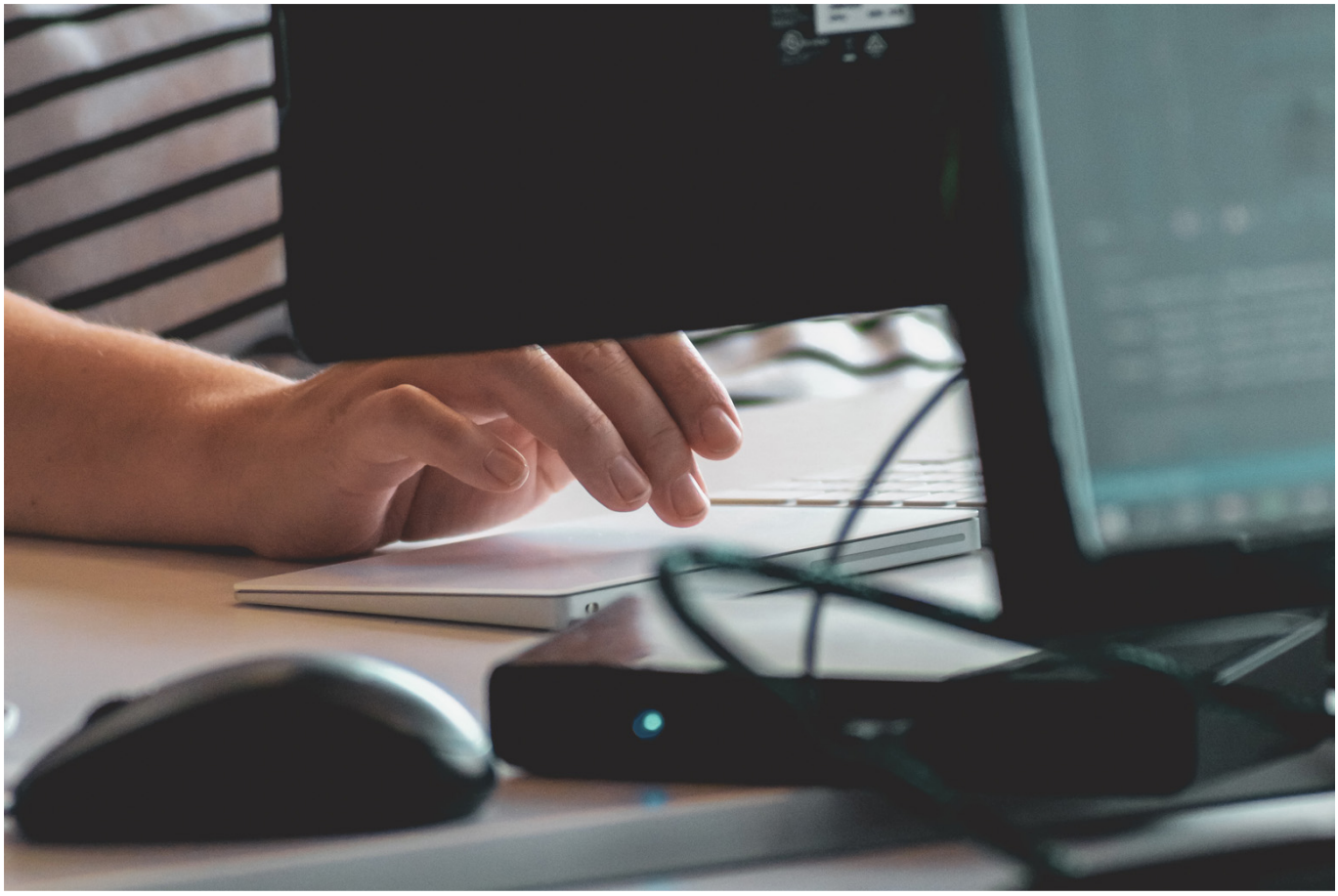
O vazamento de dados é uma questão muito comentada nos dias de hoje e, com a existência da Lei Geral de Proteção de Dados, é importante saber sua regulamentação e direitos envolvidos.

Dessa forma, conheça as sete principais dúvidas sobre o **vazamento de dados** e sua regulamentação no Brasil.

QUANDO OCORRE O VAZAMENTO DE DADOS?



Ele pode ser definido como um incidente onde os dados pessoais e/ou informações consideradas privadas e sigilosas, são publicamente expostas a terceiros sem autorização.

Neste sentido, as informações poderão ser acessadas, principalmente para a aplicação de golpes financeiros, além de poder prejudicar os negócios e a imagem de uma empresa.

QUE TIPOS DE DADOS COSTUMAM SER EXPLORADOS?

Segundo um relatório da IBM, cerca de 80% dos vazamentos de dados nas empresas estão relacionados a perdas ou roubos de dados pessoais dos clientes.

Neste sentido, também há o vazamento dos dados que envolvem propriedade intelectual, dados anonimizados de usuários, e dados pessoais de colaboradores.

QUEM RESPONDE LEGALMENTE PELO VAZAMENTO DOS DADOS DENTRO DE UMA EMPRESA?

Conforme a LGPD, quem responderá por uma violação de segurança dentro da empresa, como o vazamento dos dados pessoais, são os **agentes de tratamento**, ou seja, o controlador e operador.

O controlador, segundo a lei, é a empresa ou a pessoa que coordena e define como o dado pessoal será tratado, da coleta à eliminação.

Já o operador, é a pessoa que realiza o tratamento de dados em nome do controlador, ou seja, é a pessoa ou a empresa que processa e trata os dados pessoais seguindo as ordens do controlador.

Neste sentido, a lei dispõe que estes agentes possuem a responsabilidade de adotar medidas de segurança competentes para proteger os dados pessoais de seus clientes.

QUAIS SÃO AS SANÇÕES PREVISTAS NA LGPD?

Dentre elas, podemos citar:

- Advertência com o prazo para corrigir as infrações realizadas
- Multa simples de até 2% do faturamento da empresa no ano anterior
- Multa diária de até 2% do faturamento da empresa no ano anterior
- Tornar pública a infracção cometida
- Bloqueio dos dados pessoais relacionados à infracção
- Eliminação dos dados pessoais relacionados à infracção
- Suspensão parcial do funcionamento do banco de dados a que se refere à infração

- Suspensão da atividade de tratamento dos dados pessoais a que se refere à infração
- Proibição parcial ou total das atividades relacionadas ao tratamento de dados

Estas sanções só poderão ser aplicadas caso sejam realizadas dentro de um processo administrativo, onde poderá ser garantido o contraditório e a ampla defesa às empresas.

QUAIS SÃO AS CONSEQUÊNCIAS PARA AS EMPRESAS?

Um vazamento de dados poderá trazer diversas consequências, como:

- Sanções administrativas e multas
- Quebra de confiança na relação com o consumidor e com os titulares de dados em geral
- Danos de reputação e imagem para a empresa
- Ações judiciais individuais e/ou coletivas por parte dos titulares de dados e de entidades em defesa do consumidor

Dessa forma, se mostra como melhor opção agir de forma preventiva, adotando medidas que evitem que quaisquer tipos de dados estejam vulneráveis.

O CONSUMIDOR PODE PROCESSAR UMA EMPRESA?

Se o consumidor sofrer algum dano referente ao vazamento de seus dados, ele poderá sim, ingressar com uma ação visando à reparação do dano sofrido, seja por danos morais ou materiais.

Diante deste cenário, resta cada vez mais necessário que as empresas busquem a **proteção adequada**, pois poderão sofrer com os custos de ações judiciais e suas condenações.

COMO EVITAR QUE OCORRA O VAZAMENTO DOS DADOS DE CLIENTES?

Sem dúvidas, a melhor forma de evitar o vazamento dos dados de clientes é o investimento em segurança da informação e a melhoria destes sistemas dentro das empresas.

Dessa forma, além de evitar o acesso aos dados por pessoas não autorizadas, a empresa

também estará de acordo com o previsto na LGPD.

Neste sentido, algumas medidas que as empresas podem adotar para garantirem a segurança são:

- Investimento em ferramentas de prevenção a ameaças, como antivírus e firewall
- Estabelecer políticas internas e ferramentas de controle e autenticação de acesso
- Manter sempre atualizados os sistemas e softwares
- Realizar análises de vulnerabilidade e segurança dos sistemas
- Promover campanhas de conscientização e treinamento de seus colaboradores e gestores
- Criar políticas internas e externas de segurança da informação

Assim, estas são as principais dúvidas sobre o **vazamento de dados**. Gostou do conteúdo e quer aprender mais sobre o universo do Direito? Continue acompanhando nosso blog e siga nosso Instagram.