# Com programa de vigilância, EUA querem ter o maior banco de dados do mundo

12/06/2013

Figura central no escândalo de violação da privacidade e vigilância do governo Obama, PRISM é o codinome que a Agência Nacional de Segurança dos EUA (NSA) deu a seu programa clandestino de coleta de dados de cidadãos de todo o mundo. Não é um *software*, nem é, oficialmente, um programa de grampeamento de comunicações por meio de telefones, e-mails, redes sociais ou programas como o Skype, por exemplo. É um programa de vigilância da internet, que faz parte da ambição da NSA de criar o maior banco de dados de habitantes do mundo. Uma vez que os serviços de inteligência dos EUA e do Reino Unido identificam um "suspeito", basta uma consulta ao banco de dados para obter informações sobre todos os seus contatos e colocar todos os "suspeitos" sob investigação.

O objetivo da NSA com o PRISM e outras iniciativas similares é o de colher metadados de milhões de pessoas no mundo, para ajudar no desmonte de grupos "terroristas" ou de "inimigos dos EUA", sempre que necessário. Metadados incluem nomes das pessoas que se comunicam e suas localizações, números de telefones de quem faz e recebe ligações e endereços de IP (para futuras investigações de computadores pessoais).

Nessa fase, os órgãos de inteligência não têm interesse no conteúdo das comunicações. Bastam os metadados, que servem como pontos que precisam ser ligados para se começar a desenvolver as investigações iniciais. Se os órgãos de segurança conseguirem construir um caso, em que há razoável suspeita de atentado contra os EUA, com informações suficientes para convencer um juiz, o processo passa para a segunda fase, a de obter conteúdo das comunicações.

Aí começam as discussões do que precisa e do que não precisa de mandado judicial. O governo americano interpreta que a coleta de metadados pode ser feita com uma simples intimação às empresas de Internet, emitida pelo próprio Executivo, como funciona na Inglaterra. Nos EUA, isso estaria em conformidade com a Lei de Vigilância de Inteligência Estrangeira (FISA – *Foreign Intelligence Surveillance Act*), que é filha do Patriot Act.

No caso da obtenção de metadados das companhias de telecomunicações, os órgãos de segurança americanos têm conseguido ordens judiciais de um "tribunal secreto". Para operações de obtenção de conteúdo ou de quebra de sigilo, como grampeamento de comunicações por telefone, *e-mails*, bate-papos, redes sociais e GPS, os órgãos de segurança têm, teoricamente, de obter mandado judicial para fazer "buscas e apreensões", na forma protegida pela Constituição.

As notícias do fim de semana, publicadas pelo *The Guardian* e pelo *Washington Post*, informaram que a NSA e o FBI obtêm metadados de nove empresas: Google, Yahoo!, Microsoft, Facebook, Apple, AOL, PalTalk, Skype e YouTube. Mas, para os jornais, é óbvio que a coleta de dados não se restringe a essas marcas, porque a maior parte do tráfego da Internet passa pelos

EUA e são facilmente acessados pelos órgãos de segurança. Um segundo programa da NSA, o UPSTREAM, permite aos órgãos de segurança coletar dados diretamente dos cabos de fibra óptica, que interligam toda a rede de computadores do país. Isso garante ao país uma capacidade quase ilimitada de espionagem.

Além da Internet e das telecomunicações, os órgãos de segurança têm capacidade para vasculhar contas de cartão de crédito, contas bancárias e qualquer meio de movimentação de dinheiro, que possa estar relacionada com atividades terroristas ou criminosas, como financiamento de grupos suspeitos ou compra de material para fabricação de bombas ou qualquer outro artefato.

**Capacidade do software**
No caso das provedoras de serviços de Internet, a NSA usa preferencialmente, segundo os jornais, a máquina Narusinsight, equipada com um software chamado *Narusinsight Intercept Suite*. Um única máquina pode monitorar o tráfego combinado de milhões de usuários de banda larga. De acordo com a Narus, esse é "o único sistema de inteligência de tráfego de rede do setor que dá suporte à captura, em tempo real, de tráfegos de *webmail*, como o Gmail da Google, o Hotmail da MSN e o Mail da Yahoo!". No entanto, como a maioria do tráfego de *webmail*, atualmente, é feito através de HTTPS criptografado, o conteúdo das mensagens só pode ser monitorado com o consentimento das provedoras de serviço.

A empresa Narus foi fundada por dois israelenses em 1997 e, posteriormente, comprada pela Boeing. Seu software de monitoramento e análise de tráfego em tempo real tem capacidade de "classe empresarial" de spyware (um programa espião, capaz de coletar secretamente informações de usuários de computadores. Tem capacidade para vigilância em larga escala, incluindo de redes complexas de IP (como a Internet). Com desempenho de processamento de pacotes em alta velocidade, pode vasculhar vastas quantidades de informações que viajam pela Internet.

Com recursos de "normalização, correlação, agregação e análise", o programa fornece um modelo de usuário, elemento, protocolo, aplicação e comportamento da rede, em tempo real. Isto é, ele pode rastrear um usuário individual, monitorar que aplicativos está usando (como navegador, aplicativo de mensagens, e-mail) e o que está fazendo com esse aplicativo (por exemplo, sites que visitou, o que escreveu nos e-mails ou nas mensagens de IM), além de conectar usuários uns com os outros, não apenas pelos sites que visitam, mas também pelas palavras ou frases que usam em suas comunicações. O programa também pode reproduzir vídeos transmitidos por *streaming*, interpretar páginas de sites, examinar e-mails e seus arquivos anexados, além de protocolos de transferência de arquivos.

É uma versão moderna do Echelon, que foi bastante utilizado por países de língua inglesa (EUA, Reino Unido, Canadá, Austrália e Nova Zelândia) no princípio dos anos 60, nos tempos da Guerra Fria contra a União Soviética. O programa possibilitava a interceptação de comunicações feitas por satélite e por rádio a longas distâncias. Mas evoluiu para interceptação de comunicações por micro-ondas, celular e fibra óptica. Em 2006, 99% de todas do tráfego mundial de voz e de dados era feito por fibra óptica. Ainda pode interceptar comunicações por telefone, fax e tráfego de dados feitas por satélite. Os Estados Unidos foram acusados, nos anos 90, de usar o Echelon para espionagem industrial, em vez de militar e diplomática. Em 2000 e

2011, o software foi investigado por um comitê do Parlamento Europeu.

Fonte: https://conjur.jumps.com.br/2013-jun-12/programa-vigilancia-eua-maior-banco-dados-mundo/