

# 1. Artigos da LGPD Violados (em um cenário de falha de segurança)

Considerando que o Mega Vazamento de Dados expôs informações de praticamente toda a população brasileira, e presumindo uma falha na segurança ou na gestão dos dados por parte do(s) agente(s) de tratamento responsável(is), os principais artigos da LGPD (Lei nº 13.709/2018) que teriam sido violados são:

- **Art. 6º, VI (Princípio da Segurança):** O tratamento de dados pessoais deve garantir a **segurança** dos dados, protegendo-os de acessos não autorizados, acidentais ou ilícitos de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. A ocorrência de um vazamento em massa sugere que medidas de segurança adequadas não foram implementadas ou falharam.
  - **Art. 6º, VII (Princípio da Prevenção):** O tratamento de dados deve adotar medidas para **prevenir** a ocorrência de danos em virtude do tratamento de dados pessoais.
  - **Art. 46 (Dever de Segurança):** Os agentes de tratamento de dados (Controlador e Operador) devem adotar **medidas de segurança, técnicas e administrativas** aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. O vazamento indica uma falha neste dever.
  - **Art. 42 (Responsabilidade):** O Controlador ou o Operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados, é **obrigado a repará-lo**.
- 

## 2. Responsabilidades da Empresa após a Descoberta do Vazamento

De acordo com a LGPD, o agente de tratamento (o Controlador, que toma as decisões sobre o tratamento dos dados) possui responsabilidades claras e imediatas após tomar conhecimento de um incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

### Comunicação Obrigatória (Art. 48)

O **Controlador** tem o dever de comunicar o incidente:

1. **À Autoridade Nacional de Proteção de Dados (ANPD):**
  - A comunicação deve ser feita em **prazo razoável**, conforme definido pela ANPD (atualmente, o Regulamento da ANPD estabelece um prazo de **dois dias úteis** a partir da data do conhecimento).
  - O comunicado deve, no mínimo, descrever: a natureza dos dados afetados, as informações sobre os titulares envolvidos, as medidas de segurança

utilizadas, os riscos gerados pelo incidente e as medidas que foram ou serão adotadas para reverter ou mitigar os efeitos do prejuízo.

**2. Ao Titular de Dados Afetados:**

- A comunicação deve ser feita de forma **clara e acessível**, e deve ser realizada imediatamente.
- Deve conter, no mínimo: os dados de contato do Encarregado, a descrição da natureza dos dados pessoais afetados, a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, os riscos relacionados ao incidente e as medidas que foram ou serão adotadas.

## Outras Responsabilidades

- **Comunicação ao Encarregado (DPO):** Se houver um Operador envolvido, este deve comunicar o incidente ao Controlador, e o Controlador deve informar o seu **Encarregado (DPO)** para que ele possa atuar na coordenação da resposta ao incidente e na comunicação com a ANPD.
- **Documentação e Mitigação (Art. 6º, X):** A empresa deve **documentar** toda a avaliação interna do incidente, as medidas corretivas e de mitigação de danos adotadas, para fins de cumprimento do princípio da **responsabilização e prestação de contas** (*Accountability*).
- **Adoção de Medidas:** Implementar ações imediatas para **conter o vazamento**, investigar a causa raiz, e adotar medidas para evitar a reincidência.

---

## 3. Penalidades Aplicáveis pela ANPD (Art. 52 da LGPD)

De acordo com o Art. 52 da LGPD, em caso de descumprimento, a Autoridade Nacional de Proteção de Dados (ANPD) pode aplicar as seguintes sanções aos agentes de tratamento:

Penalidade	Detalhamento
<b>Advertência</b>	Com indicação de prazo para adoção de medidas corretivas.
<b>Multa Simples</b>	<b>Até 2% do faturamento</b> da empresa (ou grupo) no Brasil no seu último exercício, <b>limitado</b> no total a <b>R\$ 50.000.000,00 (cinquenta milhões de reais)</b> por infração.
<b>Multa Diária</b>	Imposição de multa por dia de descumprimento, observando o limite total de R\$ 50 milhões.
<b>Publicização da Infração</b>	Divulgação da infração após devidamente apurada e confirmada. O objetivo é dar <b>publicidade</b> à falha, gerando um forte <b>dano reputacional</b> .
<b>Bloqueio dos Dados</b>	Suspensão temporária do tratamento dos dados pessoais a que se refere a infração.

<b>Eliminação dos Dados</b>	Determinação de eliminação dos dados pessoais a que se refere a infração.
<b>Suspensão Parcial</b>	Suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses (prorrogável).
<b>Suspensão Total da Atividade</b>	Suspensão da atividade de tratamento de dados pessoais pelo período máximo de 6 (seis) meses (prorrogável).
<b>Proibição Parcial/Total</b>	Proibição total ou parcial de exercer atividades relacionadas a tratamento de dados.

A aplicação da penalidade é determinada com base na gravidade da infração, no tipo de dados vazados (pessoais ou sensíveis), na boa-fé do infrator, na adoção de medidas corretivas e na cooperação com a ANPD, entre outros fatores. Em um caso de mega vazamento, as multas e as sanções de publicização/bloqueio/eliminação seriam as mais prováveis.