Por Marcia Alves

Entre todos os avanços trazidos pelo Marco Civil da Internet, o mais importante foi a proteção e a inviolabilidade da privacidade, garantindo o sigilo nas comunicações dos usuários e impedindo a venda de informações dos registros de conexões. A expectativa é que a regulamentação da Lei 12.965/2014 estabeleça formas de controle sobre o uso de registros, inclusive por parte das autoridades governamentais, tanto policiais como administrativas.

Segundo o pesquisador e gestor do Centro de Tecnologia e Sociedade da Fundação Getulio Vargas, Luiz Fernando Moncau, a Europa pode servir de exemplo. Em entrevista à Agência Brasil ele comentou que em alguns países europeus já vigora uma regra de guarda de dados, que estabelece a publicação de relatório periódico sobre dados solicitados e destes qual o percentual serviu para resolver casos judiciais.

No Brasil, o que sabe até o momento é que Ministério da Justiça está à frente da regulamentação do Marco Civil e prevê longa discussão pública. A fiscalização ficará a cargo de órgãos de defesa do consumidor, Ministério Público e até polícias. Por ora, especialistas avaliam que o efeito do marco é mais “didático” do que punitivo.

Uma das lacunas do Marco Civil da Internet e também do Projeto de Lei 4060/2012 sobre Proteção de Dados, atualmente em trâmite, é a ausência de obrigatoriedade de notificação sobre a violação de dados. Para a sócia da JBO Advocacia, Marcia Cicarelli Barbosa de Oliveira, se não houver uma lei que positive esse dever será difícil implementar o principio de proteção de dados.“Se o consumidor não for notificado sobre a violação dos seus dados, nunca tomará as ações cabíveis contra a empresa que deixou de protegê-los”, diz.

A preocupação é factível, considerando que houve um aumento de mais de 100% de ataques de hackers no país entre 2011 e 2013, quando o número de casos saltou de 2.562 para 4.665, segundo informações da revista Valor. Estudo elaborado em 2013 pela Symantec e pelo Ponemon Institute aponta que a violação de dados no Brasil gera perdas médias de R$ 2,64 milhões de reais, podendo chegar a R$ 9,74 milhões. Segundo a pesquisa, o custo médio de R$ 143 por registro comprometido cai para até R$ 19 em organizações com uma boa estrutura de segurança.

Para o coordenador-geral na Secretaria Nacional do Consumidor (Senacon/MJ), especialista em proteção de dados pessoais, Danilo Doneda,o país está atrasado nessa questão. Ele comentou no blog do Estadão que a primeira lei nacional de proteção de dados foi feita na Suécia, em 1973. De lá para cá, mais de cem países (incluindo os vizinhos Argentina, Uruguai, Chile e Colômbia) criaram legislações próprias, dos quais 92 mantêm agências específicas. “Alguns setores demoraram a entender que a proteção de dados não está só ligada a privacidade, mas a segurança jurídica”, disse.

Dados de segurados em risco

No âmbito do mercado de seguros, a entrada em vigor do Marco Civil da Internet trouxe a perspectiva de expansão dos seguros para riscos cibernéticos, que, atualmente, são comercializados por apenas duas seguradoras. Mas para desenvolver o grande potencial desse seguro no país também é importante que a regulamentação da internet estabeleça a obrigatoriedade de notificação de quebra de confidencialidade, que em outros países foi um fator-chave no crescimento do mercado de seguros.

“O dever de notificar a violação de dados é uma espécie de gatilho para o seguro de riscos cibernéticos”, diz Marcia Cicarelli. Ela explicou que a partir dessa notificação já começa a se estabelecer o valor de indenização, que representa os gastos das empresas com notificação,

monitoramento e consultoria a todos que tiveram seus dados violados, além dos custos para restabelecer o sistema.

Embora o foco das empresas de seguro seja o vasto número de organizações vulneráveis a ataques de hackers, também elas – as próprias empresas de seguros – não estão livres de ataques cibernéticos. O recente relatório IBM Security Services 2014 apontou que o setor de seguros junto com o segmento financeiro são o alvo preferido de cibercriminosos (23,8%), seguido pela indústria (21,7%), informação e comunicação (18,6%), varejo (6,2%) e saúde (5,8%). Juntos estes setores concentram mais de 75% dos ataques virtuais.

Considerando que, atualmente, o número de usuários de internet no Brasil já passa de 100 milhões de pessoas, dos quais, segundo o Google Brasil, 44% fazem pesquisa online antes de contratar um seguro, inclusive transmitindo informações pessoais, então o risco de violação de dados é alto. Sem contar o número de transações de e-commerce, que já atingiu a marca de 51 bilhões de compradores em 2013, segundo pesquisa divulgada pelo site eCommerceOrg.

Nessa seara de venda de seguros pela internet, vale registrar o crescimento das empresas pontocom, que estima-se hoje sejam quase 20 em operação, as quais manipulam diariamente dados de segurados e potenciais compradores de seguros. ”O armazenamento de dados em sistema acessíveis por meio de login e senha (refiro-me às páginas de corretoras), podem ser um prato cheio para a obtenção de dados pessoais, como RG, CPF, profissão, endereço e estado civil”, destaca o advogado Thales Barbosa, da JBO Advocacia.

Risco maior para os seguros pessoais

Em sua avaliação, o risco é maior para empresas que atuam no ramo de pessoas. “No processo de avaliação de propostas para a emissão de apólices novas ou renovações, as seguradoras de vida e saúde lidam com dados sensíveis dos segurados, como histórico de doenças, tratamentos de saúde realizados e históricos familiares. A perda de dados deste tipo pode acarretar em grave violação dos direitos à privacidade e intimidade, consagrados na Constituição Federal (Art. 5º, inciso X), da qual decorrem os chamados danos morais”, adverte.

Ele destaca que a captação de seguros na internet por corretoras também pode gerar a responsabilização de seguradoras, em caso de violação de dados. “Em principio, a responsabilidade pela perda de dados será sempre de quem os armazenou. No entanto, se constatado o compartilhamento de dados entre seguradora e corretora, e a violação de dados afetar este compartilhamento, é possível que ambos sejam solidariamente responsáveis pela reparação do dano, de acordo com o Código de Defesa do Consumidor (CDC, Art. 7º, parágrafo único)”, observa.

“A tendência de crescimento de usuários da Internet e do comércio eletrônico aumentam a importância da proteção de dados. Mas, a sociedade terá de cobrar a aprovação de regulamentação que inclua o dever de notificação sobre a violação de dados”, conclui Marcia Cicarelli.

Fonte: CVG-SP, em 15.08.2014.