LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

GUIA RÁPIDO

ZG
ZAVAGNA GRALHA
ADVOGADOS

SUMÁRIO

01. **INTRODUÇÃO**
p. 3

02. **OBJETIVOS DA LEI**
p. 4

03. **PRINCIPAIS CONCEITOS DA LGPD**
p. 5

04. **PRINCÍPIOS DO TRATAMENTO DE DADOS**
p. 6

05. **HIPÓTESES DE TRATAMENTO**
p. 7

06. **PERSONAGENS**
p. 9

07. **RESPONSABILIDADE E INDENIZAÇÃO PELOS DANOS**
p. 12

08. **PASSOS PARA A IMPLEMENTAÇÃO DA LGPD**
p. 14

INTRODUÇÃO

A Lei Geral de Proteção de Dados Pessoais (LGPD), embora tenha surpreendido muitas pessoas, foi construída a partir de consenso internacional que se desenhava há anos sobre a necessidade de proteção da privacidade e garantia de direitos individuais na internet.

A conhecida revolução tecnológica e digital permitiu novas formas de interação entre as pessoas e entre os ambientes. As tecnologias de captura de informações e a própria "internet das coisas", presentes tanto nos espaços públicos quanto nos espaços privados, promoveram a digitalização de uma grande quantidade de dados relacionados à atividade humana. O volume de dados mundial é atualmente composto por 33 trilhões de gigabytes e estimado em 175 trilhões de gigabytes para 2025. Aliado a ferramentas de big data, esse volume permite detectar traços do mundo físico, como transações, movimentações financeiras, tráfego, preferências de consumo, localização, entre tantos outros.

Essa realidade permite o processamento, a mineração e a análise de dados em uma escala exponencial, enquanto os mercados relacionados a essas tecnologias vêm se expandindo. No entanto, no plano dos indivíduos e da privacidade, os reflexos dessas mudanças não são tão favoráveis. A falta de conhecimento, transparência, segurança e controle destes dados e dos fins para os quais estão sendo utilizados leva à necessidade de uma regulamentação.

Os recentes escândalos envolvendo dados pessoais, como os casos Snowden e Cambridge Analytica, evidenciaram a necessidade de atenção para o assunto e promoveram grandes mudanças no cenário mundial. De forma concreta, é possível observar que, no plano internacional, a proteção dos dados pessoais se tornou uma exigência tanto no âmbito privado quanto no público. A General Data Protection Regulation (GDPR), implementada em 2018 pela União Europeia, é um exemplo das exigências relativas à proteção de dados pessoais ultrapassando as fronteiras nacionais.

É nesse contexto que o Brasil, adotando uma tendência global, promulgou a LGPD, ainda que de forma tardia, promovendo o tema da proteção de dados pessoais e instituindo a privacidade como um direito individual garantido aos seus cidadãos.

OBJETIVOS DA LEI

A LGPD busca alcançar três objetivos principais:

Criar regras e obrigações claras sobre o tratamento de dados pessoais;

Tutelar os direitos fundamentais de liberdade e privacidade do titular;

Promover o livre desenvolvimento da personalidade da pessoa natural.

Por meio da LGPD, institui-se os padrões de proteção de dados e regulação dos direitos e obrigações dos personagens envolvidos na proteção de dados pessoais. Para tanto, a lei adotou standards internacionais de proteção de dados, inclusive incorporando ensinamentos da GDPR.

Diante da nova regulamentação, dos deveres e das obrigações criadas pela LGPD, o indivíduo passa a poder exercitar direitos em relação aos dados pessoais dos quais é titular e conquista maior controle e transparência na relação com os controladores desses dados. A regulamentação permite aos titulares dos dados pessoais opor estes direitos por meio de procedimentos exigidos pela lei.

A LGPD, promovendo os dados pessoais a uma extensão da personalidade dos titulares, consagra a autonomia em relação ao principal direito de personalidade: a liberdade de tomar suas próprias decisões no que diz respeito a sua individualidade. O titular é garantido de dispor dos seus dados pessoais como bem lhe aprouver ou, ao menos, tomar ciência do que está sendo feito, a finalidade e a forma como seus dados pessoais estão sendo tratados.

Esses objetivos são também um retrato da realidade brasileira em termos de conscientização e práticas relativas à proteção dos dados pessoais. Em levantamento recente, o SERASA EXPERIAN apontou que cerca de 85% das empresas entrevistadas não estariam prontas para as exigências da lei.

Nessa mesma linha, apesar dos casos notórios de vazamento de dados pessoais e de uma atuação incipiente do judiciário quanto ao tema em termos de direitos do consumidor, no Brasil, não há confiabilidade na proteção de dados pessoais e na segurança da informação. Bem verdade, apenas 1% dos consumidores não tem nenhuma preocupação com este tipo de aspecto (SERASA).

PRINCIPAIS CONCEITOS DA LGPD

Para facilitar a compreensão do tema e a proteção de dados pessoais, a LGPD definiu alguns conceitos-chave. Veja abaixo os mais relevantes:

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável (teoria expansionista). Alguns exemplos de dado pessoal: nome e sobrenome, CPF, RG, endereço, e-mail, IP, imagens de vídeo, gravações de voz etc.;

Dado pessoal sensível: é uma subdefinição de dado pessoal relacionada às características próprias destes dados pessoais, quais sejam 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;

Tratamento de dados: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

TRATAMENTO DE DADOS É TODA OPERAÇÃO REALIZADA COM DADOS PESSOAIS

PRINCÍPIOS DO TRATAMENTO DE DADOS

A LGPD elenca os princípios que deverão nortear o tratamento de dados pessoais. Veja quais são e o que significam:

FINALIDADE: propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

ADEQUAÇÃO: compatibilidade do tratamento com as finalidades informadas ao titular;

NECESSIDADE: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

LIVRE ACESSO: consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

QUALIDADE DOS DADOS: exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

TRANSPARÊNCIA: informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

SEGURANÇA: utilização de medidas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

PREVENÇÃO: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

NÃO DISCRIMINAÇÃO: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

HIPÓTESES DE TRATAMENTO

QUANDO EU POSSO TRATAR DADOS?

A LGPD, visando manter a transparência e o uso apenas dos dados pessoais necessários, determina que o tratamento só pode ocorrer quando uma das hipóteses abaixo ocorrerem.

- Execução de **contrato**;
- Exercício regular de direito em **processo judicial, administrativo ou arbitral**;
- Cumprimento de **obrigação legal/ regulatória**;
- Execução de **políticas públicas**;
- Órgãos de **pesquisa/estudo**;
- Proteção do **crédito**;
- Proteção à **vida**;
- Tutela da **saúde**;
- **Legítimo interesse**: neste caso é muito importante que seja realizado previamente um teste legítimo interesse.
- **Consentimento**: deverá ser sempre livre, inequívoco e informado.

Em outras palavras, o consentimento deverá ser qualificado e apresentar algumas características especificas:

- Não pode haver qualquer vício de vontade e deverá ser oriundo de uma **ação positiva do titular**. A lei não admite consentimento tácito ou por omissão;
- Sem **manipulação ou indução da pessoa a aceitar**, o que deve ser demonstrável por meio de qualquer prova; e
- **Transparência**, clareza, precisão e facilidade de acesso às informações sobre o tratamento de dados.

As chamadas bases legais de tratamento são reduzidas e ainda mais específicas para o tratamento dos dados pessoais sensíveis, como mostra abaixo:

- **Consentimento**: forma específica e destacada, para finalidades específicas;
- Cumprimento de **obrigação legal** ou regulatória pelo controlador;
- Execução de **política pública**;
- Proteção a **vida**;
- Exercício regular de direitos, em contratos e em **processos judiciais**;
- Tutela da **saúde**;
- Prevenção à **fraude** e à **segurança** do titular.

LEMBRANDO que quando o dado pessoal pertencer a uma criança ou adolescente o tratamento deverá ser sempre realizado em seu melhor interesse e as informações relativas a este tratamento devem ser de fácil compreensão ao público infantojuvenil. O consentimento, nesse caso, deverá se dar de forma específica e em destaque, por pelo menos um dos pais do menor ou pelo responsável legal.

PERSONAGENS

A regulação da LGPD gira em torno de quatro figuras principais: o **titular**, os **agentes de tratamento** (controlador e operador), o **encarregado** (ou DPO – Data Protection Officer) e a **Autoridade Nacional de Dados**.

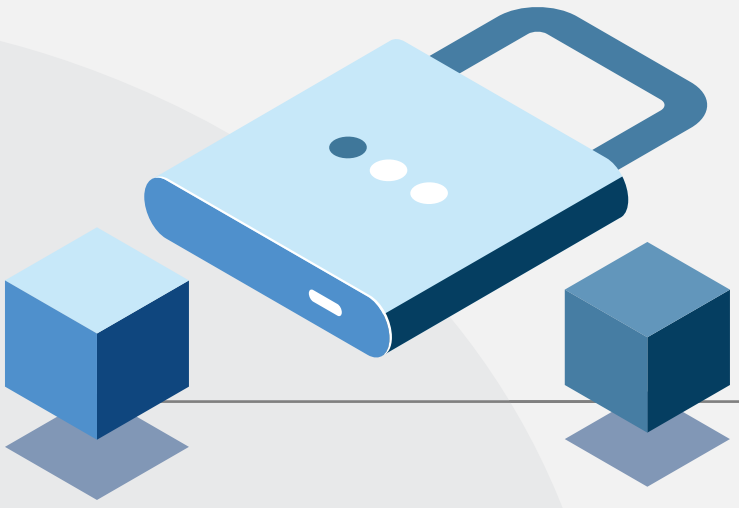
Titular

O titular é qualquer pessoa natural a quem os dados pessoais se referem. Os dados pessoais tratados podem estar ligados a pessoa diretamente, quando a pessoa é explicitamente identificada, ou indiretamente, sem associação explícita com a pessoa, mas que torna possível a sua identificação por meio de inferência.

Direitos do titular

A LGPD coloca o titular no centro de controle dos seus próprios dados, atribuindo a ele os seguintes direitos em relação a quem os controla:

- Confirmação da existência do tratamento;
- Acesso aos dados;
- Correção dos dados incompletos, inexatos ou desatualizados;
- Eliminação de dados desnecessários ou tratados em desconformidade a Lei;
- Informação sobre o uso e compartilhamento dos dados;
- Oposição ao tratamento;
- Portabilidade a outro fornecedor de serviço ou produto;
- Revogação do consentimento;
- Revisão de decisões automatizadas (por exemplo: profiling de crédito e de consumo ou aspectos de sua personalidade).



Agentes de Tratamento

São as pessoas naturais ou jurídicas que decidem sobre ou realizam o tratamento de dados pessoais. Sobre eles a LGPD impõe uma série de deveres e obrigações que visam garantir os direitos do titular.

Controlador

É a organização a que competem as decisões referentes ao tratamento de dados pessoais. Em regra, será a empresa diretamente responsável por fornecer o produto e serviço ao consumidor. Sobre eles recaem os principais deveres e obrigações da Lei, dentre os quais:

- Tratar o dado sempre dentro de uma das hipóteses legais e observando os princípios de tratamento elencados no artigo 6º da LGPD;
- Provar que o consentimento foi obtido em conformidade com LGDP (Art. 8º, §2º);
- Comunicar à ANPD e ao titular incidentes de segurança que possam acarretar risco relevante aos titulares (art. 48);
- Informar o titular caso haja alguma alteração na finalidade da coleta de dados (Art. 8º, §6º);
- Verificar a observância das instruções e das normas sobre proteção de dados pelo operador (art. 39);
- Obter consentimento específico do titular para compartilhar dados com outros controladores, caso não houver outra base legal (Art. 7º, § 5º);
- Elaborar relatório de impacto à proteção de dados, quando requerido pela ANPD (Art. 38);
- Adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais quanto à Confidencialidade, Integridade e Disponibilidade (art. 46);
- Adotar de regras de boas práticas e governança em privacidade (art. 50);
- Manter registro das operações de tratamento que realizarem (Art. 37);

Operador

É a organização que realiza o tratamento de dados pessoais em nome do controlador. Em geral, são empresas terceirizadas que prestam serviço ao controlador e necessitam, para tanto, utilizar os dados pessoais coletados por ele. Assim como o controlador, o operador possui uma série de obrigações legais, mesmo que em menor medida, entre elas:

- Manter registro das operações de tratamento que realizarem;
- Realizar o tratamento segundo as instruções lícitas fornecidas pelo controlador;
- Adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais quanto à Confidencialidade, Integridade e Disponibilidade (art. 46);
- Adotar de regras de boas práticas e governança em privacidade (art. 50);
- Responder solidariamente com o controlador pelos danos causados ao titular quando descumprir a legislação de proteção de dados ou quando e não tiver seguido as instruções lícitas do controlador.

Encarregado (DPO – Data Protection Officer)

O DPO é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

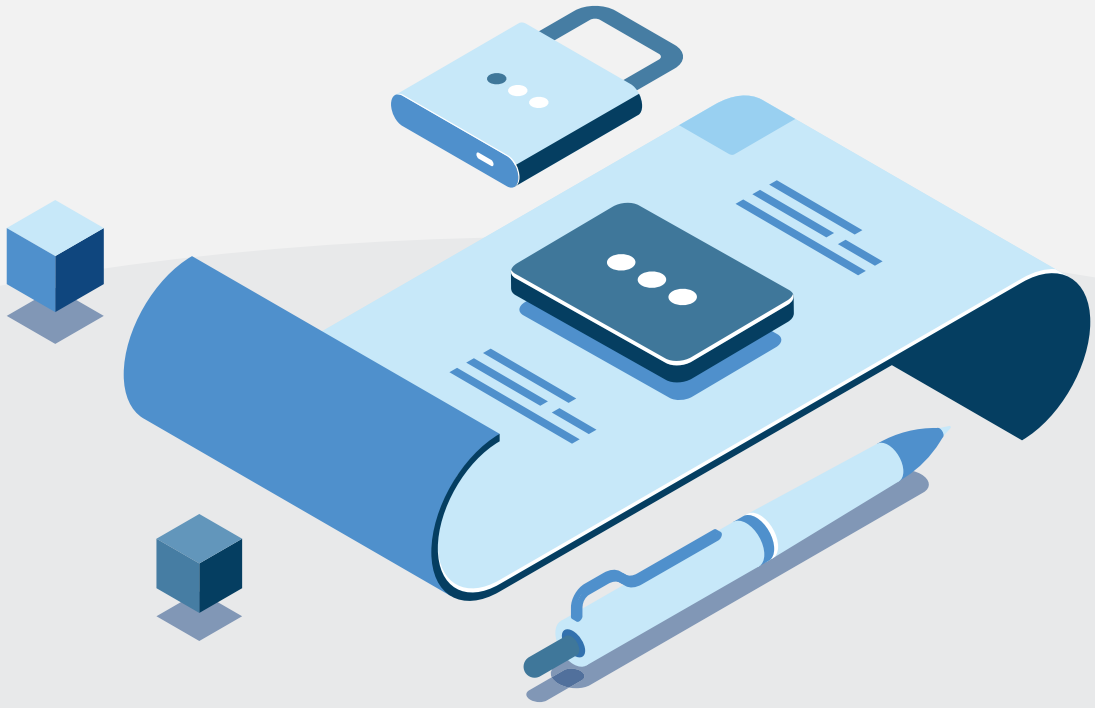
O controlador deverá indicar encarregado pelo tratamento de dados pessoais, que pode ser uma pessoa física ou jurídica, interna ou terceirizada.

Caberá ao Encarregado aceitar reclamações e comunicações dos titulares e da ANPD, prestar esclarecimentos e adotar providências, assim como orientar os funcionários e os contratados da organização a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.

Autoridade Nacional de Proteção Dados

A Autoridade Nacional de Proteção de Dados (ANPD) é o órgão da administração pública responsável, dentre outras atribuições, por:

- Zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional;
- Editar normas para regulamentar a aplicação da LGPD;
- Aplicar as sanções administrativas previstas na LGPD.



SANÇÕES E RESPONSABILIDADE PELOS DANOS AO TITULAR

Responsabilidade civil pelos danos

A empresa, controladora ou operadora de dados, é obrigada a reparar dano causado ao titular, em decorrência da violação à legislação de proteção de dados pessoais.

Nas relações de consumo, também são aplicáveis o Código de Defesa do Consumidor para fins de responsabilidade, isto é, haverá a obrigação de indenizar o dano pelo tratamento indevido mesmo que se ausente a culpa do controlador.

Vale lembrar que a própria LGPD delimita algumas hipóteses em que os agentes de tratamento não serão responsabilizados judicialmente. Isso ocorrerá quando: (i) não realizaram o tratamento de dados pessoais que lhes é atribuído, (ii) não houve violação à legislação de proteção de dados, embora tenham realizado o tratamento que lhe é atribuído, e (iii) o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Penalidades administrativas

Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas na Lei, ficam sujeitos às sanções administrativas aplicáveis pela ANPD. Embora associados, não é necessária a ocorrência de um incidente de segurança ou de um vazamento de dados para que a agência nacional aplique as penalidades, basta o descumprimento das diversas exigências legais.

AS EMPRESAS SÃO OBRIGADAS A REPARAR DANOS CAUSADOS AO TITULAR EM DECORRÊNCIA DA VIOLAÇÃO À LEGISLAÇÃO DE PROTEÇÃO DE DADOS

As sanções previstas em lei, em razão das infrações cometidas à LGPD, são:

- Advertência;
- Multa simples, de até 2% (dois por cento) do faturamento no seu último exercício, limitada, no total, a R$ 50 milhões de reais por infração;
- Multa diária, observado o limite total a que se refere ao item anterior;
- Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- Eliminação dos dados pessoais a que se refere a infração.

Como a ANDP irá dosar a penalidade imposta?

O Valor da Sanção (VS) será diretamente proporcional a: (i) gravidade e natureza das infrações e dos direitos pessoais afetados; (ii) vantagem auferida ou pretendida pelo infrator; (iii) condição econômica do infrator; (iv) a reincidência; (v) o grau do dano; e a (vi) gravidade da falta.

Por outro lado, Valor da Sanção (VS) será inversamente proporcional a: (vii) boa-fé do infrator; (viii) a cooperação do infrator; (ix) a adoção de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados; (x) a adoção de política de boas práticas e governança; (xi) a pronta adoção de medidas corretivas.

Poderíamos resumir os critérios acima na seguinte fórmula:

VS= (i) (ii) (iii) (iv) (v) (vi) / (vii) (viii) (ix) (x) (xi)

Isso quer dizer que a gravidade ou valor do sansão sempre será analisado no caso concreto com base em diversos critérios.
Se o controlador dos dados demonstrar que tomou as medidas adequadas e em conformidade com a LGPD, em que pese ter ocorrido algum incidente de segurança, a pena aplicada deverá ser menos rígida. Por outro lado, se não tomou medida alguma para evitar que o incidente acontecesse, pode ter sua penalidade aumentada.

PASSOS PARA A IMPLEMENTAÇÃO DA LGPD

Como a LGPD determina as exigências para a conformidade, mas não ensina como colocá-los em prática, elaboramos um plano com as principais etapas para auxiliar sua empresa na implementação.

Fase 1: Planejamento e Preparação

Objetivos:
Organizar e engajar a empresa para a LGPD, mapear os dados, avaliar os riscos

a. Formação de um Comitê e Grupo de Trabalho

b. Apresentação do projeto e cronograma

c. Treinamentos de conscientização em SegInfo e LGPD

d. GAP analysis

e. Entrevistas com os responsáveis de cada processo

f. Mapeamento dos dados (incluindo inventário e classificação dos dados dos dados)

g. Análise de risco

h. Plano de Implementação

Fase 2: Operação e Implementação

Objetivo:
Iimplementar controles operacionais
e documentais compatíveis com LGPD

a. Medidas técnicas (SegInfo e TI)

- Encriptação e anonimização dos dados quando necessário
- Implantação de controles de acesso e permissões adequadas
- Mecanismos de monitoramento e prevenção de perdas de dados
- Armazenamento de logs
- Ferramentas de gestão do consentimento/pedidos do titular
- Etc.

b. Medidas organizacionais (jurídicas e documentais)

- Avaliar a pertinência e a base legal do tratamento dos dados
- Redação e revisão dos contratos que envolvam tratamento de dados
- Elaboração de Política de Privacidade
- Elaboração de Políticas de Segurança da Informação
- Documentar todo processo de compliance
- Criar plano de repostas a incidentes
- Elaboração de Relatórios de Impacto de Proteção de Dados (DPIA)
- Etc.

Fase 3: Continuidade e Atualização

Objetivo:
Garantir a manutenção da conformidade com a LGPD

a. Revisão pós-projeto

b. Garantir meios de prestação de contas

c. Testes de segurança e vulnerabilidades

d. Auditorias constantes

e. Inclusão da privacidade na rotina (privacy by design)

REFERÊNCIAS BIBLIOGRÁFICAS

Lei Geral de Proteção de Dados Pessoais - Lei Nº 13.709, de 14 de agosto de 2018.

ABNT NBR ISO/IEC 27001:2013 - Sistemas de Gestão de Segurança da Informação.

ABNT NBR ISO/IEC 27002:2013 – Código de Prática para a Gestão de Segurança da Informação.

ABNT NBR ISO/IEC 27005:2011 – Gestão de Riscos em Segurança da Informação.

ISO/IEC 27701:2019 – Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines.

IT Governance. GDPR – An Implementation and Compliance Guide, 2017.

VOIGT, Paul; VON DEM BUSSCHE, Axel. The Eu general data protection regulation (GDPR). A Practical Guide, 1st Ed., Cham: Springer International Publishing, 2017.

PMI (Project Management Institute). Project Management Body of Knowledge – PMBOK. 5 ed.

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

GUIA RÁPIDO

ZG
ZAVAGNA GRALHA
ADVOGADOS