

INVASÃO DE PRIVACIDADE

Marcio Aith

Folha de S. Paulo, 7.10.01

Para um grupo de parlamentares e as entidades protetoras de liberdades civis, o pacote antiterrorismo proposto pelo governo dos EUA expande exageradamente o poder de vigilância do Estado sobre cidadãos e instala, dentro de cada lar, uma autoridade onipresente similar à do Big Brother (Grande Irmão), personagem imaginado por George Orwell em sua obra "1984".

Curiosamente, pesquisas de opinião indicam um apoio maciço da população à maioria dessas medidas, uma resposta aos atentados que mataram cerca de 6.000 pessoas em Nova York e no Pentágono (leia na página A-19).

Para se proteger, norte-americanos mostram-se dispostos a jogar no lixo conquistas históricas que fazem parte do "american way of life" e formaram a base central da democracia de pesos e contrapesos do país. Ao menos no plano teórico, os Estados Unidos aceitam pagar, com um pedaço de sua privacidade, o preço para livrarem-se do terrorismo.

No entanto, um estudo mais atento sobre esse debate revela desafios mais complexos que o dilema liberdade versus segurança e expõe fortes interesses econômicos e o uso intenso de retóricas, oficiais e não-oficiais.

Esse debate já era intenso e tinha impacto na vida das pessoas antes mesmo dos atentados do último dia 11 de setembro. Com os atentados, os EUA acordaram para o assunto.

Mais vigilância

No ano passado, a Prefeitura de Jersey City, cidade com uma comunidade islâmica numerosa e de onde terroristas planejaram o atentado de 1993 ao World Trade Center, instalou câmaras de vídeo em quase todas as ruas do centro. Alguns moradores sentiram sua privacidade atingida.

Em Tampa, na Flórida, todos os torcedores que foram ver a final do campeonato de futebol americano, em janeiro deste ano, tiveram seus rostos gravados em vídeo e comparados com um banco de dados de "procurados" por um software de reconhecimento facial. O mesmo programa é usado em Ybor, região que concentra a vida noturna de Tampa.

A empresa que desenvolveu o sistema, a Viisage, é líder de um mercado milionário. Para "refinar a sua clientela", separando doentes de saudáveis e bons motoristas dos barbeiros, seguradores estão pagando a governos estaduais valores anuais de até US\$ 5 milhões (exemplo de um caso no Colorado) para terem acesso a uma base de fotos e

de registros de carteiras de motoristas formulada pela Viisage.

Na esteira dos atentados do dia 11 de setembro, outra companhia do setor ofereceu de graça ao FBI (a polícia federal dos Estados Unidos) um software semelhante para "caçar terroristas".

"Independentemente do combate ao terrorismo, os americanos já estavam admitindo, como algo inevitável e incontrolável, o uso de suas informações confidenciais por grandes empresas", diz Grayson Barber, advogado especializado em direito à imagem. Para ele, uma das explicações para a aceitação do pacote antiterrorismo pode ser a seguinte: "Já que a invasão de privacidade é inevitável, pelo menos usem esse abuso para pegar terroristas".

Nenhum assunto é mais sensível que o monitoramento da internet pelo governo. Há alguns anos, o FBI desenvolveu um sistema chamado Carnivore.

Trata-se de um aparelho (uma caixa preta) que, quando acoplado aos provedores de internet, é capaz de grampiar o tema dos e-mails e o conteúdo das home pages visitadas pelo internauta.

Desde 1986 o FBI precisa obter ordem judicial para interceptar comunicação via internet, comparando-a às ligações telefônicas. O pacote dispensa essa exigência "em casos excepcionais".

O critério do que é excepcional será definido pelo governo.

Como o Carnivore intercepta não só a comunicação de um único internauta, mas de todos os clientes do provedor onde tiver sido instalado, o pacote antiterror, em tese, permite o monitoramento de milhares de pessoas ao mesmo tempo. Esse tipo de ameaça à privacidade não tem preocupado os juizes americanos.

Nos últimos três anos, só ocorreram duas negativas para o uso do Carnivore. No ano passado, dos 2.202 pedidos de grampo, não houve nenhuma negativa. Para fortalecer aqueles que defendem maior controle, um juiz negou em agosto último uma autorização para instalar o Carnivore justamente no provedor de um dos suspeitos de ter arquitetado o ataque ao World Trade Center, o franco-marroquino Zacarias Moussaoui. Ele está preso porque seu professor numa escola de aviação desconfiou de seu desinteresse por decolagem e pouso.

Falta inteligência humana

Para Bill Malik, diretor da empresa de segurança Gartner, as preocupações sobre liberdades civis podem até fazer sentido, mas seria inocente imaginar que terroristas possam ser monitorados só com as leis atuais.

"É infantil a idéia de que bandidos comunicam-se por meio de um só telefone ou um único endereço eletrônico. Eles mudam, e o FBI precisa acompanhar essas mudanças", defende.

Segundo Malik, o desafio não é só equilibrar as liberdades civis e a segurança. "Poucos ousam colocar a verdadeira questão: será que a privacidade total é uma idéia antiga?"

"Isso é uma falácia", responde Will Doherty, diretor da Electronic Frontier Foundation, uma entidade cujo objetivo é harmonizar as novas tecnologias e a proteção às liberdades civis. "Associar automaticamente segurança a restrições às liberdades civis é um erro. A única inteligência do governo que precisa ser fortalecida é a humana, e não a eletrônica." Doherty dá o exemplo das imagens gravadas por câmeras de alguns dos supostos sequestradores dos aviões: "Alguns foram gravados comendo pizza, outros tirando dinheiro em bancos e até fazendo compras no Wal-Mart. Para que serviram essas imagens se a CIA e o FBI não sabiam que eles eram terroristas?".

Segundo Doherty, mais importante do que invadir a privacidade das pessoas é checar se os instrumentos tradicionais de inteligência (infiltração em grupos terroristas e cooptação de seus integrantes) estão funcionando.

"Não estou criticando o FBI, mas, se dermos instrumentos poderosos nas mãos de instituições não preparadas, só os inocentes vão sofrer", argumenta. Depois de ser atenuado pela Câmara norte-americana, o pacote alternativo à proposta antiterror da Casa Branca autoriza o grampo de telefones e o rastreamento de comunicações pela internet mesmo sem uma ordem judicial.