Opinião: Impactos de um ataque cibernético sob a ótica da LGPD

Muito tem se falado acerca do ataque cibernético sofrido pela rede varejista Lojas Renner no último dia 19, que neutralizou os sites da empresa até o sábado (21/8) e deixou o app sem funcionar até domingo (22/8). Ataques como esse estão se tornando recorrentes no país, merecendo destaque a invasão sofrida pela JBS, que culminou no pagamento de um resgate de US$ 11 milhões para evitar o vazamento de

Para aqueles que não sabem do que se trata, esse tipo de ataque é chamado de *ramsomware*, no qual um vírus impede o acesso às informações armazenadas em determinado sistema, com o objetivo de forçar o pagamento de valores gigantescos para recuperar os dados, geralmente em criptomoedas, o que torna quase impossível rastrear o criminoso.

Além da cobrança de resgate, derrubada do acesso ao site e aplicativo (que pode significar a paralisação das operações essenciais do negócio) e prejuízos à imagem da empresa, especialmente no quesito segurança da informação, esse tipo de incidente também pode gerar responsabilidades legais em decorrência da Lei Geral de Proteção de Dados (LGPD), que obriga as empresas a adotarem medidas de segurança aptas a proteger dados pessoais de acessos não autorizados e de situações ilícitas, de destruição ou perda.

Nessa esteira, a LGPD criou a Autoridade Nacional de Proteção de Dados (ANPD), a quem é atribuída a responsabilidade por zelar pela proteção dos dados pessoais, inclusive fiscalizando e aplicando sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso.

A Autoridade Nacional de Proteção de Dados disponibilizou para consulta pública a minuta do Regulamento de Fiscalização e Aplicação de Sanções Administrativas, no qual estabelece toda a normatização sobre a forma em que serão processadas as denúncias, reclamações, representações e requerimentos apresentados à ANPD. Até a entrada em vigor desse regulamento, a autoridade informou que não iniciará a sua atuação sancionadora, a fim de conferir segurança jurídica aos administrados.

2023 - www.conjur.com.br - Todos os direitos reservados.

Embora a ANPD tenha competência para aplicar as penalidades (vigentes desde o último dia 1º), a própria autoridade já adiantou que outros órgãos públicos (como o Procon) podem atuar, delimitados pelas suas próprias competências, ao abrigo de suas legislações específicas (a exemplo do Código de Defesa do Consumidor), ainda que utilizando fundamentos da Lei Geral de Proteção de Dados para situar uma ofensa nas respectivas esferas de atuação.

E foi o que aconteceu. Com base em preceitos da LGPD, o Procon-SP notificou a Lojas Renner para prestar contas sobre a existência de um plano de proteção e recuperação que esteja sendo executado, sobre o processo de criptografia utilizado na coleta, tratamento e armazenamento de dados dos clientes (titulares dos dados), bem como sobre a presença de um encarregado de dados nomeado.

Isso mostra que se um incidente de segurança, além de acarretar dano aos titulares de dados pessoais no tocante ao tratamento indevido, também ensejar em ofensas às normas da legislação civil, penal, consumerista etc., os responsáveis poderão ter de arcar com sanções aplicadas em processos administrativos, movidos por outras agências reguladoras ou órgãos de defesa do consumidor, e, inclusive, podem ser responsabilizados civil ou penalmente pelo ato.

Assim, não obstante a Autoridade Nacional de Proteção de Dados ainda não esteja efetivamente aplicando as sanções administrativas previstas na LGPD, o Procon já vem fiscalizando os eventos que possam ter impacto nos direitos consumeristas (como se vê no caso das Lojas Renner) e, primordialmente, desde o início da vigência da lei, os próprios titulares dos dados podem acionar o Poder Judiciário para garantir o cumprimento de seus direitos, inclusive perquirindo indenizações, caso alguma operação de tratamento de dados pessoais feita em desconformidade com a lei acarrete em prejuízos materiais ou extrapatrimoniais.

Diante do risco de ataques cibernéticos, é necessário munir-se com rigorosas políticas de segurança da informação de proteção de dados pessoais, seja para evitar os prejuízos com o "sequestro" de informações ou, ainda, para garantir que os direitos dos titulares sejam observados e, com isso, mitigar as contingências de processos administrativos e/ou judiciais.

Date Created
31/08/2021

2023 - www.conjur.com.br - Todos os direitos reservados.