LEI GERAL DE **PROTEÇÃO DE DADOS**

Trata-se de *material gratuito* que não substitui assessoria jurídica e nem tem por finalidade esgotar os temas da Lei Geral de Proteção de Dados. Essa apresentação visa tão somente apresentar os conceitos básicos da lei.

Introdução

>> A preocupação pela preservação da privacidade não é nova. Nasceu com a própria sociedade e sempre foi importante para a harmonia social. Mesmo não sendo uma noção recente, somente no final do séc. XIX o direito à privacidade começou a ser objeto de normatização.

>> O termo "direito à privacidade" surgiu no mundo jurídico com o artigo escrito por Samuel Warren e Louis Brandeis, publicado em 1890 na Harvard Law Review. Define o direito à privacidade como o direito de ser deixado só "right to be let alone".

>> "Com o desenvolvimento da tecnologia, passa a existir um novo conceito de privacidade" (REsp 1168547/RJ – Min. LUIS FELIPE SALOMÃO).

>> No Brasil, além da **LGPD**, a privacidade é protegida por diversas fontes, dentre as quais destacamos a **Constituição Federal (CF/88)**, o **Código de Defesa do Consumidor, a Marco Civil da Internet** (Lei 12.965, de 2014) e sua regulamentação (Decreto 8.771, de 2016), a **Lei do Cadastro Positivo** (Lei Complementar 166, de 2019) e a **Lei de Acesso à Informação** (Lei 12.527, de 2011).

Está em apreciação uma Proposta de Emenda à Constituição (17/2019) que inclui a proteção de dados pessoais na lista das garantias individuais da Constituição Federal.

Linha do tempo da LGPD:

- 2010 – Primeira Consulta Pública
- 2015 – Segunda Consulta Pública
- 2018 – Evolução Política Global (GDPR, caso da Cambridge Analytics)
- 2018 – Aprovada LGPD
- 2020 – Vigência da LGPD

Linha do tempo do GDPR:

- 1980 – Convenção 108/1980
- 2002 – Diretiva 2002/58/CE
- 2018 – GDPR

EUA:

>> Right to Privacy reconhecido pela Suprema Corte.
>> Privacy Act 1974
>> CCPA

A quem se aplica?

A LGPD se aplica a tratamento de dados pessoais realizados em meio digital ou analógico.

A finalidade da LGPD não é prejudicar a atividade econômica ou dificultar o tratamento dos dados.

O foco é proteger os direitos dos titulares e orientar os agentes de tratamento.

A Lei Geral de Proteção de Dados Pessoais será aplicada:

- Pessoa jurídica de direito público ou privado que realize o tratamento de dados pessoais.
- Pessoa natural com exceção daquela que trata dados pessoais para fins particulares e não econômicos.

Aplicação territorial:

- Operação de tratamento de dados no território nacional.
- Atividade de tratamento de dados que ofereça bens ou serviços localizados no território nacional.
- Dados pessoais que tenham sido coletados no território nacional.

Exceções de Aplicação:

- Para fins exclusivamente jornalísticos, artísticos ou acadêmicos.
- Particulares sem uso econômico.
- Tratamentos que visem à segurança pública, defesa nacional, segurança do Estado ou atividades de prevenção e repressão criminal.
- A LGPD não se aplica provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

Princípios previstos na Lei Geral de Proteção de Dados

O artigo 6° da LGPD reúne os princípios que devem ser observados em todo o ciclo de tratamento dos dados pessoais:

- ✓ **RESPONSABILIDADE E PRESTAÇÃO DE CONTAS (ACCOUNTABILITY):** Demonstração de medidas eficazes ao cumprimento das normas.
- ✓ **NÃO DISCRIMINAÇÃO:** Os dados pessoais não podem ser utilizados de forma discriminatória, ilícita ou abusiva.
- ✓ **TRANSPARÊNCIA:** As informações devem claras e precisas aos titulares.
- ✓ **SEGURANÇA:** Deve ser garantido o uso de medidas técnicas e administrativas aptas a proteger os dados pessoais de extravios, invasões, transmissões ou modificações.
- ✓ **PREVENÇÃO:** Devem ser adotadas medidas para evitar danos aos titulares.
- ✓ **QUALIDADE DOS DADOS:** Os dados coletados e tratados devem ser exatos e fiéis.
- ✓ **FINALIDADE:** Os dados pessoais devem ser tratados com propósitos legítimos e informados. Sempre que possível o titular deverá ter conhecimento prévio do tratamento.
- ✓ **ADEQUAÇÃO:** Devem ser tratados apenas os dados compatíveis com as finalidades informadas ao titular
- ✓ **NECESSIDADE OU MINIMIZAÇÃO:** Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos.
- ✓ **LIVRE ACESSO:** Garantia, aos titulares, de consulta facilitada e gratuita obre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

AUTODETERMINAÇÃO INFORMATIVA: A autodeterminação informativa decorre dos princípios da finalidade e transparência. Em síntese, a autodeterminação informativa é um dos fundamentos da LGPD, garantindo ao titular o direito de controle sobre o tratamento dos seus dados.

Tipos de dados

O artigo 5° da LGPD traz os conceitos básicos da lei. Veja:

Tratamento:

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.

DADO PESSOAL:
informação relacionada a pessoa natural identificada ou identificável. Trata-se do **conceito expansionista**, alongando a qualificação dos dados. Ex.: CPF, RG, nome, título de eleitor, número da CNH, hábito de consumo, idade, profissão.

X

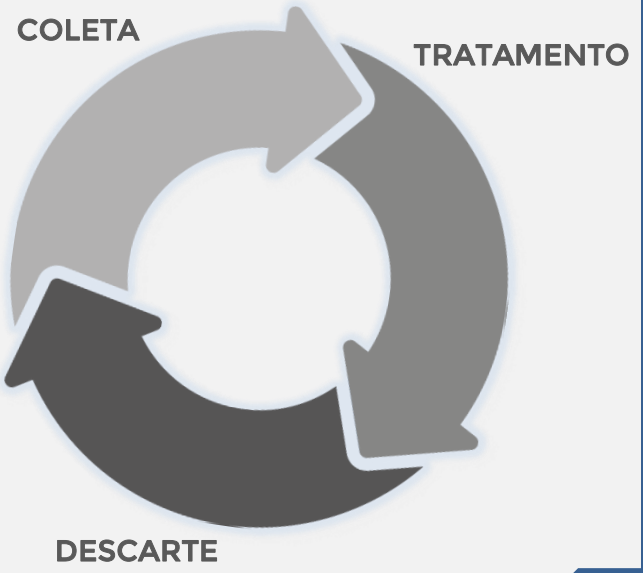
DADO PESSOAL SENSÍVEL:
dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

DADO ANONIMIZADO:
dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

X

DADOS PSEUDOANOMIZADO:
É o dado que perde a possibilidade de ser associado direta ou indiretamente a uma pessoa. No entanto, existem meios para reverter o mecanismo utilizado. Será considerado dado pessoal. **Ex.:** Criptografia.

O tratamento deve obedecer a um **ciclo de descarte.**



Controlador, Operador, Titular

Os agentes de tratamento são o controlador e o operador.

CONTROLADOR

pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

OPERADOR

pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. O operador sempre obedecerá ao controlador.

TITULAR

pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Microssistema legislativo:

Pilares de um programa de **proteção de dados:**

Direitos dos Usuários

Previstos nos artigos 17 ao 22 da LGPD, os direitos dos titulares são:

>> Confirmação sobre a existência de tratamento e acesso aos dados pessoais.

Por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

>> Correção de dados incompletos, inexatos ou desatualizados.

>> Informação sobre com quais entidades o controlador compartilha os dados.

>> Portabilidade dos dados a outro controlador/fornecedor de produtos ou serviços, não incluindo os dados anonimizados.

>> Oposição a tratamento irregular.

>> Eliminação dos dados pessoais.

>> Revogação do consentimento.

>> Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD.

>> Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.

>> Direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.

Os direitos previstos na LGPD serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.

A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente.

Bases legais para o tratamento dos dados

As bases legais ou requisitos para o tratamento dos dados pessoais estão previstas nos artigos 7° (dados pessoais) e 11 (dados pessoais sensíveis) da LGPD.

Para que os dados sejam tratados de forma lícita, o tratamento deverá ser enquadrado em pelo menos uma das bases legais.

A estratégia de implementação deve ser baseada nas exceções do consentimento, isso porque o consentimento é revogável a qualquer momento.

ATENÇÃO: Não há hierarquia entre os dados pessoais e dados pessoais sensíveis.

Base legal para tratamento de dados pessoais:

- **Consentimento** do titular.
- **Cumprimento** de obrigação legal ou regulatória.
- **Execução** de políticas públicas pela Administração Pública.
- **Realização** de estudos por órgãos de pesquisa.
- **Tutela** da saúde, somente por profissionais da saúde.
- **Proteção** de crédito.
- **Proteção** da vida ou da incolumidade física do titular.
- **Exercício** regular de direitos, inclusive em contrato e processo judicial, administrativo ou arbitral.
- **Para** a execução de contratos e procedimentos a eles relacionados.

Base legal para tratamento de dados pessoais sensíveis:

- **Consentimento** (preferencialmente).
- **Cumprimento** de obrigação legal ou regulatória.
- **Execução** de políticas públicas pela Administração Pública.
- **Realização** de estudos por órgãos de pesquisa.
- **Tutela** da saúde.
- **Garantia** de prevenção à fraude e à segurança do titular.

Responsabilidade Civil

A Lei Geral de Proteção de Dados, nos seus artigos 42 a 45, estabelece as regras referentes à responsabilidade civil dos agentes de tratamento de dados pessoais.

Embora a Lei Geral de Proteção de Dados não seja clara, o entendimento predominante é o de que a responsabilidade civil é de **natureza objetiva.**

O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem **dano patrimonial, moral, individual** ou **coletivo**, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

O operador **responde solidariamente** pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador se equipara ao controlador, salvo nos casos de exclusão previstos no art. 43 da LGPD.

Os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, **salvo nos casos de exclusão** previstos no art. 43 da LGPD.

Os agentes de tratamento só não serão responsabilizados quando provarem:

1
que não realizaram o tratamento de dados pessoais que lhes é atribuído;

2
que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou

3
que não realizaram o tratamento de dados pessoais que lhes é atribuído;

Data Protection Officer (DPO) - Encarregado

O DPO é 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)

A nomeação de um DPO é uma medida de governança essencial.

A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

A Lei Geral de Proteção de Dados não exige que o encarregado seja empregado do controlador ou operador, sendo possível a terceirização da função, denominada “DPO as a service”.

Entre outras, as atividades relacionadas ao encarregado (DPO) são:

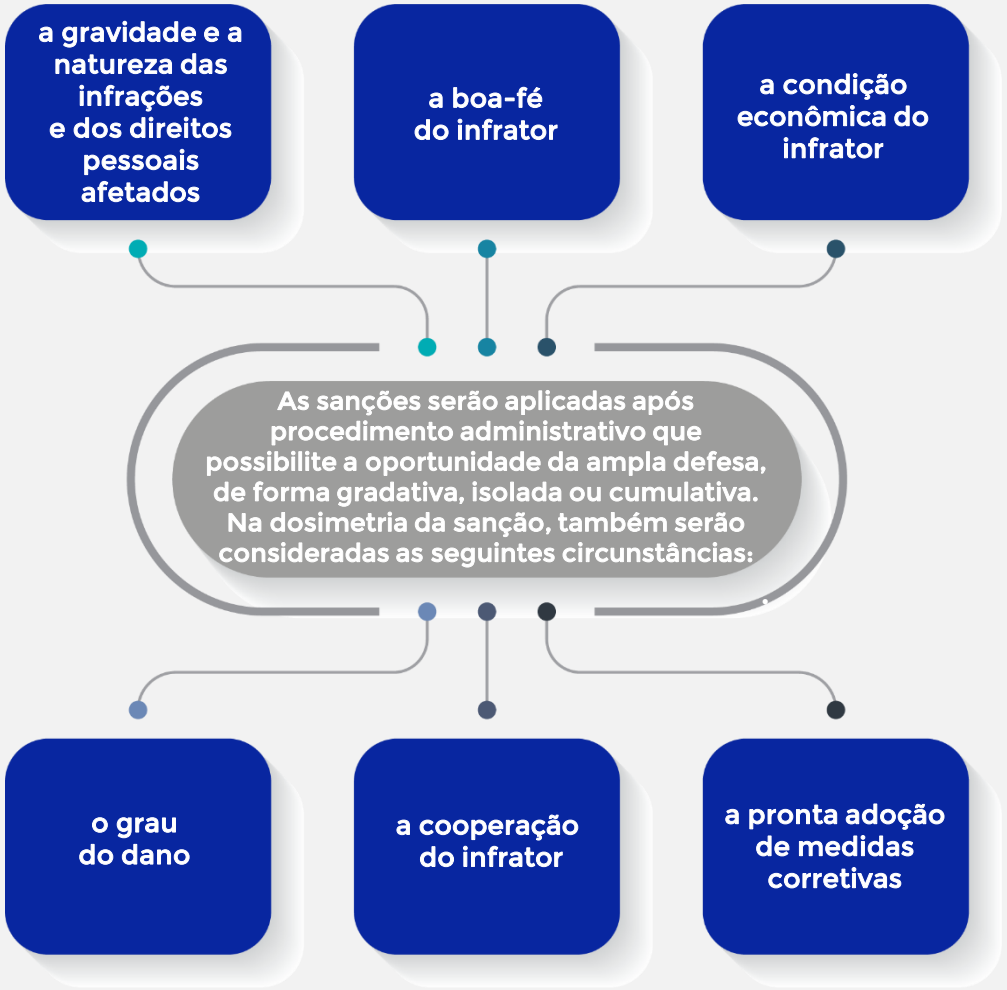
1. aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
2. receber comunicações da autoridade nacional e adotar providências;
3. orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
4. executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Recomenda-se que o DPO seja pessoa diferente da que exerce a função de *compliance officer*.

Sanções previstas na LGPD

Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela Autoridade Nacional de Proteção de Dados:

- advertência, com indicação de prazo para adoção de medidas corretivas
- multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- multa diária, observado o limite total a que se refere o inciso II do artigo 52 da LGPD;
- 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;
- proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.



Casos e multas

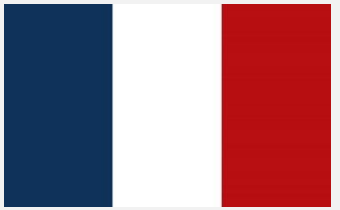
1 **2016**

Uber foi punido com multa de US$ 148 milhões após encobrir vazamento de dados

2 **2019**

British Airways foi punida com multa de 204 milhões de euros por violação às normas de segurança do artigo 32 do GDPR

3 **2019**



Google foi punido com multa de 50 milhões de euros por violar bases legais do GDPR

4 **2020**

A TIM foi punida em 27,8 milhões de euros por violar bases legais do GDPR

5 **2018**

Concessionária do Metrô de SP é processada por painel que faz reconhecimento facial de passageiros (Linha 4/Amarela – Metrô/SP). A ação pede o pagamento de indenização por danos coletivos no valor mínimo de R$ 100 milhões

6 **2019**

Em acordo extrajudicial, a Netshoes pagou R$ 500 mil em danos morais após vazamento de dados

*Conteúdo meramente informativo, sem a intenção de imputar a prática de infrações às empresas mencionadas acima.

Projeto de implementação

O programa de implementação visa mitigar riscos de não conformidade às normas de proteção de dados, o que pode levar a ações de fiscalização e a perda de confiança de parceiros e clientes.

1.º passo

Avaliação e conscientização:

Reunião de kick off para conhecer a empresa e suas principais atividades.

2.º passo

Mapeamento dos dados (Data Mapping):

Conhecer e mapear todos os fluxos de dados pessoais.

3.º passo

Diagnóstico e análise de riscos (Gap Analysis):

Elaborar uma matriz de risco identificando os pontos em desconformidade com a legislação e apontar as correções necessárias.

4.º passo

Planejamento (Prognóstico):

Elaborar o plano de ação com as atividades de mitigação dos riscos.

5.º passo

Implementação do Programa de Governança:

Execução do plano de ação.

6.º passo

Monitoramento e melhoria contínua:

Acompanhar a evolução legislativa e regulatória para que a empresa se mantenha em conformidade, bem como evitar incidentes de segurança.

Privacy by Design: é uma abordagem à engenharia de sistemas que, basicamente, diz que um produto ou sistema precisa ser pensado para proteger os dados dos usuários desde sua concepção. Ou seja, o sistema teria que ser desenvolvido já pensando em salvaguardas e funcionalidades para proteger os dados.

Privacy by Default: o produto ou serviço deve ser lançado e recebido pelo usuário com todas as salvaguardas que foram concebidas durante o seu desenvolvimento, da forma mais restrita possível. Também chamada de privacidade como configuração padrão.

Considerações Finais

Aprovada em agosto de 2018, mas com vigência a partir de agosto de 2020, a LGPD ou Lei Geral de Proteção de Dados é uma lei federal que visa trazer segurança jurídica a respeito de dados pessoais que são compartilhados por meio da internet.

A lei se aplica a diversos segmentos que atuam online, desde *e-commerce* a redes sociais, passando inclusive por organizações governamentais e sociais.

O objetivo central da lei é a segurança dos dados dos usuários, já que sabemos que hoje em dia diversas empresas comercializam, repassam e compartilham informações pessoais obtidas de maneira consensual ou não, o que pode fazer com que um usuário nem saiba exatamente quais dados pessoais estão expostos.

Com a aplicação da LGPD, passa-se a ter uma atenção maior a coleta, gestão e armazenamento dos dados. A lei não vem proibir o uso de dados pessoais, mas impor que eles sejam tratados com justificativa, de forma correta, transparente e com segurança.

Vê-se que as maiores multas aplicadas em decorrência do GDPR decorrem da falta de: implementação de medidas de segurança; de base legal insuficiente para o tratamento dos dados; observância dos princípios do GDPR.

Portanto, o projeto de adequação, além de necessário, deve ser constante, não se esgotando com a mera implementação.

Dicas de documentários e vídeos

- ✓ **Privacidade Hackeada – Documentário da Netflix**
- ✓ **O Dilema das Redes (The Social Dilemma) - Documentário da Netflix**
- ✓ **Por que proteção de dados pessoais importa? Bruno Bioni – TEDxPinheiros (Veja aqui: https://tinyurl.com/y3huukco)**

Ainda não começou? O que **priorizar?**

Publicar uma Política de Privacidade.

Indicar um canal de contato para o exercício dos direitos dos titulares.

Nomear um DPO (Encarregado).

São medidas urgentes que devem ser complementadas por outros instrumentos de governança durante o projeto.

CONTATO

Márcio Pompeu

ADVOGADO

(014) 99133-8059

contato@marciopompeu.com.br

www.marciopompeu.com.br