BRUNA CHIECO

Privacidade na berlinda

As discussões no Brasil sobre a melhor maneira de garantir a privacidade e segurança dos dados trafegados na internet, após as revelações da existência de um programa de espionagem do governo dos EUA, estão longe de um consenso, embora todos defendam a necessidade de um marco civil

As revelações sobre o programa de espionagem do governo dos Estados Unidos reacenderam as discussões envolvendo privacidade, segurança e o sigilo dos dados trafegados na internet em todo o mundo, inclusive no Brasil. Os documentos vazados pelo ex-técnico da CIA Edward Snowden indicaram que a Agência de Segurança Nacional (NSA dos EUA) e o FBI (polícia federal americana) tinham acesso direto aos dados de usuários nos servidores de empresas de internet, como Apple, Google, Facebook e Microsoft.

No caso específico do Brasil, as denúncias trouxeram novamente à baila o debate em torno do marco civil da internet. O governo Dilma Rousseff decidiu incluir no texto do projeto de lei (PL 2126/2011), que aguarda votação na Câmara dos Deputados desde 2011, a obrigatoriedade de armazenamento de dados no Brasil. O ministro das Comunicações Paulo Bernardo chegou a sugerir que o governo pedisse urgência constitucional para o projeto. A ideia é que os dados fiquem armazenados em data centers instalados no Brasil, por meio da replicação dos servidores das empresas de internet estrangeiras. Para Bernardo, a "nacionalização" do armazenamento de dados dará condições para o governo brasileiro exigir o cumprimento da legislação que protege a privacidade dos cidadãos.

Embora o relator do marco civil da internet, deputado Alessandro Molon (PT-RJ), sustente que o projeto de lei (PL 2126/2011) protege a privacidade do internauta, ele diz que a proposta não impede práticas de espionagem. "A tecnologia permite hoje um nível de controle sobre os indivíduos muito arriscado. Mas preciso dizer com toda franqueza que nenhuma lei impedirá a espionagem. Como nenhuma lei impede a prática de crimes", disse ele, durante audiência pública, no início de agosto, na Comissão de Ciência e Tecnologia da Câmara dos Deputados.

PARA ABRANET, É INADEQUADO ALTERAR O MARCO CIVIL, POIS ISSO TORNARIA INÓQUOS OS PROPÓSITOS DO TEXTO

A obrigatoriedade de armazenamento local de dados também é refutada pela Associação Brasileira de Empresas de Tecnologia da Informação e Comunicação (Brasscom). O diretor de Convergência Digital da Brasscom, Nelson Wortman, atacou a possibilidade de se inserir artigos que tratam desta exigência, argumentando que "o Brasil é menos competitivo que muitos países das Américas no processo de implantação de data centers". Ele ressaltou ainda que "é um equívoco pensar que a localização de um data center garantirá segurança e ampliará o acesso".

A Câmara Brasileira de Comércio Eletrônico (Câmara-e.net), por sua vez, defende um debate amplo da proposta, pois vê riscos da mesma trazer "restrições no futuro, afetando o crescimento e neutralidade da indústria de internet no Brasil, bem como às liberdades fundamentais e liberdade de expressão do

cidadão brasileiro". A entidade acredita que o armazenamento de dados obrigatório pode "gerar altos custos e criar um gargalo tecnológico". Os custos também foram citados por pelo executivo. Ele calcula que o impacto financeiro e tributário para as empresas, se a determinação for mantida, será o dobro do que se gasta para manter as operações nos EUA. "Para manter a operação de um data center no Brasil pelo período de um ano, o gasto atual é de US$ 1 milhão. Nos EUA, esse valor cai pela metade e se compararmos com países vizinhos, o gasto no Brasil é maior 46%", destacou.

Para a Associação Brasileira de Internet (Abranet), é inadequado alterar o projeto de lei do marco civil, pois isso tornaria inócuos os propósitos do texto. A posição oficial da entidade é que o debate sobre o armazenamento de dados no Brasil precisa ser amadurecido e o marco civil não é o instrumento adequado para isso. "O marco civil é objeto de debate há quase três anos e chegamos ao texto do Molon, que tem o consenso de todos que debateram", destacou o presidente-executivo da Abranet, Eduardo Neger. "Preocupa-nos as propostas de alterações na legislação sem o devido debate."

O executivo reitera que o texto atual do marco regulatório já é bastante equilibrado e que transferir os dados de empresas para o Brasil pode não ser um processo tecnicamente simples. "É preciso discutir esse tema para saber se terá alguma eficácia. Não sabemos se é possível [a obrigatoriedade de que os

FOTO: DIVULGAÇÃO

dados fiquem armazenados em data centers instalados no Brasil] e se isso cumprirá com o objetivo da privacidade, pois o servidor não determina quem acessa os dados. Tudo está na internet e não é a posição geográfica do data center que garantirá a privacidade. É um assunto extremamente denso, que não deve ser introduzido no marco civil. Se chegarmos a alguma conclusão, deve ser colocada em alguma outra legislação."

Com opinião diferente, o diretor da empresa de data center Alog, Victor Arnaud, diz que, se a decisão for acompanhada de benefícios para as empresas estrangeiras, a obrigatoriedade poderá tornar o Brasil mais atrativo às relações comerciais. "A regulação deve vir acompanhada de diretrizes para facilitar a presença digital dessas empresas no país. Caso a empresa tenha os dados no Brasil, quem ganha é o usuário. Mas tudo isso deve ser orquestrado, é preciso criar condições para tal", observa Arnaud, ao dizer que a criação de polos tecnológicos em regiões do país com tributação mais baixa, junto com a desoneração da folha de pagamento, entre outras medidas, estimulam as empresas a se instalarem no Brasil.

Legislação

Juristas e especialistas sustentam que nenhuma solução é completa sem uma legislação local. O advogado Márcio Cots, membro da comissão de crimes eletrônicos e alta tecnologia da OAB-SP, diz que a aprovação de uma legislação é o primeiro passo para o Brasil avançar no debate sobre privacidade, pois sem um marco regulatório, o país perde força nessa discussão e não ganha referência para pressionar outros Estados quanto ao uso ilegal de dados pessoais.

"O Brasil está bem atrasado nesta questão em relação a vários países com legislação específica sobre privacidade de dados. A lei tem que seguir um espectro mais amplo para resolver a questão como um todo. O projeto que existe [marco civil] trata de algumas questões mais específicas, independente de onde os dados estejam", destaca. Cots acrescenta que as informações dos brasileiros armazenadas em algum fornecedor de serviço em nuvem ou na própria internet ficam a mercê das regras do provedor justamente pela inexistência de legislação. "Quando não há uma regra estabelecida

> "O marco civil é objeto de debate há quase três anos e chegamos ao texto do Molon que tem o consenso de todos que debateram"
> **EDUARDO NEGER, DA ABRANET**

COMO A ESPIONAGEM DOS EUA AFETA O BRASIL

O jornalista americano Glenn Greenwald, colunista do jornal inglês The Guardian, que teve acesso as informações de Edward Snowden, revelou durante audiência pública conjunta da Comissão de Relações Exteriores e de Defesa Nacional da Câmara dos Deputados e da Comissão de Relações Exteriores e Defesa Nacional do Senado, realizada em agosto, que a espionagem feita no Brasil envolve cerca de 70 mil pessoas. O jornalista também acusou operadoras brasileiras de telecomunicações de trabalharem com uma grande empresa americana que fornece dados para a NSA, dizendo que o governo americano "tem acordos com empresas de telecomunicações brasileiras grandes", permitindo, assim, livre acesso ao sistema das teles para que determinada companhia dos EUA colete dados e os forneça à NSA. "A questão para os brasileiros é quais empresas brasileiras estão trabalhando com essa empresa", disse o jornalista.

Antes dessas denúncias, o Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal (SindiTelebrasil) já havia se manifestado por meio de comunicado afirmando "categoricamente que nenhuma prestadora de serviços de telecomunicações associada ao SindiTelebrasil provê ou facilita informações que possam quebrar o sigilo de seus usuários, salvo mediante ordem judicial na forma da lei brasileira".

Outra acusação de Greenwald, baseada nos documentos de Snowden, diz que o governo dos EUA monitora comunicações eletrônicas dentro e fora do país sob o pretexto de combate ao terrorismo e garantir a segurança nacional, mas na verdade o objetivo seria obter informações privilegiadas sobre acordos econômicos, estratégias políticas e competitividade industrial de outros países. Um exemplo disso foi publicado pela revista Época em julho, revelando que o governo de Barack Obama espionou oito países, entre eles o Brasil, para conseguir aprovar no Conselho de Segurança da Organização das Nações Unidas (ONU) sanções contra o Irã, em 2010. A reportagem traz uma carta da embaixada americana no Brasil comemorando a vantagem que a espionagem trouxe ao EUA nas negociações do caso.

por lei, os termos de uso da empresa se sobrepõem."

Com uma legislação é mais fácil pressionar as empresas para se adequarem às regras de privacidade do país, como a União Europeia faz constantemente com empresas americanas como Google e Facebook, exigindo mudanças em suas políticas de privacidade para que fiquem de acordo com as leis dos países europeus. "O Brasil está atrasado, mas existe o projeto de lei de proteção de dados, que é baseado na legislação europeia, com intenção de devolver os dados aos próprios usuários, dando ao cidadão autonomia para decidir sobre suas informações", ressalta Cots, citando o projeto de lei que trata do uso dos dados pessoais dos usuários — como históricos de navegação e cookies — por parte das empresas. A proposta pretende tirar o Brasil da condição de único país do G20 sem uma legislação sobre o tema.

"O Brasil está bem atrasado nesta questão em relação a vários países com legislação específica sobre privacidade de dados"

MÁRCIO COTS, DA COMISSÃO DE CRIMES ELETRÔNICOS DA OAB-SP

Na opinião do advogado Renato Opice Blum, um acordo entre os países é essencial para resolver as questões de uso de dados de usuários. Segundo ele, manter o controle das informações no Brasil facilitaria o cumprimento de uma ordem judicial, pois como os dados estariam armazenados em servidores instalados aqui, ficariam sujeitos às leis do país. Hoje, no entanto, como a maioria dos servidores das empresas de internet estão nos Estados Unidos, elas estão sujeitas à legislação daquele país. "Então ocorre um conflito internacional de normas", ressalta.

Para Blum, as leis não podem ter tratamento distinto, pois sempre haverá conflitos entre os países envolvidos. Ele cita o caso do próprio Google, alvo de uma ação judicial impetrada pelo Superior Tribunal de Justiça (STJ), que determinou quebra do sigilo das comunicações feitas por usuários do serviço investigados por crimes. O Google Brasil, em sua defesa, alegou não ser possível cumprir a ordem judicial uma vez que todos os dados do serviço estão armazenados nos servidores dos Estados Unidos e, desta forma, sujeitos às legislações daquele país. "Nesse caso, o STJ insiste em obter os dados e, se virar uma situação insustentável, pode tornar até a operação comercial inviável."

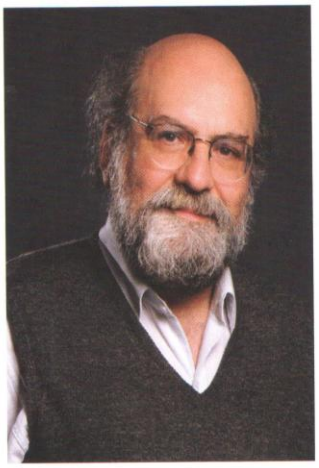
Opinião semelhante tem o advogado Victor Auilo Haikal, sócio do escritório Patricia Peck Pinheiro Advogados, para quem a solução ideal seria a criação de uma legislação internacional que definisse

claramente como os dados são armazenados e o que pode ser feito com eles. "A atividade de espionagem das agências de inteligência norte-americanas já violam a legislação brasileira pela interceptação indevida do tráfego ou pelo acesso ilegítimo a base de dados", destaca Haikal. "Porém, a legislação de outros países dá margem para que ocorram essas atividades. O que pode ser feito é um acordo entre os países para o estabelecimento de condutas sobre o que fazer no mundo cibernético."

Os três advogados concordam num ponto: que a sociedade é que deve decidir como quer que seus dados sejam utilizados, cabendo ao Estado a conscientização dos usuários sobre como esses serviços utilizam suas informações pessoais.

Porta dos fundos

Mesmo que as partes envolvidas cheguem a um consenso sobre a questão do armazenamento dos dados, o problema



envolvendo a privacidade não será totalmente resolvido. Isso porque boa parte do tráfego informacional da internet ocorre por meio de cabos submarinos que se concentram em determinadas regiões por razões técnicas. Além disso, há suspeita de existência e funcionalidades de backdoor (porta do fundos) nos equipamentos de rede, já que os principais fabricantes mundiais são de origem norte-americana. "A maioria dos dados estão no exterior, em locais desconhecidos, e é preciso contar com a ética do provedor de serviço para garantir o não vazamento", destaca Demi Getschko, diretor presidente do Comitê Gestor da Internet no Brasil (CGI.br).

O especialista diz que a backdoor é motivo de preocupação, pois muitas vezes o fornecedor de equipamentos deixa uma porta aberta no dispositivo a pedido de governo para casos de emergência, mas nada impede que um hacker acesse essa porta. "É uma brecha de segurança que pode ser explorada por alguém de fora."

Para Nelson Simões, presidente da Rede Nacional de Ensino e Pesquisa (RNP), as denúncias ex-técnico da CIA Edward Snowden comprovaram algo que já é conhecido há algum tempo — a existência de atividades de vigilância. Segundo ele, o dispositivo chamado "Deep Packet Inspection", que serve para analisar em tempo real dados digitais que circulam pela internet, pode estar sendo utilizado pelo governo e empresas para rastrear as comunicações das pessoas. "Mas nunca havia sido comprovado que o governo usava para inspeção profunda de tráfego global", destaca. "Isso é usado normalmente por forças de segurança, mediante autorização judicial. Ainda que no caso norte-americano esteja dentro da legislação deles, ultrapassou a fronteira da comunicação dos países, incluindo o Brasil."

Simões reitera que vivemos em um mundo no qual os dispositivos se comunicam entre si com múltiplas interconexões, ambiente este sujeito a vulnerabilidades e riscos inerentes. "A porta dos fundos de um dispositivo também é conhecida há muito tempo. Não acredito que isso seja um risco importante ou problema fundamental a ser resolvido, mas há dispositivos de muitas naturezas e é difícil assegurar que não tenha vulnerabilidade no hardware ou no software", destaca ele, acrescentando a importância de um marco legal que proteja e assegure a privacidade dos direitos civis para contemplar todas essas questões.

"A backdoor é motivo de preocupação, pois muitas vezes o fornecedor de equipamentos deixa uma porta aberta no dispositivo e nada impede que um hacker a acesse"

DEMI GETSCHKO, DO CGI.BR