Americanos festejam evolução da comunicação privada

A Internet é isso: um mecanismo que facilita e dificulta as comunicações. O paradoxo situa-se no fato de que, ao mesmo tempo em que a rede mundial de computadores proporciona eficiência aparentemente segura na troca de informações privadas, oferece brechas devassáveis que vulnerabilizam o sistema.

Os EUA estão comemorando os trinta anos da criação da chamada Public-Key Cryptography (PKC), um sistema de criptografia para proteção de documentos públicos. Uma prática que, nessas três décadas, virou uma ferramenta indispensável para o mundo dos escritórios de advocacia e da comunicação corporativa, segundo o advogado Andrew Zangrilli, do site Findlaw.

“Essa criptografia mantém as comunicações digitais em segredo e de maneira segura. Na Era da Informação, em que as pessoas conduzem boa parte de suas vidas via on line, a Public-Key Cryptography (PKC) é uma tecnologia ubíqua (capacidade de estar conectado à rede, e fazer uso da conexão, constantemente, a todo o momento, nas mais variadas situações). Está em tudo, no sistema bancário, no comércio eletrônico e na troca de e-mails”, diz Andrew Zangrilli

O PKC foi uma invenção civil, inicialmente chamada de “troca assimétrica de chaves”, criada por Whitfield Diffie e Martin Hellman, em 1976. Em 1977 um grupo de estudantes do Massachussets Institute of Technology (MIT) criaram o algoritmo chamado RSA, que incorporava a assinatura digital na preservação de documentos públicos. Após essas invenções, a história do PKC foi pontuada de lutas entre um governo que queria controlar o sistema e uma indústria que o pressionava para liberar o PKC para uso comercial. A tensão entre governo e iniciativa privada marca toda a história do PKC, analisa o colunista Andrew Zangrilli.

A Agência Nacional de Segurança dos EUA (NSA), o braço mais poderoso da inteligência americana — voltado para a produção de informação, contra-informação e espionagem — ainda vindica o controle de tipos de PKC, alegando que as poderosas funções do sistema “são uma arma de guerra” . Só em 1996 foram relaxadas as tensões e a iniciativa privada pode fazer uso do PKC. Hoje o sistema é moda e necessidade em todos os grandes escritórios de advocacia dos EUA.

Meta Fields