Por Elisa Mombelli (*)

Na Black Friday de 2013, a Target, uma gigante do varejo norte-americano, sofreu um dos maiores ataques virtuais da história, em que dados de 77 milhões de consumidores foram roubados – incluindo dados pessoais, cartões de crédito e informações bancárias. Decorrido mais de um ano do incidente, o caso continua a repercutir na justiça americana.

No fim do ano passado, uma decisão da corte de Minnesota, EUA, deu prosseguimento à ação ajuizada pelas instituições financeiras contra a Target. Os bancos acusam a empresa de ter falhado na segurança e proteção dos dados, e exigem o ressarcimento dos prejuízos decorrentes das fraudes praticadas com as informações vazadas (prejuízo estimado em US$ 400 milhões).

Nos Estados Unidos, diversas outras ações semelhantes precedem este caso. Em 2007, a Visa e a TJX Companies fecharam um acordo milionário para encerrar a ação movida pela Visa contra a varejista, após uma invasão de malware em que 46,5 cartões de crédito foram atingidos. Da mesma forma que no caso anterior, a financeira acusou a TJX de apresentar falhas de segurança.

E a cadeia de responsabilidades não parou por aí. Em outro notório incidente envolvendo roubo de dados, até a consultoria de segurança foi processada, por ter certificado, dois meses antes da invasão, que a empresa atingida cumpria com os padrões de segurança exigidos pela Visa (o chamado Visa CISP - Cardholder Information Security Program). No caso, a compliance de segurança da empresa alvo do ataque - a intermediadora de pagamentos CardSystem Solutions - não foi suficiente para evitar a invasão. A ação terminou em um acordo cujos termos não foram divulgados.

Se esses casos tivessem ocorrido no Brasil, as instituições financeiras também seriam obrigadas a ressarcir os danos decorrentes das fraudes praticadas com os dados dos consumidores. Trata-se de responsabilidade objetiva, decorrente do risco da atividade, conforme jurisprudência já consolidada. E, da mesma forma que nos Estados Unidos, teriam também direito regressivo contra a empresa responsável pela guarda e proteção dos dados, principalmente após a aprovação do Marco Civil da Internet, que trouxe como princípios fundamentais a proteção de dados pessoais e a privacidade.

Nos termos da legislação brasileira, com efeito, todo prejuízo deve ser indenizado pelo agente que deu causa ao incidente, seja ele intencional, seja fruto de negligência, ou de forma objetiva, no caso de a empresa desempenhar “atividade de risco” - conceito em que já são enquadradas as instituições financeiras, mas poderá abarcar também as organizações que coletam e guardam dados de consumidores, e, principalmente, as empresas de tecnologia que oferecem as soluções de segurança utilizadas no armazenamento dos dados pessoais.

Assim, observamos a seguinte cadeia de responsabilidades. Num primeiro momento, os consumidores lesados em fraudes praticadas com os dados roubados devem ser indenizados pelas instituições financeiras, responsabilidade esta que é objetiva (STJ, AgRg no AREsp 602.968/SP, julgado em 02/12/2014, DJe 10/12/2014). Devem, também, ser indenizados nos casos de ofensa à honra, imagem ou privacidade gerados pela divulgação de dados sensíveis (TJ/SP, Apelação nº 0019741-18.2009.8.26.0032; TJ/GO, Recurso Inominado nº 20060110966598).

Por sua vez, as instituições financeiras obrigadas a ressarcir seus clientes podem cobrar o custo destas fraudes da empresa que foi alvo da invasão/vazamento, se for possível demonstrar que houve negligência na segurança de dados pessoais, e comprovando a relação direta entre as transações e as informações roubadas.

Por fim, empresas que fornecem soluções tecnológicas de segurança para armazenamento de dados - bem como as empresas de auditoria encarregadas de certificar a adequação destas medidas aos padrões de segurança exigidos - também podem vir a ter sua responsabilidade questionada, tanto pelos bancos quanto pela própria empresa vítima da invasão.

A fim de mitigar os riscos, fornecedores de softwares e soluções de segurança podem se precaver de duas formas: mediante a contratação de um seguro específico, ou com a inserção de uma cláusula limitar de responsabilidade nos contratos caso ocorra uma eventual indenização regressiva quando a solução for utilizada no armazenamento de dados pessoais. Com a inserção de cláusulas pertinentes e adequadas no contrato, a responsabilidade da empresa responsável pela segurança, se for reconhecida, poderá ser reduzida ou até mesmo afastada.

Até agora, vazamentos e transferências de dados pessoais não autorizadas têm sido tratados no Brasil pelo Procon e pelo Ministério da Justiça, mas não chegaram a virar litígio entre as empresas envolvidas.

Contudo, os casos narrados no início deste artigo, muito embora sejam precedentes da justiça americana, ilustram situações que podem vir a ser enfrentadas em breve pelo Judiciário brasileiro. Casos ainda sem precedentes no Brasil, mas que tendem a aparecer após a aprovação do Marco Civil da Internet. Sendo a privacidade e a proteção de dados princípios fundamentais erigidos pela nova lei, vem aí uma nova onda de ações judiciais em que contratos e responsabilidades deverão ser discutidos, e a obrigação de indenizar poderá ser reconhecida nos casos de invasão e vazamento, mesmo antes de aprovada a lei específica de proteção dos dados pessoais.

(*) **Elisa Mombelli** é advogada especialista em Direito Digital, sócia do escritório Assis e Mendes.

Fonte: Jus Econômico, em 05.02.2015.