Inovação Uniemp
Print ISSN 1808-2394

Inovação Uniemp vol.3 no.4 Campinas July/Aug. 2007

ARTIGO

Perigo real e imediato: privacidade no século XXI

JOÃO HENRIQUE DE AUGUSTINIS FRANCO

Ministro viola sigilo bancário de caseiro. Vídeo com apresentadora de TV e namorado em praia espanhola é colocado no YouTube. Câmeras são instaladas em banheiros de escola pública. Orkut vira ferramenta de seleção de candidatos. INSS decide monitorar mensagens de correio eletrônico e pode punir servidores por uso indevido. Usuários de cibercafés de São Paulo deixam para trás senhas, e-mails, fotos e outras informações. Projeto que regulamenta uso da internet fere privacidade. Sorria, você está sendo filmado!

"Poder e habilidade de controlar as informações verdadeiras sobre você, que outros podem

vir a saber", na definição de Lawrence Lessig, professor de direito em Stanford e autor do famoso *Code and other laws of cyberspace*, a privacidade tem sido mais e mais ameaçada pela evolução incessante das tecnologias de informação e de comunicação.

Fazer um telefonema ou um saque em um caixa automático, pagar com cartão de crédito, passar por um pedágio eletrônico ou visitar um sítio na internet deixam uma trilha persistente de informações digitais, batizada de *data shadow* por Alan Westin nos anos 60. Professor da Universidade Columbia, Westin já vislumbrava, naquela época, a possibilidade de criação de dossiês pessoais contendo registros detalhados de contas bancárias, de apólices de seguro e de crédito pessoal.

Segundo o sociólogo Domenico de Masi, silêncio, espaço e privacidade serão luxos cada vez mais raros. E na visão de Simson Garfinkel, professor universitário e autor de *Database Nation*, a privacidade no século XXI não será ameaçada por um totalitarismo estatal orwelliano, mas sim pelo próprio capitalismo, "onde cem pequenos irmãos observam e interferem em nossa vida cotidiana".

Mais do que o Grande Irmão de Orwell, a Google Inc. lembra o Mefistófeles de Goethe. Afinal, de forma pactuada, conhece os interesses de quem faz pesquisas na internet, as informações nos computadores onde está instalado o Google Desktop, a lista de contatos no Google Talk, os vídeos vistos no YouTube, as informações pessoais colocadas no Orkut, os links visitados por quem utiliza o Google Accelerator, as informações profissionais inseridas no Google Calendar e o conteúdo das mensagens trocadas via Google Mail. Em troca, os usuários desses serviços concordam em terem essas informações examinadas para a geração de links patrocinados. A eficiência desse modelo de negócio e de sua gestão é inquestionável, como atestam o valor de mercado da Google Inc. (US$ 150 bilhões) e seu faturamento em 2006 (US$ 10 bilhões). Sem pacto e sem compensação, entretanto, estão aqueles que não são assinantes do Google Mail, mas acabam tendo o conteúdo de sua correspondência eletrônica vasculhado sem seu consentimento ou conhecimento. A recente aquisição da Doubleclick pela Google Inc., uma transação de US$ 3,1 bilhões, está gerando polêmica nos EUA, pois adicionaria ao gigantesco volume de informações da primeira o também enorme banco de dados da Doubleclick, cujos anúncios são vistos por cerca de 80% dos usuários da internet. Como a efetivação dessa transação representará uma ameaça à privacidade, muito maior do que a coleta de informações de usuários do MS-Windows e do MS-Office ou o finado número de série do Pentium III, entidades de defesa dos direitos civis dos EUA estão questionando a compra da Doubleclick perante a Federal Trade Commission (FTC), órgão do governo norte-americano.

Os atentados de 11 de setembro são um divisor de águas na questão da privacidade. Após o ataque às torres gêmeas, o governo dos EUA criou o programa Total Information Awareness (TIA) com o objetivo de coletar e analisar o maior número de informações sobre cidadãos norte-americanos (e sobre estrangeiros com os quais eles tenham tido contato) e assim permitir a detecção e identificação de terroristas. Diferentemente da rede de espionagem global Echelon, o TIA montaria um gigantesco repositório com registros pessoais de todo tipo - biométricos, profissionais, financeiros, médicos, comerciais etc. - possibilitando o uso intensivo de técnicas de mineração de dados para identificar padrões e estabelecer associações. Embora o Congresso norte-americano tenha suspenso o aporte de recursos para o projeto em 2003, aparentemente seus objetivos estão sendo perseguidos em outros programas governamentais.

"MAIS DO QUE O GRANDE IRMÃO DE ORWELL, A GOOGLE INC. LEMBRA O MEFISTÓFELES DE GOETHE. AFINAL, DE FORMA PACTUADA, CONHECE OS INTERESSES DE QUEM FAZ PESQUISAS NA INTERNET..."

Vítimas das polícias secretas do pré e do pós-guerra, Gestapo, KGB e Stasi, que coletaram e usaram informações pessoais para praticar atrocidades, os europeus são muito zelosos com questões ligadas à privacidade. Em 1995, a União Européia (UE) aprovou a Diretriz 46, que estabelece regras para o processamento e movimentação de dados pessoais; como no caso de outras diretrizes da UE, coube a cada país-membro, desde então, aprovar a legislação nacional correspondente. Em 2001, o Parlamento Europeu reconheceu oficialmente, a despeito das negativas, também oficiais, do governo norte-americano, a existência da rede de espionagem eletrônica Echelon. Em 2005, na esteira dos atentados de Madri e Londres, a UE aprovou uma diretriz permitindo que órgãos policiais europeus possam obter informações sobre uso de celulares e acessos à internet; essa mesma diretriz ainda estabelece que os prestadores de serviço devam manter tais informações

disponíveis por dois anos.

Localmente, a Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil) determina que um certificado digital de pessoa física ("e-CPF") contenha vários dados pessoais de seu titular (data de nascimento, RG, CPF, PIS/Pasep e título de eleitor) para garantir a autenticidade da chave pública correspondente. Por outro lado, uma vez que certificados digitais são documentos eletrônicos públicos, todo repositório de e-CPFs acaba sendo também um grande cadastro de informações pessoais, que pode ser pesquisado por qualquer interessado de forma automatizada e anônima.

A tecnologia RFID (Radio Frequency Identification), que permite a identificação de produtos, veículos, animais e pessoas, tem sido objeto de questionamentos por apresentar características consideradas invasivas. Sua operação é bastante simples: as características de um *chip (tag)* afixado ao item são lidas à distância, via radiofreqüência, por um dispositivo de leitura, que também se encarrega de fornecer energia ao *chip*. Além da identificação do item e do fabricante, cada *tag* possui um número de série, o que permite seu rastreamento. ONGs de defesa da privacidade como o Electronic Privacy Information Center (Epic) fazem várias críticas à tecnologia RFID: 1) o consumidor pode não saber da existência do *tag* (apelidado pejorativamente de *spychip*) preso ao item adquirido, nem ser capaz de removê-lo caso perceba sua presença; 2) a leitura das características do *tag* pode ser feita sem o conhecimento ou consentimento do consumidor; 3) o *tag* permanece funcional mesmo após o produto ter sido adquirido e levado para casa, possibilitando o monitoramento de seu uso.

Diferentemente da segurança, que é um ativo de curto prazo, diz Ed Gerck, especialista em voto eletrônico, privacidade é um ativo de longo prazo, fazendo com que a troca da segunda pela primeira não seja usualmente um bom negócio. Se no caso do comércio eletrônico a segurança do vendedor e a privacidade do comprador estão em pratos diferentes da balança e esta acaba pendendo para o vendedor, em outro contexto, o do voto eletrônico, afirma Gerck, a privacidade não deve ser sacrificada em nome da segurança. A razão é simples: conhecidos todos os eleitores e todos os votos, devem ser garantidos tanto o anonimato do eleitor (dado um voto, não deve ser possível identificar seu eleitor) como o segredo do voto (dado um eleitor, não deve ser possível conhecer seu voto).

De acordo com Jonathan Zittrain, professor da Universidade de Oxford, os problemas que afligem o *copyright* e a privacidade são essencialmente semelhantes: a perda do controle possibilita, no primeiro caso, cópias perfeitas e sem custo de conteúdo protegido por

copyright e, no segundo, o monitoramento contínuo e barato do comportamento individual. A despeito dessa similaridade, a defesa da privacidade e a proteção de *copyright* estão em lados opostos do espectro político, o que explica porque grupos que defendem tenazmente a primeira ataquem o segundo (aí incluída a tecnologia Digital Rights Management-DRM) com igual empenho.

Internautas em geral e usuários de comércio eletrônico em particular já estão cientes da proteção dada aos dados pessoais e ao número do cartão de crédito quando em trânsito na internet, condição indicada pelo ícone "cadeado fechado". Parece não haver a mesma preocupação, entretanto, em verificar se a empresa vendedora possui uma política de privacidade e, em caso afirmativo, quais são os procedimentos adotados para a proteção dos dados pessoais de seus clientes.

O século XXI está em seu início, mas a batalha pela privacidade, iniciada há muito tempo atrás, parece não ter fim à vista.

João Henrique de Augustinis Franco *é consultor em segurança da informação.*

Cidade Universitária Zeferino Vaz
Prédio V da Reitoria, 3º piso
13083-970 Campinas - SP - Brasil
Tel.: (55 19) 3289 3120
Fax: (55 19) 3521 7857

labjor@unicamp.br