberdade e o futuro da internet* . São Paulo: Boitempo.

Bennett, C. (2014). Transparent Lives Surveillance in Canada (pp.39-51). Edmonton: AU Press, Athabasca University.

Bruno, F. (2004). Máquinas de ver, modos de ser: visibilidade e subjetividade nas novas tecnologias de informação e de comunicação.*Revista Famecos* , 24, 110-124.

Bruno, F. (2013).*Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade* . Porto Alegre: Sulina.

Lei 12.965, de 23 de abril de 2014. Dispõe sobre o Marco Civil da Internet. Recuperado em 10 fevereiro, 2016, de http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

Lyon, D. (2015).*Surveillance After Snowden* . Cambridge, UK: Polity Press.

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. Revista Big Data &Society. Recuperado em 29 março, 2016, de http://bds.sagepub.com/content/1/2/2053951714541861.

Silveira, S. A. (2012). Poder tecnológico como poder político. In: Cultura, política e ativismo nas redes sociais

(pp. 15-29). São Paulo: Fundação Perseu Abramo.

Silveira, S. A. (2014). Regulamentação e liberdade na rede: o Marco Civil da Internet. In: Lima, V. A., Guimarães, J., Amorim, A. P. Em defesa de uma opinião pública democrática: conceitos, entraves e desafios (1ª Ed. Cap.8, pp.239-255). São Paulo: Paulus.