Demócrito Filho: EUA debatem quebra de sigilo virtual sem ordem da Justiça

06/06/2013

Em 18 de abril de 2013, foi aprovado na Câmara de Representantes[1] (deputados) dos EUA (por 288 votos a 127) um controverso projeto de lei, denominado de *CISPA* (*Cyber Intelligence and Protect Act*)[2], que, se aprovado, irá permitir às agências de inteligência requisitar informações aos provedores de Internet e serviços de telecomunicação ou fazer varreduras em suas bases de dados, sem necessidade de mandado judicial[3].

Um deputado democrata, Alan Grayson, ainda tentou inserir uma emenda[4] que previa a exigência de mandado judicial para que as agências de inteligência (*NSA–National Security Agency*, *FBI–Federal Bureau of Investigation* e o *Department of Homeland Security-DHS*) tivessem acesso aos cadastros e conteúdo das mensagens pessoais dos usuários dos serviços de comunicação, mas foi vencido. Isso significa que as políticas de privacidade e termos de uso das grandes empresas da Internet, como Google, Facebook e Twitter, não terão nenhuma eficácia, pelo menos em relação ao governo federal, se aprovado o projeto de lei.

O *CISPA* tem como objetivo o aparelhamento dos serviços de segurança dos EUA para a chamada *cyberwar*, por isso reescreve algumas disposições do Ato de Segurança Nacional (*National Security Act*) de 1947. É sugerido o acréscimo do conceito de uma "cyber threat intelligence", definida como toda informação que tem relação com vulnerabilidades de redes ou sistemas informáticos (do governo ou do setor privado) ou ameaças à confidencialidade e integralidade das informações. Objetiva também possibilitar a investigação de crimes graves cometidos através de redes informáticas contra menores, como pornografia infantil digital, exploração sexual e sequestros.

A parte complicada aparece quando, na tentativa de atingir esses relevantes objetivos, incentiva a troca de informações entre as agências do governo e as companhias privadas, bem como quando imuniza as empresas de qualquer responsabilidade civil ou criminal por eventual uso ilegal posteriormente feito com informações transferidas. Assim, sob o texto do *CISPA*, qualquer empresa privada poderá fazer uso de seu sistema informático para identificar uma "cyber threat information" e, em seguida, repassá-la para os órgãos de inteligência do governo.

E-mails, mensagens de texto, arquivos armazenados em nuvem, enfim, qualquer informação pessoal poderá ser transferida, desde que a transferência seja feita para propósitos de cibersegurança. O projeto estabelece certas restrições ao uso das informações pessoais, prevendo sanções para os agentes federais que utilizá-las para outros fins, consideradas todavia insuficientes para proteger a privacidade e liberdades individuais.

A atual legislação norte-americana, especialmente a ,lei conhecida como *Wiretap Act*[5], proíbe os provedores de Internet de interceptar as comunicações dos usuários, salvo quando isso é necessário para o fornecimento do próprio serviço ou obtiverem consentimento prévio. A interceptação, como regra, depende de autorização judicial expressa.

Mas a própria lei prevê uma exceção para a exigência de mandado judicial, ao estabelecer que os provedores de serviços de comunicações eletrônicas podem repassar informações ou auxiliar os agentes policiais na interceptação ou monitoramento das mensagens quando certificado por escrito pelo advogado-geral da União (ou pessoa por ele designada) da desnecessidade de mandado judicial, ante a excepcionalidade da medida.

Essas cartas escritas aos provedores, que lhes imunizam de responsabilidade pela interceptação e entrega do conteúdo das comunicações dos seus usuários, ficaram conhecidas como "2511 letters", uma referência ao capítulo do Código federal onde o *Wiretap Act* foi incrustado (18 USC § 2511). Assim, ainda que de alcance limitado, o braço executivo do governo norte-americano já dispõe de instrumento legal para requisitar informações diretamente dos provedores de serviços de comunicações.

O problema é que o governo pretende expandir seu programa de cibersegurança, o que implica a necessidade de processar uma quantidade muito maior de informações pessoais pelas agências de inteligência. Depois dos ataques de *hackers* a sites do governo, o presidente Barack Obama assinou uma ordem executiva em fevereiro deste ano[6], autorizando o advogado-geral, o Departamento de Segurança Nacional (Homeland Security Department) e a NSA (National Security Agency) a expandir programas de monitoramento e de coleta de informações para proteger setores considerados essenciais da infraestrutura de serviços públicos, como a rede de distribuição de energia elétrica, instituições financeiras, sistema de controle de tráfego aéreo, hospitais e centros de assistência à saúde, entre outros.

O objetivo principal, como se disse, é aumentar o volume de troca de informações entre os provedores privados de serviços de comunicação e as agências de inteligência, de forma a evitar novos ataques. Mas o Executivo não tem autoridade para autorizar um monitoramento mais extenso, a não ser que o Congresso altere a legislação existente. Se o *CISPA* for aprovado, as agências de inteligência do governo federal poderão requisitar informações em volume ilimitado aos provedores de comunicações e serviços na Internet, sem necessidade de recorrer às "2511 letters" (de uso restrito) e sem supervisão ou autorização judiciária.

Da mesma forma que aconteceu com as famigeradas *SOPA* (*Stop Online Piracy Act*) e *PIPA* (*Protect IP Act*), projetos que pretendiam combater a pirataria e alargar o âmbito de proteção a direitos autorais na Internet[7], mas que terminaram não passando no Congresso[8], o *CISPA* está sofrendo uma reação muito grande de grupos e associações ligadas à defesa das liberdades civis. A *Electronic Frontier Foundation*[9], ONG que defende a privacidade dos usuários na internet, condenou a aprovação do projeto na Câmara dos Representantes. Já a *Fight for the Future* reuniu 1,5 milhão de assinaturas em petição para que os deputados rejeitassem o projeto. Agora, essa ONG pretende derrubar o projeto no Senado. Para tanto, vem fazendo uma grande mobilização na Internet. Montou um site[10] só para recolher apoios contra o CISPA, prometendo organizar o maior protesto *on line* da história.

Elas alegam que o projeto pode eliminar garantias tradicionais estabelecidas em leis como o *C able Communications Policy Act*, o *Wiretap Act*, o *Video Privacy Protection Act* e o *Electronic Communications Privacy Act*, os quais preveem supervisão judicial e outras proteções que proíbem as empresas de trocar informações privadas. De fato, o *CISPA* pode tornar ineficaz

esse conjunto de normas, pois um dos seus artigos dispõe que, “a despeito de provisões existentes em outras leis”, “as empresas podem trocar informações com qualquer outra entidade, incluindo o Governo Federal”, para fins de cibersegurança. Além disso, o projeto de lei confere uma imunidade quase absoluta às empresas, que ficarão isentas de culpa caso terceiros ou o governo use os dados repassados de forma indevida, desde que ajam de “boa-fé” ao repassar as informações.

A diferença é que, dessa vez, o projeto vem recebendo um amplo apoio do setor empresarial. Grandes companhias como IBM, Intel, AT&T, Verizon, Oracle, Symantec, Comcast e outras que formam o consórcio *Internet Security Alliance*[11] já anunciaram seu firme suporte à reintrodução do *CISPA*, escrevendo cartas ao Comitê de Inteligência da Câmara dos Representantes (*House of Representatives*) endossando a iniciativa. Quando da introdução do *SOPA* e do *PIPA*, gigantes da Internet como *Google* e *Facebook* apressaram-se em condená-las publicamente, dizendo que esse tipo de legislação permitiria que as autoridades federais fechassem muitos sites e plataformas de distribuição de arquivos sem o devido processo legal, além de atentar contra a liberdade de expressão, o que levou outros formadores de opinião e empresas na Internet a fazer o mesmo. O Google e o Facebook ainda não endossaram a nova versão do *CISPA*, mas parece que também não se pronunciaram oficialmente contra[12].

O texto ainda precisa passar pelo Senado (onde os democratas têm maioria) e, se aprovado, pela sanção de Obama. Mesmo que seja aprovado no Senado, dificilmente receberá a sanção presidencial, pois o presidente já ameaçou vetar o *CISPA*[13]. Em pronunciamento oficial[14] feito pela Casa Branca, foi dito que o *CISPA* ameaça a privacidade dos cidadãos norte-americanos e imuniza os provedores de serviços de comunicações de forma inapropriada. Mas o projeto segue em caminho à aprovação. O sentimento geral entre as empresas é de que elas precisam de uma legislação que lhes possibilite receber informações do Governo sobre ameaças à segurança de suas estruturas de rede e serviços informáticos.

A perspectiva da aprovação do projeto de lei é realmente preocupante, não somente para os norte-americanos mas para qualquer cidadão de qualquer nacionalidade que se utilize da rede mundial de comunicação. Sem as devidas garantias, o *CISPA* pode se transformar em um grande sistema de monitoramento da internet. A chamada “cybersecurity bill” irá afetar, assim, a vida de todos os cidadãos que usam serviços online prestados pelas grandes empresas americanas do setor de Tecnologia de Informação, o que inclui todos nós, brasileiros. Na prática, a lei vai permitir que nossas informações sejam repassadas ao governo dos EUA, e às empresas daquele país que o fizerem não poderão ser acionadas na Justiça americana, diante da imunidade legal que receberão.

Os grandes *players* no mercado de serviços online são empresas norte-americanas e todos os cidadãos do mundo se tornaram consumidores cativos delas. A globalização, no sentido da prestação de serviços em escala global pela rede de comunicações mundial, produziu esse fenômeno. A noção de que uma lei em regra não tem efeitos extraterritoriais, vigorando apenas dentro dos limites geofísicos do país onde é editada, perdeu a validade. Estamos presenciando agora, e na prática, que uma lei aprovada no Congresso norte-americano não produz efeitos somente sobre a vida dos estadunidenses, mas de todo o mundo. As garantias das leis brasileiras e da Constituição, que resguardam a privacidade, também de nada valerão. É como

se perdêssemos nossa soberania. Por isso, é imperativo que todos, de qualquer nacionalidade, participem desse debate. Não podemos ficar alheios ao que está acontecendo de tão importante para as nossas vidas hoje no Congresso norte-americano.

As empresas americanas que prestam serviços na Internet e o Governo dos EUA têm todo direito de se prevenir de ataques que possam destruir ou afetar criticamente sua infraestrutura de redes telemáticas e serviços de comunicação[15]. Mas isso não pode ser feito ao custo da eliminação da privacidade e liberdades civis. Algumas garantias tradicionais como a supervisão judicial na interceptação das comunicações devem ser preservadas, bem como a possibilidade de acionamento judicial por lesões decorrentes da utilização indevida de dados pessoais. Os cidadãos devem ter direito de saber quais informações suas estão sendo repassadas e que as empresas adotem adequadas salvaguardas de proteção da informação pessoal.

Em 2007, foi proposta a Lei intitulada *Federal Agency Data Mining Reporting Act*, que obrigava a todo órgão federal que usa ou desenvolve programas de *data mining* a apresentar um relatório anual ao Congresso dos EUA. Essa lei foi uma resposta à iniciativa da implantação, pelo Departamento de Estado, do sistema que ficou conhecido como *Total Information Awareness*, que consistia em uma imensa base de dados eletrônica, um "Big Data"[16], que se alimentaria de informações de outros bancos de dados públicos e privados – a face da política de combate ao terrorismo, elevada pela administração George Bush como prioridade máxima de governo[17]. Agora a situação se inverte. É o Congresso (com maioria republicana na Câmara) que pretende criar, por via legislativa, um grande sistema intra-governamental de troca de informações com empresas privadas, a pretexto de se preparar para a *ciberwar*.

Parece que os políticos conservadores que tomaram o controle da Câmara baixa do Congresso dos EUA entenderam que não é preciso gastar centenas de milhões de dólares com a criação e expansão de uma grande base de dados gerida por uma agência de inteligência do governo. Basta requisitar as informações dos *Big Datas* já criados pelo setor privado – como Google, Facebook, Twitter e outros prestadores de serviços na Internet.

[1] Conforme notícia no site da NBC News – http://www.nbcnews.com/technology/cispa-passes-house-vote-faces-senate-possible-veto-1C9357282

[2] http://thomas.loc.gov/cgi-bin/bdquery/z?d112:h.r.03523:

[3] O Projeto de Lei conhecido como *CISPA* foi reintroduzido no Congresso norte-americano em fevereiro deste ano pelo Deputado Mike Rogers (Republicano do Estado de Michigan), tendo recebido o número H.R. 624.

[4] http://www.rules.house.gov/amendments/GRAYSO_069416130828452845.pdf

[5] Codificado no estatuto federal 18 USC 2511

[6]http://pt.scribd.com/doc/125223125/IMPROVING-CRITICAL-INFRASTRUCTURE-CYBERSECURITY

[7] Os dois projetos de lei objetivavam combater *downloads* ilegais de músicas, *streaming* de filmes e shows de tv. Mas muitos formadores de opinião na Internet, incluindo os gigantes *Google* e *Facebook*, alegaram que a legislação permitiria que as autoridades federais fechassem muitos sites e plataformas de distribuição de arquivos sem o devido processo legal, além de atentar contra a liberdade de expressão.

[8] Ver notícia em: http://www.nbcnews.com/technology/sopa-not-part-cybersecurity-bill-spokesman-says-157881

[9] https://www.eff.org/

[10] http://www.sitesnotspies.org/

[11] A **Internet Security Alliance** (ISAlliance), fundada em 2001, é uma espécie de associação sem fins lucrativos, dedicada à segurança cibernética. Reúne os grandes fabricantes de produtos eletrônicos e faz lobby para as empresas quanto a interesses de segurança corporativa.

[12] Google, Facebook e outras redes sociais não endossaram essa nova versão do *CISPA*, mas tinham apoiado textos anteriores do projeto, porque essas empresas acreditam que necessitam de legislação que lhes possibilite trocar informações com órgãos do Governo, no que tange à segurança de suas estruturas de redes e plataformas de serviços.

[13] http://news.cnet.com/8301-31921_3-57421267-281/white-house-takes-aim-at-cispa-with-formal-veto-threat/

[14] http://www.whitehouse.gov/sites/default/files/omb/legislative/sap/113/saphr624r_20130416.pdf

[15] Ainda mais agora, quando se noticia uma verdadeira *ciberwar*, com ataques cibernéticos sendo perpetrados contra empresas privadas e órgãos do Governo dos EUA, originados de grupos de hackers chineses – ver notícia em: http://www.nytimes.com/2013/05/20/world/asia/chinese-hackers-resume-attacks-on-us-targets.html?smid=fb-share&_r=0

[16] **Big Data**, nome em inglês usado para definir a tectônica quantidade de dados e informações que pode ser produzida e armazenada por um sistema de base de dados eletrônica.

[17] Quem se interessar em saber mais sobre o *Total Informantion Awareness – TIA* e a reação que ele despertou, sugerimos a leitura de artigo de nossa autoria publicado no site Consultor Jurídico, em janeiro de 2003, acessível em: http://www.conjur.com.br/2003-jan-23/sistema_coleta_dados_ameaca_privacidade_eua