Luiz de Castilho: Casos de vazamentos de dados

Em 2021, o Brasil foi o sexto país mais atingido por vazamentos de dados, de acordo com um levantamento da empresa Surfshark, que atua na área de ferramentas de privacidade e segurança online. No âmbito empresarial não foi diferente. Só no primeiro semestre de 2021, pelo menos 69 instituições brasileiras foram alvo de ataques de vazamento e sequestro de dados, conforme dados da Apura Cyber Intelligence. E, embora muito tenha sido noticiado e comentado a respeito, grande parte da população [illegible]mentos.

A descrição sobre o que é um dado pessoal está prevista na Lei Geral de Proteção de Dados Pessoais, especificamente em seu artigo 5º, na qual considera toda informação relacionada a uma pessoa natural. A LGPD define, ainda, como informações sensíveis aquelas *"sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural"*. Nesse sentido, podemos entender como vazamento de dados a quebra da segurança dessas informações, a exposição sem a permissão da pessoa titular desses dados que, consequentemente, viola a confidencialidade dos dados pessoais que estão sob os cuidados do encarregado por essa segurança.

Em 2021, os brasileiros foram surpreendidos com uma sequência quase interminável de incidentes de segurança tanto no setor público, com o ConecteSUS, Ministérios da Saúde, da Economia e do Trabalho, Polícia Rodoviária Federal e Controladoria Geral da União, quanto no setor privado, com os vazamentos da Experian, Magazine Luiza, Mercado Livre, Shopee, Amazon e Americanas.

Estima-se que mais de 220 milhões de dados pessoais tenham sido expostos, os quais provavelmente estão sendo vendidos neste exato momento de forma ilegal. A vulnerabilidade na segurança de informação ficou marcada para sempre, deixando comprovado que o setor de cibersegurança está longe de ser seguro.

Mesmo com a existência do Marco Civil da Internet e a LGPD, tais vazamentos jamais serão revertidos. Mesmo na iminência de uma contenção ou recuperação rápida do banco de dados pelo encarregado, as informações copiadas provavelmente ficarão para sempre na web.

Muitos desses incidentes de segurança foram causados por *software* malicioso (*malware*), um sistema desenvolvido para infectar o computador de um determinado usuário. O mais utilizado nos casos de vazamentos de dados é o *r*

ansomware, responsável por criptografar (bloquear) banco de dados, exigindo-se resgate, normalmente com pagamento em criptomoedas.

Ocorre que muitos dos vazamentos ocorridos em 2021 eram evitáveis, ou seja, ocorreram devido ao erro humano, descuido e inobservância dos procedimentos de segurança estabelecidos pela empresa pública ou privada. Um incidente de segurança passou de ser apenas uma simples planilha. Hoje, na era da informação, qualquer dado o mais simples possível se torna uma moeda valiosa. Não por acaso o direito à proteção dos dados pessoais foi elevado como uma garantia fundamental em nossa carta magna (artigo 5º, LXXIX, CF/88).

Exige-se, portanto, uma responsabilidade ainda maior por parte dos responsáveis pelo tratamento de dados e uma intensificação nas fiscalizações por parte da Autoridade Nacional de Proteção de Dados (ANPD), não esquecendo que a segurança não depende exclusivamente do ente governamental ou da equipe de tecnologia de determinada empresa. A segurança das informações deve funcionar como um núcleo, uma organização viva, na qual cada etapa, da coleta ao armazenamento e o tratamento desses dados, possua um fluxo rigoroso e que esteja em constante fiscalização e aprimoramento.

Date Created
19/04/2022