

09/07/2013 - Obtenção de dados sem Big Brother, por Leonard H Schrank e Juan C. Zarate

(O Estado de S. Paulo) Diante das revelações sobre os programas de monitoramento de telefones e e-mails pela Agência de Segurança Nacional dos EUA (NSA), o presidente Barack Obama admitiu ser imperativo equilibrar segurança e privacidade. Mas até agora a defesa por parte do governo desses programas não tranquilizou a sociedade no sentido de que tal equilíbrio foi alcançado, ou que o direito básico de privacidade e as liberdades civis estão sendo protegidos.

Agora que os programas de monitoramento foram vazados, os americanos têm de decidir como deve ser este equilíbrio. Como criar um programa que permita à comunidade de inteligência usar dados importantes e complexos e as mais modernas tecnologias para impedir ataques terroristas e ao mesmo tempo não criar um Estado Big Brother? Em outras palavras, como podemos confiar, mas também inspecionar? Os EUA sabem, pois fizeram isso antes.

Em 2006, The New York Times revelou a existência de um programa confidencial chamado Terrorist Finance Tracking Program, ou T.F.T.P., desenvolvido e supervisionado pelo Tesouro dos EUA. O programa é operado pelo Departamento do Tesouro que usa informações que lhe são fornecidas sob intimação pela Sociedade para Telecomunicações Financeiras Interbancárias Globais (Swift, em inglês). É um sistema de mensagem financeira global criado e de propriedade do setor bancário e tem sede em Bruxelas. São mensagens financeiras transmitidas envolvendo a maior parte dos bancos do mundo. Os dados enviados pelo Swift indicam quem está transferindo dinheiro, quanto e para quem, e contém informações específicas, com identificação dos envolvidos na operação. Logo após os atentados do 11 de Setembro o Tesouro passou a receber por meio de ordem judicial do Swift de maneira a permitir aos analistas do governo rastreamento o movimento de fundos em mãos de terroristas.

O sistema Swift não inclui contas bancárias particulares. Mas se um financiador terrorista em um país enviar recursos para um terrorista em outro país, a operação constará dos dados transmitidos pelo Swift. Os nomes do emitente e do favorecido e informações sobre a conta bancária também serão inseridos na mensagem.

Desde o início a proteção das liberdades civis e da privacidade do indivíduo foram consideradas fundamentais para o programa. Ao contrário da NSA, nós entendemos que ele eventualmente seria submetido a um escrutínio público, nos EUA e no exterior.

Em razão da importância e ao sigilo dos dados, para uso dos dados do Swift foi exigido que o acesso dos dados pelo governo fosse direcionado e limitado, impedindo uma ampla garimpagem de dados, mas permitindo buscas e análises concentradas num alvo para impedir ataques terroristas. Buscas com outra finalidade eram proibidas.

Tanto o Tesouro quanto o Swift asseguraram que as restrições com relação às informações obtidas usadas pelos analistas fossem estritamente atendidas. Auditores externos contratados pelo Swift confirmavam o alcance limitado do uso das informações e os próprios representantes do Swift tinham autoridade para impedir o acesso aos dados se houvesse alguma preocupação de que as restrições estabelecidas não estavam sendo atendidas. Esses monitores independentes trabalhavam in loco nas agências do governo e tinham acesso em tempo real ao sistema. Cada vez que um analista consultava o sistema o “escrutinador” podia imediatamente examinar a demanda. E cada consulta tinha de conter um motivo em anexo justificando o pedido como assunto envolvendo contraterrorismo. Com o tempo o escopo dos dados requisitados e retidos foi reduzido.

O que confirmou que a informação era usada da maneira como dissemos - para salvar vidas.

Quando políticos e defensores europeus da privacidade de dados se opuseram ao programa, o influente juiz francês Jean-Louis Burguière foi designado pelo Parlamento Europeu para reexaminá-lo. Burguière apresentou um relatório em 2008 e outro em 2010, confirmando que o

Tesouro cumprira com as exigências de proteção das liberdades civis.

O programa foi também bastante eficaz. As informações financeiras fornecidas ajudaram a frustrar ataques terroristas nos EUA, Alemanha, Espanha e Grã-Bretanha. Informações recolhidas dos bancos de dados do Swift forneceram milhares de pistas, incluindo algumas que levaram à captura do principal representante da Al-Qaeda no Sudeste Asiático e à descoberta de uma rede de financiamento de atividades terroristas em Nova York e no Paquistão.

O uso dos dados foi legal, limitado, direcionado, supervisionado e inspecionado. O programa estabeleceu um padrão ouro sobre como proteger dados confidenciais fornecidos para o governo. O Tesouro teve acesso legal a grandes volumes de dados envolvendo mensagens financeiras do Swift (o equivalente bancário dos metadados telefônicos) e conseqüentemente esclareceu isso para a sociedade dentro do país e no exterior.

Esse programa pode ser um modelo com o objetivo de limitar o uso pelo governo de grandes volumes de dados num mundo em que o acesso à informação é necessário para nossa segurança e ao mesmo tempo é preciso proteger a privacidade e as liberdades do indivíduo.

Para dar aos cidadãos americanos a confiança de que sua privacidade não está sendo violada, o governo precisa provar que os programas estão sujeitos a um monitoramento adequado e as restrições quanto ao uso dos dados da NSA estão sendo respeitadas. As empresas privadas afetadas devem ser informadas sobre como seus dados estão sendo usados e devem ter direito de se expressar sobre a maneira como os programas são estruturados, restringidos e protegidos. É possível que o governo já esteja cumprindo parte disso, mas deve informar às pessoas.

Basicamente, o governo Obama necessita demonstrar que os programas não são apenas importantes e legais, mas também que o uso pelo governo dos dados é restrito e submetido a uma inspeção. / TRADUÇÃO DE TEREZINHA MARTINO

Acesse o PDF: [Obtenção de dados sem Big Brother \(O Estado de S. Paulo,](#)

reprodução do The New York Times - 09/07/2013)