Notícias

Novo mercado da privacidade é consequência das revelações de Snowden

Por Ana Paula Zaguetto
04/11/2014

Após o vazamento de fotos de celebridades do serviço de armazenamento de arquivos iCloud, o debate sobre segurança e privacidade dos dados pessoais voltou à tona e provocou mudanças por parte de grandes empresas do setor. A Apple lançou uma nova seção em seu site (**https://www.apple.com/privacy/**) onde divulga sua política de privacidade em uma linguagem amigável (diferente do que normalmente são os termos de privacidade) e sugere práticas aos usuários para que possam aumentar a sua segurança ao utilizar serviços na web. No site, há também uma carta do CEO da Apple, Tim Cook, que afirma o compromisso da empresa com a segurança dos dados dos usuários e nega o uso desses dados para monetização e fornecimento de informações ao governo. "Nós não construímos um perfil baseado no conteúdo do seu e-mail e de seus hábitos de busca na web para vender à anunciantes", diz um trecho da carta, considerada uma indireta ao Google e uma forma da empresa se diferenciar de seu concorrente.

Uma das medidas adotadas pela Apple foi o reforço da criptografia dos dados (codificação da informação para impedir que seja acessada). O Google não ficou atrás, anunciando uma nova versão do sistema operacional Android onde a encriptação dos dados será padrão. A decisão das duas empresas mostra que a privacidade está se tornando um atrativo na hora de conquistar consumidores. "Tem um novo mercado se constituindo cuja característica é oferecer privacidade aos usuários", explica Henrique Parra, professor da Unifesp e pesquisador da Rede Latino-Americana de Estudos sobre Vigilância, Tecnologia e Sociedade (**Lavits**), que relaciona esse movimento do mercado às denúncias feitas por Edward Snowden, tornando pública a colaboração entre empresas de software e hardware americanas e o sistema de vigilância estatal. "Algumas revelações afetaram a reputação de empresas que agora fazem um movimento de oferecer, como um produto, novas possibilidades para a proteção dos dados pessoais de seus usuários".

Conflitos entre Estado e mercado

Mas se, por um lado, a disputa de mercado entre as empresas pode trazer benefícios para os cidadãos, por outro setores do governo não veem a criptografia com bons olhos. James B. Comey, diretor do FBI, **declarou** que o avanço da criptografia tem criado "um significante problema de segurança pública", dificultando o acesso à informações para resolver crimes e "prevenir o terrorismo". No entanto, segundo Parra, o Estado sempre terá condições de conseguir informações necessárias para a resolução de um crime. O que a criptografia dificulta é a coleta massiva de dados: "é uma questão econômica. Se você não usa e-mail criptografado, do ponto de vista da escala industrial da vigilância, analisar os dados coletados é muito barato. Se as pessoas passarem a usar comunicação criptografada, a análise dos dados coletados massivamente encarece".

Um dos problemas apontados pelo pesquisador na coleta massiva de dados é que tal Estado parte do princípio de que todas as informações privadas devem estar disponíveis *a priori*, baseado no pressuposto de que todo cidadão é um criminoso em potencial. "Esta inversão é uma séria ameaça à democracia. Na realidade, com os meios digitais temos que criar novos mecanismos (legais e tecnológicos) para proteger a privacidade dos cidadãos.".

Garantias para a privacidade

Parra defende que teremos que discutir um novo marco regulatório para proteção dos dados pessoais no contexto da comunicação digital e do surgimento de grandes bancos de dados corporativos e estatais. Como evitar, por exemplo, que os dados gerados pelos usuários de um site ou serviço qualquer, mesmo que não identificados, sejam usados contra os cidadãos? "Muitas iniciativas na internet cresceram através de uma economia baseada na coleta de dados dos usuários. Uma informação isolada sobre um usuário pode não ser relevante, o problema é quando se começa a juntar e cruzar muitos dados sobre os usuários". Dessa forma, mesmo que a identidade não seja revelada, é possível imaginar situações em que informações estatísticas sejam utilizadas por empresas ou pelo estado para obter vantagens econômicas ou controle político sobre o cidadão.

A própria decisão das empresas em assegurar a privacidade dos usuários não é algo confiável. Se no momento essa é uma atitude que traz benefícios financeiros, uma mudança nesse cenário pode fazer com que as empresas mudem sua estratégia de mercado, deixando de garantir a privacidade. Nesse sentido, o combate à vigilância cresce em duas direções. Uma é a sociedade civil organizada, que luta pelos direitos civis na era da vigilância, como a entidade internacional Eletronic Frontier Foundation (EFF). A outra são ações coletivas e o ativismo hacker que denunciam violações aos direitos humanos e disseminam tecnologias de comunicação mais seguras e que promovem a privacidade