# Ferrigolo: Os ataques cibernéticos ao Poder Judiciário e a LGPD


tório de ataques cibernéticos ao Poder Judiciário.

O primeiro ocorreu no dia 3/11/2020, no Superior Tribunal de Justiça, que identificou o ataque cibernético à sua rede e a seus sistemas. As atividades do STJ foram suspensas e no dia 18 daquele mês o tribunal comunicou que a Secretaria de Tecnologia e Informação e Comunicação concluiu o restabelecimento do sistema.

No dia 11 de novembro, o sistema de processo eletrônico (*eproc*) do Tribunal de Justiça do Rio Grande do Sul sofreu um ataque *hacker*. Quem entrou no sistema do TJ-RS se deparou com uma mensagem atacando o Judiciário, que ficou pouco mais de uma hora no ar.

Outro caso ocorreu no Tribunal Regional Federal da 1ª Região quando este sofreu um ataque *hacker* no dia 27 daquele mesmo mês. O site da instituição foi tirado do ar, tendo sido restabelecido três dias após o ataque, de forma gradual.

Já no dia 15 de janeiro, os sistemas eletrônicos do Tribunal Regional Federal da 3ª Região sofreram um ataque cibernético que sobrecarregou os sítios da corte e provocou instabilidade ao longo do dia. A área de Tecnologia da Informação atuou prontamente para conter o ataque e salvaguardar nossos sistemas.

E no dia 28 de abril a invasão ocorreu novamente no Tribunal de Justiça do Estado do Rio Grande do Sul, e até o momento em que este texto foi escrito os serviços não haviam sido restabelecidos de forma ampla. Os cibercriminosos estariam pedindo o equivalente a US$ 5 milhões em criptomoedas para fornecer as chaves que podem decodificar o conteúdo criptografado em servidores e estações de trabalho.

Nesse passo, a questão que se coloca em debate é: são mera coincidência os ataques com a vigência da Lei Geral de Proteção de Dados?

A Lei nº 13.709/2018 entrou em vigor no dia 18 de setembro de 2020, trazendo normas para disciplinar a maneira do tratamento dos dados pessoais dos indivíduos.

A Lei Geral de Proteção de Dados (LGPD), inspirada no regulamento europeu (GDPR), determina regras e critérios sobre coleta, armazenamento e tratamento de dados.

Dessa forma, para cumprimento da lei, é necessária a implementação de um programa de conformidade com análise nas rotinas/fluxos e processos das empresas da aplicação dos princípios e normas previstos na lei.

Portanto, com base na crescente invasão cibernética recente e na vigência da Lei Geral de Proteção de Dados, torna-se imprescindível a realização e observância das regras com o fim de dar segurança jurídica para a utilização desses sistemas.

Destaca-se que a ausência de regulamentação anterior sobre o tratamento de dados gerou uma pressão internacional para que o Brasil colocasse como prioridade tal pauta.

Com a nova lei, o sistema brasileiro de proteção de dados pessoais deixa de depender unicamente de leis especiais, como o Marco Civil da Internet e o Código de Defesa do Consumidor, ou de garantias apenas principiológicas, como a proteção constitucional à intimidade e à vida privada. De forma sistêmica, o ordenamento jurídico passa a harmonizar as leis existentes, contando com uma lei transversal e multissetorial, aplicável a agentes públicos e privados em diferentes setores da economia e da vida em sociedade.

Portanto, nesse contexto, não há como inferir se é mera coincidência ou não os ataques cibernéticos ao Judiciário brasileiro à vigência da Lei Geral de Proteção de Dados. O que se conclui apenas é que as adequações e o programa de conformidade e à LGPD devam ser realizados por todas as empresas, públicas ou privadas, para o combate ao vazamento de dados, sob pena de causar prejuízos materiais e morais.

**Date Created**
10/05/2021