A ESPIONAGEM ELETRÔNICA - a resposta do Governo americano e das empresas de tecnologia

Demócrito Reinaldo Filho
Juiz de Direito (32ª. Vara Cível do Recife)

Temendo ser processadas como colaboradoras do sistema de espionagem eletrônica mantido pela NSA (*National Security Agency*, na siga em inglês da agência de inteligência norte-americana), diante de um previsível espoucar de ações judiciais em vários países, as principais empresas de Internet americanas encaminharam uma carta ao Governo dos EUA, na qual requerem autorização para tornar públicas as informações sobre usuários que foram obrigadas a repassar à agência[1]. Assinam a carta quase duas dúzias de empresas de tecnologia, entre elas a Apple, o Facebook, o Google, a Microsoft, o Twitter e o Yahoo. Essas empresas pedem mais transparência em torno das "national-security letters", como são conhecidas as ordens emanadas por agentes do Governo para que repassem informações dos usuários.

As empresas de tecnologia querem divulgar o número de ordens e requisições que recebem, o número de usuários e contas afetadas e o tipo de informação requisitada. Assegurar a transparência em torno desse assunto "é importante para o povo americano, que tem direito de ter um debate público sobre a conveniência dessas requisições...bem como para o usuário internacional dos serviços dos provedores americanos, preocupado com a privacidade e segurança de suas comunicações", diz trecho da carta.

As empresas também pedem ao Congresso para editar legislação que exija mais transparência do Governo nesse assunto, que deve ser obrigado a produzir relatórios mais transparentes, bem como permitir que as companhias privadas divulguem seus próprios relatórios. A carta é endereçada ao Presidente Obama, aos líderes no Congresso e às autoridades dirigentes das agências de inteligência e segurança. É assinada também por três dúzias de associações e entidades de defesa de direitos civis.

Essa não é a primeira vez que as empresas de tecnologia tomam algum tipo de iniciativa para se desvencilhar da responsabilidade por terem repassado informações às agências de inteligência, inclusive de usuários não residentes nos EUA. Desde que foram divulgadas as denúncias sobre o programa PRISM, que coleta informações de usuários das grandes empresas da Internet, os gigantes do Vale do Silício estão de alguma maneira tentando lustrar suas imagens perante o público, chamuscadas pela revelação do escândalo de espionagem. Procuram demonstrar que têm um genuíno compromisso com a privacidade e segurança dos dados de seus usuários, não sendo meros serventes do Governo. De fato, às denúncias de espionagem se seguiu uma forte campanha das empresas de tecnologia para se mostrarem como defensores da transparência[2]. Apple, Google, Facebook e Yahoo publicaram declarações logo em seguida à divulgação das denúncias de Edward Snowden, negando que tenham conferido um acesso amplo aos seus servidores, mas parecem não ter considerado isso

[1] Cópia da carta pode ser acessada em: https://www.cdt.org/files/pdfs/weneedtoknow-transparency-letter.pdf

[2] Ver reportagem (em inglês) publicada no site da CNN, em 18.07.13, acessível em: http://edition.cnn.com/2013/06/18/tech/web/tech-companies-data-transparent/index.html?iref=allsearch

suficiente, porquanto estão desenvolvendo uma campanha para se imunizar de responsabilização futura. Nota-se sem qualquer esforço que estão tendo orientação de advogados e profissionais do meio jurídico, pela linguagem que utilizam nas declarações.

Algumas empresas de tecnologia já haviam redigido cartas, de forma individual, às autoridades do Governo norte-americano, objetivando a publicação de estatísticas sobre as ordens que recebem para repasse de informações sobre usuários. A Google, por exemplo, requereu ao Procurador-Geral dos EUA[3], Eric Holder, que lhe fosse dada permissão para divulgar o número de "national-security requests" que tem sido instada a cumprir sob o pálio do *Foreign Intelligence Surveillance Act* (FISA) - uma das leis invocadas para legitimar a execução dos projetos de coleta de informações. Todavia, não se pode dizer que tenha sido uma estratégia válida, em termos de evitar responsabilização, pois antes do vazamento do escândalo de espionagem do PRISM a Google não havia reconhecido publicamente que recebe requisições com base no FISA. De certa maneira, a iniciativa apenas tornou público que ela colabora com as investigações das agências de inteligência. Ademais disso, a iniciativa pode não ter sido tão voluntária quanto parece. Antes mesmo das denúncias envolvendo o PRISM, integrantes da Eletronic Frontier Foundation[4], uma entidade de defesa dos direitos civis, já haviam instado o Google a publicar informações estatísticas[5] sobre as ordens fundamentadas no FISA.

Outras empresas têm seguido a mesma estratégia, numa tentativa de demostrar compromisso com a transparência. Microsoft ingressou com petições perante a corte judiciária e junto ao Procurador-Geral, também requerendo autorização para publicar relatório com o número de requisições que recebe[6]. Antes, porém, já havia divulgado relatório[7] contendo as requisições (*national-security letters)* recebidas no segundo semestre de 2012, mas de forma agregada a outras ordens e mandados para investigação de crimes, não individualizando o número de ordens apoiadas no FISA. O Facebook firmou um acordo com o Governo e divulgou uma nota[8], informando a quantidade de requisições recebidas no último semestre de 2012, incluindo as "national-security letters" expedidas com base no FISA. O Yahoo conseguiu, perante o tribunal que supervisiona a atividade de vigilância (o *FISC-Foreign Intelligence Surveillance Court*), uma decisão autorizando-o a tornar público uma requisição que recebeu em 2008[9].

As grandes empresas de tecnologia, como se percebe, querem demonstrar independência do Governo e até mesmo um traço libertário. Na verdade, elas temem perder a confiança de seus usuários, o que pode comprometer seus negócios. Elas estão

---

[3] Cf. reportagem publicada no site da *Time*, de 11.06.13, acessível em: http://business.time.com/2013/06/11/google-were-no-nsa-stooge-and-well-prove-it-if-the-feds-let-us/

[4] www.eff.org

[5] Ver publicação oficial da EFF, acessível no site em: https://www.eff.org/deeplinks/2013/03/hey-google-can-we-have-data-about-fisa-court-orders

[6] Cf. reportagem publicada no site da *Time*, de 17.07.13, acessível em: http://techland.time.com/2013/07/17/microsoft-asks-attorney-general-to-ease-gag-order-on-nsa-program/

[7] Relatório acessível em: http://blogs.technet.com/b/microsoft_on_the_issues/archive/2013/06/14/microsoft-s-u-s-law-enforcement-and-national-security-requests-for-last-half-of-2012.aspx

[8] Ver nota em: http://newsroom.fb.com/News/636/Facebook-Releases-Data-Including-All-National-Security-Requests

[9] Cf. reportagem publicada no site European Union Times, de 16.07.13, acessível em: http://www.eutimes.net/2013/07/yahoo-wins-lawsuit-to-declassify-docs-proving-resistance-to-prism/

conscientes das inúmeras alternativas aos serviços que prestam no mercado - algumas inclusive permitem que os internautas naveguem no ciberespaço de forma anônima. A organização Prism.break.org, por exemplo, estimula o uso de ferramentas de software livre[10], como alternativas aos serviços prestados na rede pelas empresas acusadas de colaborar no esquema de vigilância. Ademais, a carta conjunta endereçada às autoridades governamentais foi elaborada depois que as empresas começam a ser processadas nas cortes judiciárias, juntamente com o Governo, em uma série de ações coletivas (*class actions*) aforadas recentemente[11].

Essas iniciativas das empresas, de quererem alguma forma de transparência em relação às ordens secretas que recebem das autoridades governamentais para coleta de dados e registros das comunicações dos usuários, pode ter algum reflexo no contexto político e judicial interno dos EUA, perante os cidadãos americanos. Mas nenhum resultado certamente terá em relação às denúncias de espionagem dos dados de comunicação da Internet dos "estrangeiros" (onde nós, brasileiros, nos incluímos). É que de acordo com as denúncias de Edward Snowden, podem ser distinguidos basicamente dois tipos de programas ou sistemas de secretos de vigilância.

O primeiro, um programa de vigilância destinado a coletar vastas quantidades de registros de ligações telefônicas, conhecido como "The Associational Tracking Program", conduzido pela NSA e outras agências de inteligência e de segurança, que ficou conhecido após a revelação, pelo jornal *The Guardian*[12], de uma decisão do tribunal FISC[13], sediado em Washington. A ordem judicial[14] em questão determinava à Verizon, uma das maiores companhias telefônicas dos EUA, que fornecesse à NSA todos registros telefônicos de ligações internas e que se originassem de fora para os EUA, durante 03 meses. A ordem se limitava a determinar a entrega dos "metadados", o que inclui apenas os números dos terminais que geraram e receberam as ligações, horário e duração das chamadas e, em se tratando de telefones celulares, os números IMSI[15] e IMEI[16]. Não incluía o conteúdo das ligações, ou seja, o teor das conversas, bem como os nomes e endereços dos usuários ou informações financeiras. Mesmo assim, já foram ajuizadas até o momento quatro ações coletivas (*class actions*), alegando a inconstitucionalidade[17] desse sistema de vigilância de chamadas

---

[10] https://prism-break.org/

[11] No dia 19 do mês de julho, uma grande coalização de entidades da sociedade civil ingressou com o que parece ser a quarta ação contra o programa de vigilância interno de registros de chamadas telefônicas. Na ação, ajuizada perante um tribunal federal da cidade de São Francisco (*Nothern District Court of California*), se requer a imediata suspensão do programa de coleta de registros de dados de ligações telefônicas. A cópia da petição inicial dessa ação pode ser encontrada em: http://www.wired.com/images_blogs/threatlevel/2013/07/effstamped.pdf .

[12] Conforme reportagem publicada no dia 06.06.13, acessível em: http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order

[13] Cópia da decisão está disponível em: http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order

[14] Publicada no site do jornal *The Guardian*, no seguinte endereço: http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order?guni=Article:in%20body%20link

[15] O **International Mobile Subscriber Identity** (**IMSI**) é usado para identificar um usuário de uma rede de telefonia móvel (celular) e é uma identificação única associada a todas as redes de telefonia celular.

[16] **International Mobile Equipment Identity** (Identificação Internacional de Equipamento Móvel), mais conhecido por **IMEI**, é um número de identificação global e único para cada telefone celular.

[17] O argumento essencial é que, ao permitir a coleta massificada dos registros telefônicos de milhões de usuários, o programa viola a 1ª., a 4ª. e a 5ª. Emendas à Constituição dos EUA, além de desrespeitar algumas leis que exigem a identificação de suspeita fundada da autoria de crime para realizar interceptação de comunicações.

telefônicas[18]. A revelação desse sistema aumentou a pressão sobre congressistas norte-americanos, que agora estão mais dispostos a aprovar emendas tendentes a restringir o alcance da *Section 215* do *Patriot Act*[19], Lei que autoriza à NSA requisitar a coleta dos registros de chamadas telefônicas[20]. A *Section 215* do *Patriot Act* permite ao tribunal secreto (*Foreign Intelligence Surveillance Court – FISC*) expedir mandados para a captura de qualquer tipo de registros "tangíveis", o que inclui registros e dados bancários, médicos e telefônicos. O Governo só necessita demonstrar que a informação é "relevante" para uma determinada investigação. O *Patriot Act* foi editado apenas seis semanas após os ataques terroristas de 11 de setembro de 2001 e, desde então, vem sendo renovado periodicamente. A prioridade para os congressistas reformistas é estreitar o escopo dessa disposição, de forma a impedir a expedição de mandados para capturar dados de forma indiscriminada, limitando a possibilidade de ordem para coleta de dados sem uma suspeita fundada de cometimento de crime por um determinado indivíduo.

O sistema que vem causando tanta indignação aos americanos é utilizado para vigilância no âmbito interno, coletando os registros telefônicos das empresas de telefonia dos EUA, daí que é um problema unicamente afeto a eles próprios. O segundo programa que também veio à tona com as denúncias de Edward Snowden, constante e em operação há alguns anos, atinge diretamente os cidadãos de outros países. Trata-se do PRISM[21], que permite coletar e analisar informação proveniente dos servidores das grandes empresas da Internet. Não se restringe a metadados, pois compreende o conteúdo das comunicações, alcançando arquivos de áudio, vídeos, fotografias e e-mails. As denúncias divulgadas (no dia 06 junho deste ano) pelos jornais *The Guardian*[22] e *Washington Post*[23] são no sentido de que 09 grandes empresas de tecnologia (Google, Microsoft, Facebook, Yahoo, Skype, Apple, Paltalk, Youtube e AOL) proporcionam um ilimitado e direto acesso da NSA aos servidores e bases de dados, como parte da execução do PRISM. Amparadas em outro texto legal – o *FISA*-Foreign *Intelligence Surveillance Act*[24], as agências de inteligência do Governo americano requisitam a instalação de "back-doors", que seriam dispositivos que permitem filtrar o fluxo de informações ou sugar os dados constantes em um sistema informático. As empresas mencionadas como colaboradoras do Governo na execução desse programa apressaram-se a negar qualquer tipo de cooperação, alegando que

---

[18] A última delas aforada por uma heterodoxa coalização de entidades, como já mencionado. Ver reportagem em: http://www.gamepolitics.com/2013/07/16/eff-files-lawsuit-against-nsa-over-associational-tracking-program#.Ue6heKwQMZY

[19] Cf. reportagem no site da NBC, do dia 23.07.13 , acessível em: http://tv.msnbc.com/2013/07/23/in-aftershock-of-leaks-reformers-take-a-stab-at-nsa-powers/

[20] A primeira tentativa de barrar a escalada do sistema de vigilância massivo da NSA, no entanto, parece ter falhado. No dia 24.07.13, a Casa dos Representantes (equivalente à Câmara dos Deputados aqui no Brasil) derrotou por uma maioria apertada (205 votos a favor e 217 contra) uma emenda que cortava fundos para o programa de coleta de registros de dados de telefones. A emenda, apresentada pelo Deputado Justin Amash (Republicado do Estado do Michigan) impedia a destinação de fundos do orçamento anual (para 2014) do Departamento de Defesa para o programa de vigilância. Segundo reportagem publicada na revista Wired, o Governo do Presidente Obama teria se empenhado em derrubar a emenda. Ver em: http://www.wired.com/threatlevel/2013/07/house-nsa-repeal-vote/

[21] Abreviatura em inglês para *Planning Tool for Ressource Integration, Synchronization and Management*.

[22] Ver notícia no jornal *The Guardian* em: http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data

[23] Ver notícia no jornal *Washington Post* em: http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

[24] Section 501, codificada como 50 U.S.C. 1861.

somente liberam informações específicas solicitadas em uma determinada requisição, após análise da legalidade da ordem recebida.

Como se observa, Edward Snowden revelou em particular a existência de dois programas de vigilância[25] do Governo dos Estados Unidos: um que compila os dados das comunicações telefônicas de milhões de americanos e outro, denominado PRISM, que vigia as comunicações eletrônicas de estrangeiros e estaria sendo executado desde 2007. A prova de que o segundo desses programas tem "estrangeiros" como alvos veio de uma declaração do Presidente Obama, que, numa tentativa de acalmar a opinião pública interna, acabou deixando entrever que as agências de inteligência americanas estariam tendo acesso aos segredos de milhões de indivíduos sem a cidadania americana, quando afirmou que o PRISM "não se aplica aos cidadãos americanos e não se aplica às pessoas nos EUA"[26].

Mesmo antes das revelações de Edward Snowden já haviam denúncias de que companhias telefônicas e de Internet cooperavam com o Governo norte-americano, espionando os usuários e repassando os dados pessoais coletados para a NSA.

Desde a era Bush que o Governo americano desenvolveu e opera projetos secretos de vigilância em massa, em estreita cooperação com as companhias telefônicas e as grandes empresas de Internet. As leis aprovadas desde então imunizam as empresas de tecnologia por cooperarem com o Governo, repassando informações para as agências de segurança e inteligência. Em 2006, o jornal *USA Today* noticiou que a Verizon, a AT&T e a Bell South, três grandes companhias de telefonia dos EUA, haviam entregue à NSA bilhões de registros sobre ligações domésticas. Segundo a reportagem, a transferência dos dados teria começado logo após os atentados terroristas de 11 de setembro de 2001. Embora limitada à entrega de "metadados", a colaboração das companhias telefônicas não teria amparo legal, pois uma outra empresa, a *Qwest*, recusara-se a cooperar, exigindo mandado judicial ou carta escrita pelo Advogado-Geral[27], conforme prevê o *Foreign Intelligence Surveillance Act* (FISA).

A revelação do sistema de vigilância gerou dezenas de ações judiciais contra as companhias de telefone. Uma delas, o caso *Hepting v. AT&T*, foi movida pela *Eletronic Frontier Foundation* contra as empresas de telefonia, em defesa dos usuários, por violação de privacidade pela colaboração com a NSA no programa de vigilância dos dados telefônicos. O processo se baseou numa prova conclusiva, o depoimento do ex-empregado da AT&T, Mark Klein, que declarou que sua antiga empresa enviava o fluxo da Internet para uma sala secreta em São Francisco, controlada pela NSA. O processo foi instaurado em janeiro de 2006, e meses depois foram ajuizadas várias outras ações contra as companhias telefônicas, após a reportagem do jornal *USA Today* confirmando a existência do esquema de vigilância das comunicações. Contudo, já depois de instruído, em julho de 2008 o Congresso aprovou a imunidade retroativa, excluindo as companhias que repassaram dados telefônicos (de seus usuários) de qualquer responsabilidade. A imunidade retroativa veio como parte do pacote legislativo conhecido como FISA Amendments Act (FAA)[28], que ampliou os poderes de vigilância

---

[25] Na verdade, os slides divulgados por Edward Snowden indicam a existência de outros programas de vigilância e análise de dados, como por exemplo o *Farview* e o *X-Keyscore*. Mas ao que tudo indica o PRISM e o programa de coleta de registros telefônicos seriam dois dos principais.

[26] O Presidente Obama afirmou (em inglês): "Now, with respect to the Internet and emails -- this does not apply to U.S. citizens and it does not apply to people living in the United States." Veja a declaração completa do Presidente em: http://www.whitehouse.gov/the-press-office/2013/06/07/statement-president

[27] Ver notícia publicada pela CNN, em 15.05.06, disponível em: http://money.cnn.com/2006/05/15/news/companies/verizon/

[28] http://www.govtrack.us/congress/bills/110/hr6304/text

eletrônica para as autoridades do Poder Executivo[29]. Até mesmo o Presidente Obama, então Senador pelo Estado de Illinois, votou a favor da norma imunizadora retroativa do FAA, num Senado de maioria democrata e que poderia ter derrotado a Lei enviada pela Administração do Presidente Bush. Obama havia dito, mais de uma vez, que tentaria obstaculizar a passagem da legislação, mas terminou votando a seu favor[30].

Na ação judicial coletiva que resultou no caso *Hepting v. AT&T* se pedia fosse suspenso o monitoramento eletrônico e condenadas as companhias a pagar bilhões de dólares pelos prejuízos causados à privacidade dos seus usuários. Os autores alegaram que o programa massivo de coleta de registros telefônicos violava a 4ª. Emenda da Constituição dos EUA, que protege os cidadãos contra buscas e apreensões desarrazoadas, bem como atentava contra o direito à privacidade. Mas, como em 2008, o Congresso aprovou uma imunidade retroativa às companhias telefônicas envolvidas no esquema de vigilância, elas ficaram livres de qualquer responsabilidade legal pelos atos de cooperação na espionagem eletrônica[31]. Por causa do *FAA*, em junho de 2009 um Juiz Federal extinguiu o processo do caso *Hepting v. AT&T* e outras doze ações movidas contra as companhias de telefonia[32]. A *Eletronic Frontier Foundation* apelou da decisão, mas ela terminou sendo confirmada na corte de apelações[33]. Ainda se tentou recurso para a Suprema Corte, sob a alegativa de inconstitucionalidade da lei que garantiu a imunidade retroativa, mas em outubro de 2012 a corte máxima resolveu não apreciar o caso[34].

Porém, nem todas as ações contra as companhias telefônicas foram arquivadas por força da imunidade legal retroativa (conferida pelo FAA). Ainda existe pendente de julgamento um processo decorrente das primeiras denúncias surgidas em 2006, sobre a vigilância massiva e despida de mandado judicial conduzida durante a Administração Bush. Trata-se do caso *Jewel v. NSA*[35], uma ação coletiva[36] (*class action*) ajuizada em favor dos usuários da AT&T perante um Juiz Federal de São Francisco, em que a *Eletronic Frontier Foundation* acusa o Governo de trabalhar em cooperação com as empresas de telecomunicações, espionando as informações dos usuários sem autorização judicial. A acusação foi baseada em documentos internos da AT&T, uma das maiores companhias telefônicas dos Estados Unidos, que revelaram a existência de uma sala secreta dessa companhia no seu escritório de São Francisco, onde se desviava o tráfego da Internet para a NSA. Os documentos teriam sido fornecidos à EFF por Mark Klein, um técnico aposentado da AT&T, que ficou em posse deles após sua aposentadoria. Os documentos estão sob sigilo judicial, porque a Corte atendeu pedido da AT&T, mas a revista *Wired* publicou[37] uma significativa porção[38] deles em maio de

---

[29] Promulgada como lei em 2008, o FAA autoriza o Advogado-Geral a requerer a extinção dos processos contra as empresas de telefonia que participaram do programa sem mandado judicial, bastando que certifique à Corte (*FISC – Foreign Intelligence Surveillance Court*) que a vigilância não ocorreu, se deu em bases legais ou foi autorizada pelo Presidente. O Advogado-Geral ingressou com a declaração em setembro de 2008.

[30] Ver notícia publicada em 14.07.08, em: http://www.politifact.com/truth-o-meter/article/2008/jul/14/obamas-wiretapping-flip-flop-yes/

[31] Ver notícia publicada pelo CNet em 29.08.08, disponível em: http://news.cnet.com/8301-13578_3-9986716-38.html

[32] Ver decisão do Juiz em: https://www.eff.org/node/68082

[33] Ver decisão da *Court of Appeal for the Ninth Circuit* em: https://www.eff.org/node/68082

[34] Ver comunicado da negativa do *writ of certiorari* em: https://www.eff.org/node/72125

[35] Ver informações sobre esse caso em: https://www.eff.org/cases/jewel

[36] Ver notícia publicada pela Wired em 13.12.13, sobre os desdobramentos do caso, acessível em: http://www.wired.com/threatlevel/2012/12/state-secrets-front-center/

[37] http://www.wired.com/science/discoveries/news/2006/05/70947

[38] http://www.wired.com/threatlevel/2007/05/mark_klein_docu/

2006. Eles descrevem como a companhia telefônica instalou "splitters" nos cabos de fibra óptica da Internet, no *hub* de São Francisco. Além de contestar a ilegalidade e constitucionalidade do monitoramento massivo, nessa ação figuram como réus a NSA e outras agências de inteligência do Governo americano e se busca responsabilizar os agentes políticos que autorizaram seu funcionamento. A medida judicial tenta responsabilizar os agentes responsáveis pela criação, autorização e implementação do programa de vigilância sem autorização judicial, incluindo o Diretor da NSA, Keith Alexander, o ex-Vice-Presidente Dick Cheney e o ex-Procurador-Geral Alberto Gonzales. É imprevisível o desfecho desse caso, mas dificilmente se terá sucesso em condenar perante uma corte americana altos funcionários do Governo.

O Presidente Obama prometeu, no início de seu primeiro mandato, restringir esses programas, mas o que se percebeu foi que durante sua administração os programas de vigilância eletrônica se expandiram. Obama prometeu inclusive rever um privilégio legal, o instituto do "state secrets privilege", que permite ao Governo encerrar processos no seu nascedouro, desde que invoque relação com assuntos de segurança nacional. O Procurador-Geral, Eric Holder, chegou a divulgar diretrizes[39] da nova Administração, que se comprometeria a restringir o uso desse instituto apenas a casos onde houvesse a possibilidade de um "prejuízo significativo para o país". Os fatos demonstraram que a promessa não foi cumprida. O Governo Obama vem se utilizando desse expediente de forma constante, tanto que tentou barrar o processo da EFF sob o argumento de que sua continuação poderia revelar segredos de Estado, mas não teve sucesso[40].

Com a revelação da abrangência do sistema de vigilância eletrônica, agora em 2013, por Edward Snowden, a situação se complicou muito para o Governo dos EUA e as grandes empresas de tecnologia, que sofrem o risco de ser processadas em outros países. Desta vez, ficou comprovado que o sistema de espionagem eletrônica tem sido utilizado para bisbilhotar a vida de cidadãos residentes em diversas partes do mundo e obter informações privilegiadas sobre negócios e segredos comerciais de empresas e dos governos de outros países. O sistema *PRISM*, diferentemente do programa de coleta dos registros (metadados) das ligações telefônicas dentro dos EUA, é focado na obtenção de dados que envolvem o conteúdo das comunicações dos "estrangeiros". Algumas das grandes empresas de tecnologia americanas têm subsidiárias e escritórios espalhados em diversos outros países, onde possivelmente poderão ser demandadas. Especialmente na Europa, os grandes gigantes da área de tecnologia americana estão mais suscetíveis de ser demandados, tendo em vista as rigorosas leis de proteção à privacidade que vigoram nos países desse continente[41].

O escândalo de espionagem também pode acarretar prejuízos tremendos na área comercial para as empresas americanas, sobretudo para o crescente segmento de *cloud computing*[42]. Os danos à imagem das empresas americanas, traduzidos na falta de confiança de seus clientes quanto à segurança e confidencialidade dos seus dados, podem resultar em perdas de bilhões de dólares[43]. Desde os anos 70, algumas das mais

---

[39] Ver notícia publicada pela Wired em 23.09.09, acessível em: http://www.wired.com/threatlevel/2009/09/state-secrets/#more-9542

[40] Ver notícia publicada pela Wired em 13.12.13, sobre os desdobramentos do caso, acessível em: http://www.wired.com/threatlevel/2012/12/state-secrets-front-center/

[41] Ver reportagem publicada no site da MIT Technology Review, em 11.06.13, acessível em: http://www.technologyreview.com/news/515956/companies-complying-with-nsas-prism-may-face-eu-lawsuits/

[42] Ver reportagem no site do jornal inglês The Guardian, de 09.08.13, acessível em: http://www.theguardian.com/technology/2013/aug/09/nsa-surveillance-apple-google-obama

[43] Ver reportagem no site do jornal inglês The Guardian, de 08.08.13, acessível em: http://www.theguardian.com/world/2013/aug/08/nsa-revelations-fears-cloud-computing

promissoras corporações americanas ascenderam no setor da tecnologia da informação. Empresas como Microsoft, Apple e Google são grandes "exportadores" de serviços e produtos (o Gmail, Skype, iCloud, o site de busca da Google etc.), que são utilizados por milhões de pessoas pelo mundo inteiro. Esses usuários agora sabem que essas empresas podem estar entregando seus dados ao Governo americano, sejam quais forem os propósitos. A desconfiança quanto à insegurança na proteção de suas informações pessoais pode fazer com que migrem para serviços e produtos equivalentes, prestados por empresas não americanas[44].

Na verdade, a revelação do escândalo de espionagem pela NSA já parece estar causando prejuízos às empresas de tecnologia norte-americanas. Segundo pesquisa realizada entre 25 de junho a 09 de julho deste ano, pela *Cloud Security Alliance*, 10% de seus associados que não são empresas americanas cancelaram contratos com algum provedor de serviços de nuvem baseado nos EUA e 56% se disseram menos propensos a usar uma companhia americana[45]. Outra pesquisa mais recente, esta realizada pela Information Technology & Innovation Foundation (ITIF)[46], estima que os fornecedores norte-americanos de serviços de *cloud computing* podem ter um prejuízo de US$ 35 bilhões até 2016. A participação de mercado das empresas norte-americanas nesse setor encolheria dos atuais 85% para 65% nesse período, em razão da perda de espaço principalmente para empresas europeias e japonesas, que "já descobriram que o sentimento anti-americano é uma oportunidade de ouro para galgar novos degraus nesse mercado emergente e preparam suas políticas de conquista de clientes"[47].

A perspectiva de que as empresas americanas de tecnologia percam bilhões de dólares em negócios e sofram ações judiciais em diversos países parece ter sido a única razão capaz de fazer o Governo americano a recuar. Na última sexta-feira (dia 09.08), o Presidente Obama prometeu uma revisão dos programas de vigilância, com o objetivo de aumentar a supervisão e transparência. O Presidente afirmou na ocasião que pedirá ao Congresso para alterar a Seção 215 do "Patriot Act" (Lei Patriótica, em tradução livre). Adiantou também que proporá mudanças no procedimento judicial do *FISC*, o tribunal secreto cuja atribuição é emitir as ordens de requisição de informações. A ideia é estabelecer um sistema adversarial, criando a figura de um advogado especializado em privacidade, que funcionaria perante o "tribunal" para se contrapor aos pedidos do Governo de requisição de informações. O Presidente disse ainda que formará um grupo de especialistas, para estudar as melhores maneiras de balancear os poderes de investigação das agências de inteligência com as preocupações com a privacidade das pessoas. Durante a conferência com a imprensa, o Presidente Obama afirmou que sua intenção sempre foi debater o assunto da vigilância com a sociedade, mas de uma maneira "ordeira e legal". Reclamou que os vazamentos repetidos feitos por Snowden tenham iniciado o debate de uma maneira emocional e não informada[48]. Ainda no

---

[44] Ver artigo publicado por Glenn Derene, no site *Popular Mechanics*, sob o seguinte título: **Why the NSA Prism Program Could Kill U.S. Tech Companies - Spying on foreigners could create a terrible blowback to the U.S. economy. Has it really come to this?.** Acessível em: http://www.popularmechanics.com/technology/military/news/why-the-nsa-prism-program-could-kill-us-tech-companies-15564220

[45] Segundo reportagem no jornal *The Times of India*, de 25.07.13, acessível em: http://timesofindia.indiatimes.com/tech/tech-news/internet/US-surveillance-programme-hurting-US-tech-cos/articleshow/21327806.cms?

[46] www.itif.org/

[47] Ver notícia publicada no site *Convergência Digital*, em 16.08.13. Acessível em: http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=34588&sid=97#.UhFbTn__jD8

[48] Ver notícia em: http://www.npr.org/blogs/thetwo-way/2013/08/09/210539942/live-blog-president-obamas-press-conference

mesmo dia, o Governo divulgou documento[49] contendo as razões em que sustentam a legalidade e constitucionalidade do programa de coleta de metadados das chamadas telefônicas[50].

Antes do escândalo Snowden, cada vez mais o Governo vinha aumentando o seu aparato de vigilância cibernética, incentivando a troca de informações entre as agências do governo e as companhias privadas, bem como imunizando as empresas de qualquer responsabilidade civil ou criminal por eventual uso ilegal posteriormente feito com informações transferidas. Se no começo desta década a justificativa para o aumento do aparato de vigilância era a luta contra o terrorismo, nos últimos anos passou a ser o enfrentamento da "ciberwar" (a guerra cibernética, hoje travada especialmente contra a China)[51].

Tudo leva a crer que o Presidente Obama tomou a decisão de reformar as leis e os procedimentos de vigilância eletrônica depois de reunir-se com executivos das grandes empresas de TI e dirigentes de entidades defensoras das liberdades civis. Pelo menos duas reuniões foram realizadas na Casa Branca[52] na última semana com esses grupos, uma delas liderada pelo próprio Presidente. Estiveram presentes o presidente executivo da *Apple*, Tim Cook; o vice-presidente da *Google*, Vint Cerf; e o presidente executivo da *AT&T*, Randall Stephenson. Ainda se fizeram presentes representantes da associação *TechAmerica*, que defende interesses de empresas como *Google*, *Facebook*, *Microsoft* e *Yahoo*, entre outras. Além dos representantes do setor empresarial, foram também convidados os líderes da União Americana das Liberdades Cívicas (*ACLU-American Civil Liberties Union*)[53], do Centro para a Democracia e Tecnologia (*CDT-Center for Democracy and Technology*)[54] e do Centro para Privacidade da Informação Eletrônica (*EPIC-Eletronic Privacy Information Center*)[55].

As reuniões foram marcadas com o propósito de discutir os programas de vigilância, mas não foi divulgado exatamente o teor das conversas. Tudo indica, no entanto, que os presentes delinearam um quadro bem desfavorável aos interesses americanos, pois no dia seguinte o Presidente Obama anunciou a reforma. O Governo vinha dando mostras de não querer deixar de manter o sistema de vigilância funcionando nos mesmos moldes. O Presidente só havia dado poucas explicações, em eventos públicos dos quais participara, dizendo que os programas só recolhiam "metadados" e que não tinham como alvos cidadãos norte-americanos. O Governo inclusive havia revigorado a ordem para que a Verizon continue a fornecer os dados das ligações telefônicas[56] e, poucos dias antes, divulgado um programa de incentivo para as empresas que colaborassem com os pedidos de informações vindos das agências de inteligência[57]. Parece que as reuniões levaram o Governo a mudar de postura em relação

---

[49] http://s3.documentcloud.org/documents/750210/administration-white-paper-section-215.pdf

[50] Trata-se do programa de vigilância doméstica de chamadas telefônicas, distinto portanto do PRISM. A base legal desse programa reside na Seção 215 do *Patriot Act*.

[51] Ver artigo de nossa autoria publicado no site *Consultor Jurídico*, em 06 de junho deste ano, sob o título "EUA debatem quebra de sigilo virtual sem ordem judicial". Acessível em: http://www.conjur.com.br/2013-jun-06/democrito-filho-eua-debatem-quebra-sigilo-virtual-ordem-justica

[52] Ver notícia no site português *Público*, de 09.08.13, disponível em: http://www.publico.pt/mundo/noticia/obama-discute-vigilancia-e-privacidade-com-presidentes-da-apple-e-att-1602672

[53] http://www.aclu.org/

[54] https://www.cdt.org/

[55] http://epic.org/

[56] Ver notícia em: http://www.pcworld.com/article/2044883/us-court-renews-permission-to-nsa-to-collect-phone-metadata.html

[57] Ver notícia do dia 07.08, em: http://biztechreport.co.uk/2013/08/us-government-offers-cybersecurity-rewards-to-businesses/

ao enfrentamento da crise originada com a revelação dos sistemas de vigilância eletrônica massiva. De uma posição inicial que beirava um quase completo desdém, o Governo passou a dar satisfações à sociedade, na forma de promessas de mudanças no funcionamento dos programas de vigilância. Os executivos devem ter feito Obama e seus assessores enxergarem com maior nitidez o potencial prejuízo para os interesses comerciais das grandes empresas de tecnologia. O último desses encontros foi na quinta, dia 08 de agosto. Logo no dia seguinte, numa reunião com a imprensa na Casa Branca, o Presidente anunciou a reforma dos programas de vigilância.

Não se sabe exatamente o que essa iniciativa do Governo terá sobre a opinião pública americana, que está dividida quanto aos benefícios sociais dos programas de vigilância eletrônica – boa parte da população acha que os órgãos governamentais têm cometido abusos. O fato é que ela representa visível reviravolta no modo como a Administração Obama vinha lidando com os desdobramentos da crise causada com as denúncias de Edward Snowden. Reportagem do jornal Wall Street Journal[58] afirma que especialmente para a pessoa do Presidente a mudança de rumos representa uma significativa "about-face" política, quase que uma espécie de *mea culpa*, sabendo-se que ele, enquanto Senador, era um dos principais críticos dos programas de vigilância. No ano de 2005, junto com outros senadores, assinou um manifesto expressando preocupações com a possibilidade de o Governo (na época, do Presidente Bush) estar cometendo abusos na interpretação e aplicação da Seção 215 do "Patriot Act". Naquela época, Obama argumentava que essa norma daria margem à "fishing expeditions" tendo como alvo americanos inocentes. Já como Presidente, nos meses em que se seguiram ao estouro do caso Snowden, o Presidente defendeu a continuidade dos programas de vigilância como instrumentos adequados para combater o terrorismo e proteger o povo americano. Talvez a mudança de posicionamento tenha sido puro pragmatismo político. O jornalista Glenn Greenwald, que vem fazendo as reportagens sobre os vazamentos de Edward Snowden, já deixou entrever que ele ainda tem denúncias adicionais a fazer sobre os programas de vigilância[59]. Por outro lado, além das preocupações com os interesses comerciais das grandes empresas de tecnologia, o Presidente vinha sofrendo pressão de grupos ligados à defesa das liberdades civis e de parlamentares do seu próprio partido, que já haviam proposto projetos para reforma das leis de vigilância nacionais[60].

A conclusão que fica: a iniciativa das empresas de tecnologia em enviar cartas às autoridades governamentais[61], solicitando um pouco mais de transparência a respeito

---

[58] Do dia 09.08.13, acessível em: http://online.wsj.com/article/SB10001424127887324522504579002653564348842.html

[59] Foi o que disse Glenn Greenwald perante a Comissão de Relações Exteriores do Senado Federal, em audiência no dia 06.08.13. Ver em: http://www12.senado.gov.br/noticias/materias/2013/08/06/jornalista-americano-diz-que-ainda-ha-muito-a-ser-revalado-sobre-espionagem

[60] Não é de se imaginar no Congresso americano qualquer iniciativa legislativa no sentido de suspender por completo os programas de vigilância, mas no começo deste mês, o Sen. Al Franken apresentou um projeto de lei, intitulado Surveillance Transparency Act of 2013. Um dia depois, na Casa dos Representantes (*House of Representatives*, o equivalente à nossa Câmara dos Deputados), uma coalizão de partidos liderada pela Deputada Zoe Logfren, apresentou projeto semelhante – o *Surveillance Order Reporting Act*. Ambos os projetos procuram atribuir maior transparência aos programas de vigilância, autorizando as empresas a divulgar estatísticas gerais sobre a quantidade e tipo de pedidos de informações que recebem de parte de órgãos governamentais, bem como exigindo a publicação, pelo Governo, de relatórios regulares sobre as atividades de vigilância de dados.

[61] As empresas subscritoras das cartas apenas requerem que informações básicas sobre as requisições sejam reveladas ao público, a exemplo do número de ordens que recebem e quais são as autoridades que as expedem. Nem poderia ser diferente, porque o Governo jamais aceitaria – pelas mesmas e sempre

das ordens que recebem, bem como a anunciada revisão do programa de captura de registros de telefonia podem ter algum significado para acalmar os cidadãos americanos, mas nenhum efeito imunizador terá em relação às atividades de coleta de dados de cidadãos de outras nacionalidades. Não conseguirão evitar o prejuízo à imagem e a perda da confiança de seus usuários pela invasão da privacidade, ao cooperarem para capturar dados pessoais de indivíduos residentes em diversas partes do globo terrestre. O jornalista Glenn Greenwald reafirmou recentemente que o Governo dos EUA monitora comunicações eletrônicas dentro e fora do país, com a justificativa de combater o terrorismo e garantir a segurança nacional, mas na realidade, o objetivo seria obter informações privilegiadas sobre acordos econômicos, estratégias políticas e competitividade industrial de outros países[62].

Recife, 12.08.13

alegadas razões de segurança nacional – divulgar um completo relatório sobre a extensão e escopo das requisições feitas às empresas de tecnologia. Por isso, elas se limitam a buscar autorização para revelar apenas informações estatísticas sobre as requisições que recebem do Governo.

[62] Foi o que disse Glenn Greenwald perante a Comissão de Relações Exteriores do Senado Federal, em audiência no dia 06.08.13. Ver em: http://www12.senado.gov.br/noticias/materias/2013/08/06/jornalista-americano-diz-que-ainda-ha-muito-a-ser-revalado-sobre-espionagem