CENTRO DE PESQUISAS ESTRATÉGICAS PAULINO SOARES DE SOUSA
Universidade Federal de Juiz de Fora
www.ecsbdefesa.com.br

A espionagem no ciberespaço: só o governo brasileiro não sabia?

Claudio Mano
Bacharel em Filosofia pela UFJF
Membro do Centro de Pesquisas Estratégicas "Paulino Soares de Souza" da UFJF
cmpostal@gmail.com

Em artigo de março de 2012, publicado no *site* Wired[1], James Bamford nos apresenta o novo endereço de alguém antes residente nas empoeiradas páginas do memorável – e assustador – livro *1984*, de George Orwell: O Grande Irmão. No romance ficcional de Orwell, uma crítica contundente aos modelos totalitários de governo, o Estado – Grande Irmão – mantém vigilância absoluta e permanente sobre todos os indivíduos, mesmo quando na intimidade de seus lares. Ambientada no ano de 1984, a previsão dessa trama tragicamente vem a se confirmar com cerca de trinta anos de atraso. A seguir, antes de voltarmos nossa atenção às possíveis implicações, para nós brasileiros, do tema que trata o artigo citado, acompanhemos um pouco de seu relato, de modo a vislumbrar os contornos dessa moradia real, destinada a abrigar uma figura tenebrosamente abstrata.

Bramford começa nos sugerindo que, o estado de Utah, nos Estados Unidos da América, parece predestinado a acolher pioneiros. Primeiro, em meio ao século XIX, buscando um local onde pudessem professar em paz sua religião, chegaram os Mórmons. Agora, em pleno século XXI, estes recebem em sua proximidade uma nova estirpe de crentes que, como eles, lá também pretendem erguer seu local de culto. Mas "Ao invés de Bíblias, profetas e adorações, este templo estará repleto de servidores de rede, especialistas em

[1] BAMFORD James, *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)*, http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1, em 28/09/2013.

inteligência artificial e guardas armados. Ao invés de ouvir os preceitos sussurrados por Deus, os recém chegados irão capturar, armazenar e analisar imensas quantidades de palavras e imagens oriundos da intrincada rede de tele-comunicações mundial. Na pacata cidade de Bluffdale, os irmãos no Amor e o 'Grande Irmão', tornam-se antagônicos vizinhos".

Segundo Bamford, previsto para estar plenamente operacional justamente agora, em setembro de 2013, o "Centro de Dados de Utah", construído pela NSA (*National Security Agency's*), tem um custo estimado na ordem de 2 bilhões de dólares. Somente o valor da conta de consumo de energia elétrica necessária para alimentar esse voraz aspirador de dados, é estimada em 40 milhões de dólares ao ano. Sob seu monitoramento "estarão todas as formas de comunicação, incluindo o conteúdo completo de *emails*, telefonia celular e pesquisas ao Google, assim como todos os tipos de rastro deixados por transações pessoais – pagamento de estacionamentos, itinerário de viagens, compras de livros e outros –. Em certa medida, é a realização do programa de 'conhecimento total da informação', criado durante o primeiro mandato da administração Bush, um esforço detido pelo congresso em 2003 após causar clamor em função de seu potencial de invasão à privacidade dos Americanos".

Mas Bamford observa que agora, muito mais que "uma central de dados", o "centro ganha um novo, mais secreto e importante papel não revelado até o momento", sua capacidade "para decifrar códigos", pois informações sensíveis, notadamente as financeiras, militares e diplomáticas, via de regra são objeto de fortes esquemas de proteção[2]. "Segundo um outro alto oficial envolvido nesse programa, a NSA fez um enorme avanço já alguns anos, em sua habilidade de análise criptográfica, ou de decifrar os mais sofisticados esquemas de criptografia, usados não apenas por governos em todo o mundo, mas também pelos usuários de computador nos Estados Unidos. (…) 'todos são um alvo, qualquer um que utiliza comunicação é um alvo'".

Em seu artigo, Bamford também assinala a opção adotada pela assimilação total do fluxo de dados ao invés de uma captura seletiva. Assim, além de promover investigações em tempo real, uma vez armazenadas, todas informações são passiveis de toda sorte de análises. Ou seja, não são apenas aqueles indivíduos ou instituições de alguma forma suspeitos de atividades danosas aos interesses dos Estados Unidos da América que estão sob vigilância, mas sim o mundo todo. Uma vez que os cérebros eletrônicos encarregados de farejar por suspeitas nos enquadrem em seus padrões de busca, qualquer um de nós pode ser considerado uma ameaça. Nesse ponto, vale ressaltar, que não são apenas os Estados Unidos da América

[2] Ver também http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all&_r=0 em 28/09/2013

que detêm essa tecnologia e desenvolve esse tipo de atividade. França[3] e Reino Unido[4] possuem centros de monitoração de informações com características similares e certamente também, outros países.

Quem assistiu ao filme *Minority Report*, dirigido por Spielberg e estrelado por Tom Cruise, certamente perceberá uma sombria semelhança entre o enredo cinematográfico e o que estamos tratando. Na ficção de Spielberg, que se passa em Washington no ano de 2054, existe um centro de informações capaz de antecipar todas as ações criminosas. Desse modo, as forças de segurança podem surpreender o meliante antes mesmo que o crime seja consumado. Isso nos leva a propor a seguinte situação hipotética[5]: considerando que os autores do pérfido atentado de Boston utilizaram uma panela de pressão para confeccionar seu artefato explosivo e uma mochila para ocultá-lo enquanto se deslocavam pela cidade, pode ser que, ao comprar uma panela de pressão para sua esposa e pagá-la com cartão de crédito e a seguir solicitar pela Internet uma mochila para seu filho, ao chegar em casa ao final do dia você se depare com uma força tarefa em sua sala. Será esse exemplo exagerado?

De qualquer forma, o objeto deste texto não é a espionagem em si, mas sim o fato de que não é novidade o poder de monitoração e interferência nas redes de comunicação mundial pelas grandes potências, ou mesmo por grandes grupos financeiros e industriais. Sob esse ponto de vista, e dado o fato que o Estado brasileiro dispõem de agências de informação, como a Abin, é preocupante, se verdade, que a Presidente da republica somente tomou ciência da invasão de suas mensagens eletrônicas graças ao esforço jornalístico da Rede Globo de televisão. Por outro lado, em uma entrevista em Washington, após queixar-se diante da assembléia da ONU sobre a invasão de privacidade nas comunicações eletrônicas, a Presidente Dilma Rousseff manifestou-se surpresa pelo fato do governo dos Estados Unidos ter dado acesso a Edward Snowden, o pivô do vazamento dos detalhes sórdidos das atividades de espionagem nas redes de comunicação, às informações críticas sobre uma nação estrangeira amiga, uma vez que Snowden se encontrava no cargo apenas a quatro meses[6]. Ora, a fala da Presidente pode levar a entender que o maior problema foi a indiscrição ter chegado ao conhecimento público e não o fato em si: o monitoramento que ocorre diuturnamente.

---

[3]http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html em 28/09/2013

[4]http://www.lemonde.fr/europe/article/2013/06/21/les-services-secrets-britanniques-espionnent-internet-par-les-fibres-optiques_3434693_3214.html em 28/09/2013

[5]Baseado em notícia vinculada em blog do Le Monde: http://bigbrowser.blog.lemonde.fr/2013/08/02/boom-de-la-lutte-antiterroriste-contre-les-cocotte-minute-et-les-sacs-a-dos/ em 28/09-2013

[6] http://oglobo.globo.com/mundo/dilma-diz-que-parceria-esta-nas-maos-do-governo-obama-10144376 em 28/09/2013

A intromissão e interferência nas telecomunicações, acreditamos, estão aí para ficar. Pouco importa que leis sejam estabelecidas para tentar refrear essa tendência, pois afinal, o meio eletromagnético é fluido e acessível a todos. Se essa prática implica em uma invasão de privacidade incompatível com a preservação dos direitos individuais que a democracia da América do Norte preconiza, tal como herdada de seus sábios pais fundadores e gravada com zelo cívico em sua pioneira constituição, isso certamente será objeto de acaloradas discussões futuras. Na América do Norte, talvez até na comunidade européia, mas certamente fora da influência daqueles que, desprovidos de força política, tecnológica e militar, se encontram alhures.

Para enfrentar essa bisbilhotice, cabe a cada um, e em especial aos governos, tomar as medidas tecnológicas necessárias para manter a privacidade de suas comunicações em níveis compatíveis com a segurança que seus dados exigem. Vale notar que além das mensagens de correio eletrônico, trafegam pela Internet, no caso brasileiro, as declarações de imposto de renda, os acessos às bases de dados da justiça, da polícia, das forças armadas, quiçá até o conteúdo das urnas eletrônicas nos períodos eleitorais. Enfim, pode ser que a intimidade de nossas vidas seja para alguém efetivamente um livro aberto. Nesse caso, mais que uma violência à privacidade de cada um e por conseguinte, à nossa dignidade enquanto seres humanos, ao expor as entranhas do governo, represente efetivamente um problema de segurança nacional. Coincidência ou não, com o incidente presidencial, o fato é que a Abin tem entrado em contato com universidades federais no intuito de promover uma maior segurança em relação aos dados confidenciais das pesquisas em desenvolvimento[7].

Em artigo publicado[8] em agosto de 2012, já alertávamos para a imprudência de prover compulsoriamente a frota nacional de veículos com dispositivo rastreador que permitiria o bloqueio de cada um – ou de todos – a partir de uma central de controle, usando-se como meio de acesso a rede de telefonia celular. Hoje, convidamos o leitor a refletir sobre o risco que as informações armazenadas em cada computador no Brasil, que utilize um sistema operacional de fabricante estrangeiro, efetivamente correm de ser inspecionadas, copiadas, ou mesmo adulteradas. É razoável supor o irresistível poder de convencimento da NSA junto aos fabricantes de software americanos[9], provedores de telecomunicações e afins, ainda mais se o

[7] http://www.ufjf.br/secom/2013/09/27/ufjf-firma-parceria-com-agencia-brasileira-de-inteligencia-para-difundir-protecao-intelectual/ em 28/09/2013

[8] MANO Claudio, *Pode uma lei de trânsito vir a comprometer a segurança nacional?* http://www.ecsbdefesa.com.br/defesa/fts/LTSF.pdf em 30/08/2012

[9] http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data em 29/09/2013
ver também: http://www.nytimes.com/2013/10/03/us/snowdens-e-mail-provider-discusses-pressure-from-fbi-to-disclose-data.html?hp&_r=0 em 03/10/2013

argumento utilizado for o da segurança nacional da América do Norte. Daí, com quem o seu computador conversa, após estar conectado na rede mundial de computadores, passa a ser uma incógnita. Até que ponto aquele programa anti-vírus que você acabou de adquirir estará "disposto" a identificar códigos indevidos introduzidos em seu computador pelo governo do país em que a empresa que o confeccionou tem sua matriz?

Para concluir, já que adentramos o reino das especulações, por que a aeronave militar de última geração, ou mesmo o carro de combate mais sofisticado adquirido por nosso governo no exterior, quando em combate, não se recusará a engajar alvos que ostentem as cores da nação que os produziu ou de seus aliados, ou mesmo que fira seus interesses comerciais? Hoje, entre o acionamento do gatinho e o disparo do armamento, existe toda uma parafernália eletrônica que pode ser suscetível a monitoramento e interferência. Em nosso entendimento, a única defesa possível contra a intromissão e dominação tecnológica estrangeira, é o desenvolvimento de tecnologia genuinamente nacional.

Nesse aspecto, é lamentável que o Brasil até hoje não tenha conseguido consolidar uma industria automobilística nacional. Nosso mercado é explorado exclusivamente por firmas estrangeiras. Existe, em funcionamento comercial no Brasil, algum computador cujo projeto e realização se sustente inteiramente em tecnologia nacional? Isso sem falar que ao abrirmos nosso segmento de telecomunicação à tecnologia e interesses estrangeiros, perdemos uma oportunidade única de obter um expressivo volume de recursos financeiros para o desenvolvimento de uma tecnologia própria, desde o projeto e manufatura dos circuitos eletrônicos até a concepção e execução dos softwares.

É importante ficar claro que não estamos defendendo ou propondo uma postura nacionalista irracional e xenófoba em relação às outras nações. No que concerne ao ambiente comercial, certamente existe espaço para todos. Pretendemos apenas deixar clara nossa impressão que, no que tange às tecnologias, nem sempre o mais barato, mais rápido ou eficiente é o mais interessante para o progresso de uma nação no longo prazo. Vale notar, que via de regra, todas as nações protegem de alguma forma as inovações tecnológicas que nascem em seu solo, principalmente quando consideradas estratégicas, o que nos faz pensar se nada poderia ter sido feito para evitar a falência da ENGESA em 1993.

Desejamos que os jovens que saem de nossas universidades, não tornem-se apenas os apertadores de botões e usuários de programas aplicativos, mas sim projetistas de equipamentos e senhores da alma cibernética que lhes dá vida. Quem sabe se à medida em

que forem sendo revelados aspectos mais detalhados da vigilância eletrônica da qual somos vítimas, fique patente que nos faltam recursos tecnológicos próprios para enfrentá-la em pé de igualdade. Mas se for assim, talvez seja de bom tom, antes de qualquer outra medida, refletirmos o porquê de nos encontrarmos nessa situação, sob o risco de mais uma vez vermos uma oportunidade perdida.