# LEI GERAL DE PROTEÇÃO DE DADOS LGPD

## O QUE É OBRIGATÓRIO SABER

OAB
MATO GROSSO DO SUL

**Produzido pela Comissão de Estudo e Adequação à LGPD da OAB/MS em parceria com o Litech - Laboratório de Inovação e Tecnologia da OAB/MS sob a Coordenação de Giuliana Borges Assumpção Gattass**

**Autores:**
Anna Flávia Ribeiro Pinheiro, Bruno Eduardo Peixoto Lupoli,
Dayane F N Lupoli, Diogo Ferreira Rodrigues,
Fernando H. B. Alli, Heitor Canton de Matos,
Luiza C. Cavaglieri Faccin, Thiago Gomes da Silva
Luiz F. Espindola Bino

**DIRETORIA OAB-MS**

**Mansour Elias Karmouche**
Presidente

**Gervásio Alves de Oliveira Junior**
Vice-Presidente

**Stheven Razuk**
Secretário Geral

**Eclair Nantes**
Secretária Geral Adjunta

**Marco Aurélio de Oliveira Rocha**
Diretor-Tesoureiro

**Diretoria CAAMS:**

José Armando Amado
Presidente

Silvia Bontempo
Vice-Presidente

Euclydes José Bruschi Júnior
Secretário-Geral

Janaína Pouso
Secretária-Geral Adjunta

César Palumbo Fernandes
Tesoureiro

**Diretoria ESA/MS:**

Ricardo Souza Pereira
Diretor Geral

Marcelo Radaelli Da Silva
Vice-Diretor Geral

Leonardo Basmage P. Machado
Secretário Geral

Elaine Cler
Secretária Geral Adjunta

João Paulo Sales Delmondes
Diretor-Tesoureiro

**Coordenação Editorial**
Valter Jeronymo

**Assistente de Coordenação**
Alyne Rebeca

**Projeto Gráfico**
**Diagramação e Capa**
Life Editora

**Revisão**
Giuliana Borges Assumpção Gattass


**Life Editora**
Rua Américo Vespúcio, 255 - Santo Antonio
CEP: 79.100-470 - Campo Grande - MS
Fones: (67) 3362-5545 - Cel.: (67) 99297-4890
contato@lifeeditora.com.br • **www.lifeeditora.com.br**

Dados Internacionais de Catalogação na Publicação (CIP)

OAB-MS Ordem dos Advogados do Brasil Seccional Mato Grosso do Sul

LGPD - O que é obrigatório saber, OAB-MS. - Campo Grande, MS, Life Editora, 2021.

56p.

ISBN 978-65-5887-136-1

1. Segurança de Dados 2. Proteção de Dados 3. LGPD I. Título

CDD - 340

# SUMÁRIO

# APRESENTAÇÃO

A **Lei Geral de Proteção de Dados Pessoais (LGPD)** desde 2018 já manda recado que vai "chegar chegando", mesmo assim, depois de 18 de setembro de 2020, data em que começou a sua vigência, se iniciou um susto coletivo, especialmente no ambiente empresarial, pois o "será" se tornou "já".

Mesmo quase três anos depois da sua criação, e quase um ano da sua vigência, a Lei Geral de Proteção de Dados e sua implementação envolvem ainda inúmeros questionamentos como "a lei começou mesmo a valer?", "LGPD é só para empresa?", "eu preciso me adequar também?", "quando preciso me adequar?, "mas não é só para empresas de grande porte?", "que documentos preciso ter?", "como pode prejudicar a minha empresa a falta de adequação?" , "quem pode ser DPO?"

Diante de tantas dúvidas existentes nós da CEA LGPD - COMISSÃO DE ESTUDO E ACOMPANHAMENTO DA LEI GERAL DE PROTEÇÃO DOS DADOS E SEGURANÇA DA INFORMAÇÃO da OAB/MS resolvemos somar esforços com o LITECH - Laboratório de Inovação e Tecnologia

Jurídica da OAB/MS, para criação de um e-book, com um texto de fácil compreensão, que possa ser acessado gratuitamente por toda a sociedade com o principal objetivo de ajudar a esclarecer a maioria das dúvidas existentes acerca do tema.

# 1. O QUE É LGPD?

A sigla LGPD refere-se à Lei 13.709/18, Lei Geral de Proteção de Dados, que entrou em vigor no dia 18 de setembro de 2020 para preencher lacunas e substituir mais de 30 diplomas legais que, de forma esparsa, regulamentavam o uso de dados no Brasil.

A LGPD é a primeira norma no ordenamento jurídico brasileiro exclusivamente voltada para a proteção de dados e segurança da informação, suas regras, princípios, conceitos e sanções estão modificando a forma como toda a sociedade trata dados pessoais – tanto no meio físico quanto no meio digital.

Em suma, o objetivo da lei é garantir ao titular de dados mais proteção, segurança e controle sobre seus dados, com a finalidade de evitar o uso indevido ou abusivo dos seus dados por terceiros.

# 2. A QUEM SE APLICA A LGPD?

A LGPD se aplica a qualquer pessoa – seja ela natural (física) ou jurídica, de direito público ou privado – que realize tratamento de dados de pessoas para fins econômicos (isto é, não particulares) de quaisquer natureza, seja online (os obtidos por meio de ferramentas informatizadas e/ou automatizadas) ou off-line (obtidos sem a utilização de ferramentas informatizadas, no meio físico).

A LGPD é aplicável não apenas a quem trata dados no Brasil, mas também àqueles que: *i)* oferecem produtos ou serviços a quem estiver em território brasileiro ou, ainda, àqueles que *ii)* coletam e tratam dados de pessoas localizadas no país.

Assim sendo, a LGPD se aplica tanto a uma ONG quanto a um partido político, a um escritório de advogados quanto a uma clínica de fisioterapia, a uma imobiliária quanto a um(a) MEI, a um órgão público (federal, estadual, municipal e distrital), quanto a um conselho de classe (OAB, CREA, CREFITO, CRM, CRMV etc) ou a qualquer empresa, independentemente do seu modelo de constituição ou do número de funcionários ou ainda do faturamento anual.

# 3. O QUE SÃO DADOS PESSOAIS?

O conceito de dado pessoal constante no texto da LGPD é abrangente, e deve ser entendido como toda a informação relacionada a pessoa natural que a torne identificada ou identificável (inciso I, do art. 5º).

Assim, um dado é considerado pessoal quando ele **permite a identificação, direta ou indireta**, da pessoa natural a que o dado está relacionado, o titular do dado. Podemos citar como exemplos: nome, sobrenome, apelido, data de nascimento, documentos pessoais, endereço, telefone, e-mail, endereço residencial, hábitos de consumo, endereço de IP, dados bancários, entre outros.

A LGPD aborda ainda outros dois tipos de dados, os anonimizados, os sensíveis e os dados de crianças e adolescentes.

# 4. O QUE SÃO DADOS PESSOAIS SENSÍVEIS?

Dado pessoal sensível é todo aquele 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 (inciso II, do art. 5º da LGPD). O rol constante na LGPD acerca dos dados sensíveis é taxativo, ou seja, não permite interpretações extensivas.

Em suma são todos aqueles dados que, além de identificar, também **qualificam** uma pessoa natural e, consequentemente, são dados que podem levar a discriminação de uma pessoa.

# 5. DADOS ANONIMIZADOS?

Se o dado é pessoal, isso significa que existe uma informação vinculada a uma pessoa identificável. Quando o dado passa a ser anônimo, aconteceu uma quebra do vínculo entre o dado e a pessoa, restando apenas uma informação em separado, que não nos permite identificar a quem aquela informação pertence.

Por exemplo: digamos que uma grande empresa varejista resolva usar os dados contidos no seu programa de fidelidade para melhorar a logística da companhia. Você consegue visualizar o que isso significa? Significa que os dados que você forneceu enquanto cliente (para contar com benefícios dados aos consumidores) receberão uma destinação distinta daquela (melhoria da logística) a que você consentiu (programa de fidelidade). Assim, para não ferir a sua privacidade de dados, a empresa deve empregar em seus dados as chamadas *técnicas de anonimização*, fazendo com que o setor de logística tenha acesso apenas às informações necessárias ao serviço, sem que seja possível identificar o cliente por trás daquela informação.

Em resumo, os dados anonimizados são aqueles que necessitam de medidas técnicas para que possam garantir a **desvinculação do indivíduo**.

O dado anonimizado é aquele que, originariamente, era relativo a uma pessoa, mas que passou por etapas que garantiram a desvinculação do mesmo ao seu titular inicial. Se um dado for anonimizado, então a LGPD não se aplicará a ele. Entretanto, um dado só é considerado realmente anonimizado se não permitir que, todos os meios técnicos e outros, possam assim "descobrir" quem era a pessoa titular daquele dado.

Processos de anonimização, contudo, podem ser falíveis. Se de qualquer forma a identificação ocorrer, então não se trata de um dado anonimizado – e sim apenas um dado ***pseudonimizado*** que estará sujeito à LGPD por permitir a identificação do titular.

Apesar do processo de anonimização não ser infalível, é empreitada multifacetada e complexa. Bem por isso, a LGPD incentiva abertamente a anonimização dos dados sempre que possível aos agentes de tra-

tamento, uma vez que dados anonimizados são essenciais para o crescimento da inteligência artificial, da internet das coisas, do aprendizado das máquinas, das cidades Inteligentes e da análise de comportamentos. Se uma organização, pública ou privada, realizar a anonimização de dados pessoais sempre que possível, sem dúvida propiciará o aperfeiçoamento da segurança da informação e gerará, via de regra, mais confiança em seus serviços e aumento de reputação e confiabilidade na marca.

# 6. O QUE É CONSIDERADO TRATAMENTO DE DADOS?

A LGPD considera como 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.

A LGPD estabelece o chamado *ciclo de vida do dado pessoal*, ou seja, *toda operação* realizada desde a coleta até a exclusão do dado é considerada como tratamento de dados. Essa definição é de extrema importância para entender até onde a proteção da LGPD se estende e em quais momentos deve-se proteger os dados pessoais. Sendo assim, o *mero armazenamento* de dados pessoais é considerado tratamento pela lei.

# 7. A QUEM NÃO SE APLICA A LGPD?

A LGPD não se aplica quando o tratamento de base pessoais for feito por uma pessoa física, para fins particulares e não comerciais (a lei só se aplica para pessoa física ou jurídica **que gerencie bases de dados com fins ditos econômicos**).

Também não se aplica a LGPD quando o tratamento de dados ocorre para fins exclusivamente: jornalísticos e artísticos; de segurança pública; de defesa nacional; de segurança do Estado e de investigação e repressão de infrações penais.

A LGPD também não se aplica a dados de fora do Brasil e que não sejam objeto de transferência internacional. Sendo assim, se uma empresa brasileira for contratada por uma empresa europeia para realizar o tratamento de dados pessoais de cidadãos europeus e se os dados, após o tratamento, forem devolvidos para a empresa europeia, não se aplicará a LGPD (nesta hipótese, seriam aplicadas as disposições da Legislação da Europa, o famoso "GDPR": *General Data Protection Regulation*).

# 8. PRINCÍPIOS

Conhecer os princípios que regem uma norma significa conhecer sua essência. Os princípios são os valores que devem reger a interpretação e aplicação da lei.

A Lei 13.709/2018 nasceu com características modernas, considerando a pessoa natural como "fonte de proteção", apontando como fundamentos aqueles prescritos no artigo 2º da própria LGPD *(I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.)*, além de preceitos constitucionais como a liberdade *(art. 5º, caput, da Constituição Federal)*, privacidade (*art.5º, inciso X, da CF)* e o livre desenvolvimento da personalidade *(art. 5º da CF c/c os artigos 11 e 12 do Código Civil)*.

Os princípios esculpidos no art. 6º da LGPD são norteadores da conduta de todos *stakeholders* envolvidos com o tratamento dos dados pessoais. Sua observância é mais que relevante. Em verdade, é uma fonte para ação e o direito.

Vamos destrinchar os princípios previstos em cada inciso do art. 6º da LGPD.

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

O caput impõe a observância da boa-fé. A boa-fé é fonte basilar dos contratos desde sua concepção à execução, conforme já previa o art. 422 do Código Civil. A alusão à boa-fé pela LGPD vislumbra a relação contratual e mercadológica entre as partes, que inicia na coleta e concretiza-se no tratamento dos dados.

> I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

O princípio da finalidade traduz-se em especificidade, ou seja, busca assegurar ao titular que os dados fornecidos não serão utilizados para atividade diversa daquela consentida. A finalidade do tratamento deve movida pelo bom senso, razão, legalidade, bons costumes e boa fé, distanciando-se, portanto, da iniciativa subalterna, emulativa, emocional, ilícita e de má fé. Os propósitos dizem respeito à preocupação da lei em enfatizar o aspecto unívoco do tratamento, ou seja, não admitindo a equivocidade ou ambiguidade. Se o propósito for alterado, deve haver nova, especifica e expressa concordância do titular dos dados.

> II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

O tratamento relata como será a operação dos dados por parte do controlador e operador, limitando a utilização conforme os conceitos estabelecidos na finalidade. Ou seja, é imprescindível que haja uma compatibilidade do tratamento com as finalidades informadas ao titular. Deve haver uma relação lógica entre: a) o tratamento e a finalidade objetivada; b) o tratamento e a comunicação transmitida ao titular; c) a finalidade

almejada e a comunicação transmitida ao titular.

> III - 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;

O princípio da necessidade é nada mais que a limitação da realização do tratamento ao mínimo necessário para a realização de suas finalidades. Quando o controlador e operador trabalham apenas com os dados estritamente necessários, justificam sua operação e limitam sua responsabilidade.

> IV - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

O livre acesso é a garantia de consulta facilitada e gratuita ao titular sobre a forma e a duração do tratamento, bem como sobre a integralidade, de seus dados pessoais. Consentir é importante, porém dar acesso e permitir ao titular saber quanto tempo e que tipo de dados seus são tratados pelo controlador é possibilitar

que o titular exerça a titularidade de seus dados. Quando o dono dos dados pode fiscalizá-los, manuseá-los e ter noção do tempo de tratamento, ele pode decidir e consentir com maior clareza sobre o tratamento.

> V - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

É de suma importância manter a integralidade e autenticidade dos dados, bem como atualização destes para suprir tanto a necessidade de um pronto acesso pelo titular quanto a confirmação do empresário de manter ou não os dados.

> VI - Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

Possibilitar a compreensão da informação é tão importante quanto fornecê-la, sem "juridiquês" ou "tecnês". O titular deve conseguir entender de forma ob-

jetiva as ações que serão realizadas com os dados. O que a LGPD buscou garantir é que pessoas naturais, seja qual for o grau cultural ou de instrução que detenham, possam sem dificuldade compreender do que se trata a informação correspondente, até porque, para que todo o procedimento ocorra, é importante que o titular compreenda o que ocorrerá com os seus dados após tratados.

> VII - Segurança: utilização de medidas 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 difusão;

O inciso VII trata da importância da Gestão da informação, ou seja, aquelas ações administrativas realizadas por meio de métodos, estratégias e ferramentas que analisam as vulnerabilidades para mitigar o risco de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão de dados. A ideia central desse princípio é a de preservar, sempre em ambiente seguro, os dados das pessoas naturais objeto do tratamento.

> VIII - Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

Nota: Entender a implementação LGPD como um programa contínuo da empresa, trará sucesso para prevenção efetiva dos dados

> IX - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

As ações realizadas pelo controlador e operador por meio de máquinas ou processos administrativos não podem induzir ou estabelecer discriminação de qualquer natureza. Aqui o legislador pecou ao não deixar claramente assentado de que "abuso" se referia, mas é razoável entender que pretendeu se referir ao manuseio excessivo ou imoderado dos dados das pessoas naturais.

> X - 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.

O último princípio aduz a obrigação de fato e direito 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. A lei deixa claro que os dados pertencem ao titular e, portanto, não se sustentará uma versão "faz de conta" ou mera averiguação operacional e processual dos dados. O princípio da responsabilização clama a adoção de posturas sérias, técnicas e respeitosas em relação aos dados do tratamento. A lei está valendo. Que se iniciem os jogos.

# 9. BASES LEGAIS

É importante esclarecer: a Lei Geral de Proteção de Dados não veio proibir o uso e o tratamento de dados. Ela veio para organizar a situação.

O uso indiscriminado dos dados pessoais traz um transtorno ao titular. São ligações indesejadas, ofertas de serviços que não buscamos, sem contar aqueles contratos que sequer sabíamos da sua existência.

Portanto, para pôr fim a este uso indevido dos dados e responsabilizar aqueles que não zelam pelos dados de seus clientes, consumidores, usuários etc, é que a Lei Geral de Proteção de Dados surgiu.

Assim, a Lei trouxe *bases legais* para o tratamento dos dados, ou seja, determinou em quais ocasiões os dados poderão ser tratados. E se engana quem acredita que o único método é através do consentimento do titular. As bases Legais para o tratamento dos dados estão previstas no art. 7º da LGPD.

Explicamos, de forma direta e descomplicada as 10 bases legais para o processamento válido do tratamento dos dados:

### 1 - Consentimento:

Segundo a Lei, consentimento é a *"manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada"* (art. 5º, XII), ou seja, é a manifestação do próprio titular concedendo o uso, nos termos legais, de seus dados. Por exemplo, quando este titular aceita, de livre e espontânea vontade, a política de privacidade do site, aplicativo etc.

Para os Agentes de tratamento de dados é importante manter uma forma de gerenciamento deste consentimento, pois hoje o titular pode estar muito feliz com a sua forma de tratar seus dados, contudo amanhã ele poderá acordar e simplesmente não lhe conceder mais acesso ao tratamento de seus dados pessoais.

Note, portanto, como o consentimento é volátil e, por isso, é de suma importância gerenciar o consentimento.

## 2 - Legítimo Interesse:

Legítimo interesse é a base legal para tratamento de dados contida no artigo 7º, IX, da LGPD.

O dispositivo da LGPD que parametriza a aplicação do legítimo interesse como base legal é o art. 10, cujo texto dispõe:

> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
>
> I - apoio e promoção de atividades do controlador; e
>
> II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.
>
> § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

> § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.
>
> § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

O artigo fala em "finalidade" e "interesse". A finalidade é o propósito específico do tratamento de dados pessoais, enquanto o interesse é o valor mais amplo que um tratamento de dados pessoais representa para o seu controlador (ou terceiros, ou a sociedade como um todo). Um interesse, portanto, seria a garantia da segurança e da saúde de um determinado grupo de pessoas, enquanto uma finalidade seria determinado tratamento de dados que garante tal interesse.

*FONTE: ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. 2014.*

Mas o que seria um *interesse legítimo?*

Primeiramente, esse interesse deve ser legal, isto é, deve respeitar todas as leis e normas infralegais aplicáveis àquela situação específica. A coleta deve ser relacionada a uma situação concreta e, portanto, não especulativa (que decorre do próprio princípio da finalidade).

Bruno Bioni ilustra tal requisito ("legítimo") com o exemplo da proibição à coleta, mesmo com consentimento, de dados relacionados a gravidez ou HIV em situações de trabalho.

*Fonte: BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Grupo Editorial Nacional: Rio de Janeiro, 2020 (2a edição): capítulo 5.*

O artigo 10 tem por escopo promover o balanceamento dos interesses do controlador ou de terceiros frente aos do titular.

Colocando em prática as técnicas de hermenêutica jurídica sobre a interpretação do art. 10 da LGPD, podemos dizer que o dispositivo (i) refere-se tanto ao legítimo interesse do controlador, quanto de terceiros e que (ii) a relação de incisos e parágrafos do artigo impõe

condicionantes cumulativas e não alternativas. O que isso significa? Que o legítimo interesse, por conseguinte, não é aplicável apenas ao controlador, mas também à figura do "terceiro". Ou seja, o controlador pode realizar um tratamento de dados que não seja no seu próprio interesse (ou exclusivamente no seu próprio interesse), mas no de terceiros ou da sociedade como um todo – por exemplo, evitar que o cartão de crédito que o Banco nos oferece seja fraudado é interesse tanto do Banco quanto do sistema bancário e financeiro, bem como da sociedade.

(A lei brasileira não traz uma definição de quem seria o "terceiro", nem quando este se enquadra na figura de recipiente, de modo que é ainda mais desafiador interpretar o alcance da base legal do legítimo interesse de terceiro na LGPD, e é tarefa urgente da Autoridade Nacional de Proteção de Dados (ANPD) endereçar a questão.)

Mas será que os deveres exigidos para a utilização da base legal do legítimo interesse também se aplicam a microempresas e a empresas de pequeno porte?

Os deveres documentais e procedimentais referentes à utilização da base legal do legítimo interesse, a princípio, direcionam-se a todos os modelos de negócio, isto é, são horizontais. Porém, não se pode negar que um dos objetivos centrais da LGPD é harmonizar a proteção de dados pessoais dos titulares ao desenvolvimento econômico e à inovação. Portanto, é possível que a ANPD* delimite futuramente um regime normativo específico para esse grupo de empreendimentos, podendo incluir questões procedimentais mais brandas também no que toca ao legítimo interesse. Aguardamos as cenas dos próximos capítulos! *(*Conforme disposto pelo art. 55-J, XVIII, da LGPD, é competência da Autoridade Nacional de Proteção de Dados editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que esses modelos de negócios (microempresas e a empresas de pequeno porte) possam se adequar à lei.)*

### 3 - Cumprimento de obrigação legal ou regulatória

Essa base legal autoriza que a LGPD não entre em conflito com outras normas vigentes. Assim, mesmo após o encerramento do vínculo que originou o tratamento dos dados, é permitido armazenar da-

dos pessoais em função do cumprimento de obrigações do ordenamento jurídico (legislação trabalhista ou previdenciária, Lei de Acesso à Informação - Lei nº 12.527/2011, Lei do processo administrativo na administração pública federal, Marco Civil da Internet - Lei nº 12.965/2014 etc), em função de investigações criminais tributárias, cíveis, contábeis ou administrativas, entre outros.

### 4 – Tratamento pela administração pública

Essa base legal autoriza que a administração pública faça o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou previstas em contratos, convênios ou similares, observadas as disposições do Capítulo IV da LGPD. É claro que o Poder Público deverá informar a finalidade e a forma como o dado será tratado, respeitando os fundamentos da LGPD, ainda que o consentimento não seja requisito para que seja feito o tratamento.

## 5 – Realização de estudos e pesquisas

Ao trazer essa hipótese, o legislador permite que os dados pessoais sejam utilizados sem consentimento em pesquisas de caráter tecnológico, estatístico e/ou histórico.

Nunca é demais lembrar que a autorização só se aplica quando o estudo é conduzido pelo que se entende como órgão de pesquisa, cuja definição está expressamente descrita na própria Lei Geral de Proteção de Dados (art. 5, VIII):

> XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;

Apesar de não se tratar de conduta obrigatória, a lei recomenda que os dados sejam anonimizados nesses casos.

## 6 – Execução ou preparação contratual

Trata-se de hipótese em que o tratamento dos dados pessoais é indispensável ao procedimento que antecede a for-

malização de instrumento contratual, bem como à própria execução das obrigações contratualmente firmadas.

Entre os exemplos mais comuns, estão os levantamentos realizados por instituições financeiras para concessão de crédito e a coleta de dados pessoais para formalização de contrato com o objetivo de adquirir produtos ou serviços.

Por óbvio, é necessário que o próprio titular dos dados tenha sinalizado previamente o interesse na relação estabelecida, limitando-se o tratamento dos dados fornecidos à finalidade proposta.

### 7 - Exercício regular do Direito:

Aqui o Legislador trouxe uma segurança aos Agentes de Tratamento de Dados, assegurando que o tratamento de dados pode ser feito independente do consentimento do titular, quando este tratamento for **para o exercício regular de direitos em processo judicial, administrativo ou arbitral.**

Assim, a Legislação busca esclarecer que a proteção dos dados pessoais não pode interferir no direito em que as partes têm de **produzir provas em processos judiciais, uma contra as outras**.

Pense em uma empresa que sofre uma ação por suposta negativação indevida e fica impossibilitada de apresentar uma prova de negativações anteriores do autor, nos termos da súmula 385 do STJ, pois no extrato de negativação estão os dados do autor.

Desta forma, tal base legal garante às partes o direito ao contraditório e ampla defesa sem incorrer em risco de infringir alguma regra da Lei Geral de Proteção de Dados.

### 8 - Proteção da vida e da incolumidade física

Neste caso, o legislador possibilita utilização de dados pessoais sem consentimento quando a vida ou a segurança física (do titular e/ou de terceiros) estiver em risco.

Trata-se de hipótese relacionada a questões especificamente graves, sendo tal critério restritivo e somente aplicável quando as circunstâncias forem constatadas, de fato.

Entre as possíveis aplicações, está a utilização de dados de geolocalização de dispositivos móveis para localização de vítimas de incidentes.

### 9 - Tutela de saúde do titular

O legislador também elenca como hipótese o tratamento de dados com o objetivo específico de proteção à saúde.

Trata-se da base legal que fundamenta e justifica a atuação de profissionais da área da saúde (médicos, biomédicos, nutricionistas, psicólogos, enfermeiros, farmacêuticos, fisioterapeutas, educadores físicos, entre outros) e entidades membro do SNVS (Sistema Nacional de Vigilância Sanitária) no tratamento de dados contidos – por exemplo – em prontuários, exames, prescrições, termos de consentimento e sumários de transferência.

### 10 - Proteção de crédito

Trata-se do fundamento legal para consulta de informações sobre adimplência e inadimplência, essa realizada para fins de concessão (ou não) de crédito ao titular dos dados.

Cumpre sempre frisar a necessidade de compatibilização desta base legal com as normas já postas, entre elas a Lei do Cadastro Positivo (Lei n. 12.414/2011) e o Código de Proteção e Defesa do Consumidor (Lei n. 8.078/1990).

# 10. DIREITOS DOS TITULARES

A Lei Geral de Proteção de Dados também prevê direitos aos titulares quanto ao uso de seus dados pessoais. Afinal, tais informações pertencem à pessoa, ou seja, dela é  a titularidade, logo a ela pertencem os direitos sobre o seu tratamento ou não. Até mesmo porque, a rigor da lei, dados pessoais somente poderão ser utilizados, no mínimo, mediante o fornecimento de consentimento pelo titular.

Não é sem razão o Artigo 18 da LGPD, como parte do Capítulo que trata  "Dos Direitos do Titular", estabelece vários pontos sobre o direito de se obter do controlador, em relação aos seus dados, a qualquer momento e mediante requisição, providências diversas, inclusive, informações quanto à necessidade do tratamento e adequação à finalidade apontada.
Entre esses direitos dos titulares podem ser listados:

**Confirmação e acesso:** Nesse cenário, mediante solicitação, o titular tem o direito de saber se seus dados estão sendo tratados por um controlador. Ou seja, se o titular não se recorda se fez um cadastro em uma em-

presa, pode solicitar a ela que confirme ou não a existência de algum tipo de tratamento dos seus dados.

**Correção:** Direito de solicitar que dados observados como incompletos, desatualizados ou mesmo incorretos sejam corrigidos.

**Anonimização, bloqueio ou eliminação**: Pode solicitar que os seus dados sejam anonimizados, ou seja, desvinculados das informações de reconhecimento pessoal.

**Portabilidade:** Pode requerer a transferência de dados pessoais para outro controlador (até mesmo internacional).

**Revogação de Consentimento:** Pode revogar, também a qualquer momento, o consentimento de uso de seus dados pessoais tratados.

**Eliminação:** Tem o direito de pedir para que seus dados pessoais tratados, mesmo após consentimento anterior, sejam eliminados.

**Compartilhamento:** Saber informações sobre todas as entidades, de natureza – pública ou privada - com as

quais suas informações pessoais são compartilhadas.

**Explicação:** Direito de obter informações sobre as possibilidade e consequências de não fornecer o consentimento sobre determinadas ações de tratamento de dados pessoais.

**Oposição:** Negar o tratamento dos dados pessoais quando o processo é realizado de maneira ilegal.

# 11. CONTROLADOR E OPERADOR

O controlador é o agente responsável por tomar as decisões referentes ao tratamento dos dados pessoais, além de definir a finalidade deste tratamento. Entre essas decisões, estão instruções fornecidas a operadores contratados para a realização de um determinado tratamento de dados pessoais.

O artigo art. 5º, VI, da LGPD define controlador como:

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

O controlador será pessoa jurídica, tanto de direito público quanto privado, quando tomar as principais decisões a respeito do tratamento de dados dentro da sua organização.

Já o controlador pessoa natural, ou também chamado de pessoa física, age em nome próprio, de forma independente, neste âmbito encontram-se empresários individuais, profissionais liberais (médicos, advogados, contadores etc.) além dos responsáveis pelas serventias extrajudiciais.

Importante destacar que o controlador não precisa necessariamente processar os dados, mas deve tomar as decisões sobre os tratamentos.

Já o Operador é a pessoa que executa e trata o dado a mando do controlador. O operador é o agente responsável por realizar o tratamento de dados em nome do controlador e conforme a finalidade por este delimitada.

A definição legal se encontra no art. 5º, inciso X da LGPD:

> Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Nesse mesmo sentido é a previsão do art. 39 da LGPD:

> O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

A previsão acima implica dizer que o operador só poderá tratar os dados para a finalidade previamente estabelecida pelo controlador. Isso demonstra a principal diferença entre o controlador e operador, qual seja, o poder de decisão: o operador só pode agir no limite das finalidades determinadas pelo controlador.

# 12. ENCARREGADO DE PROTEÇÃO DE DADOS (DPO)

Conforme o artigo 41 da LGPD, o controlador de dados deverá indicar um encarregado pelo tratamento de dados pessoais. O encarregado é o indivíduo responsável por garantir a conformidade de uma organização, pública ou privada, à LGPD. Caberá também ao encarregado atender às comunicações dos titulares dos dados pessoais quando estes demandarem a organização para exercício dos seus direitos previstos na lei.

Além disso, também será papel do encarregado de proteção de dados a comunicação entre a organização e a Autoridade Nacional de Proteção de Dados (ANPD), devendo comprovar a adequação daquela à LGPD.

Ao contrário de outras legislações de proteção de dados estrangeiras, a LGPD não determinou em que circunstâncias uma organização deve indicar um encarregado. Assim, deve-se assumir, como regra geral, que toda organização deverá indicar uma pessoa para assumir esse papel.

# 13. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

A ANPD é o órgão da administração pública federal responsável por zelar pela proteção de dados pessoais, por implementar e fiscalizar o cumprimento da LGPD no Brasil. A Autoridade Nacional também será responsável pela aplicação de sanções em caso de descumprimento à legislação. Além disso, caberá à Autoridade Nacional estabelecer regras específicas para a proteção de dados nos casos em que a LGPD se omitiu.

# 14. CONSEQUÊNCIAS DA NÃO ADEQUAÇÃO E SANÇÕES

Àqueles que tratam dados pessoais e não se adequarem a novas regras da LGPD poderão ser aplicadas sanções administrativas pela ANPD e ainda estar sujeito a condenações na esfera judicial.

Em menos 10 meses da vigência da LGPD já foram proferidas mais de 600 decisões judiciais relacionadas a proteção de dados e segurança da informação.

As sanções administrativas vão desde uma advertência, o bloqueio de dados pessoais, a suspensão temporária ou a proibição da atividade de tratamento de dados pessoais até a aplicação de multa simples de até 2% do faturamento no seu último exercício, excluídos os tributos, limitada a R$ 50.000.000,00 por infração e ainda multa diária, respeitado o limite do da LGPD.

Nada impede que, para cada tratamento de dados em desconformidade com a lei ou incidente de vazamento de dados, sejam aplicadas tanto sanções na esfera administrativa quanto na esfera judicial, concomitantemente.

# 15. VANTAGENS DE ADEQUAÇÃO

A adequação à Lei Geral de Proteção de Dados é uma **obrigação legal** que deve ser respeitada sob pena de deixar o agente tratador de dados à mercê de sanções administrativas, ações judiciais e perda de clientela, além de outras consequências nefastas como: a péssima (e obrigatória, por força de lei) publicidade de eventual infração cometida após apuração e constatação de vazamento de dados; suspensão do banco de dados; proibição parcial ou total do exercício relacionado ao tratamento dos dados e má reputação da empresa no mercado. Além de evitar tais problemas, a adequação à Lei trará a possibilidade dos negócios trabalharem com informações mais limpas, adequadas e apoiadas em bases legais, valendo destacar algumas vantagens extras para a implementação da lei:

**Transformação Digital**

Tanto as recentes transformações sociais como a revolução do conhecimento, onda de tecnologia limpa e relações pós-pandemia quanto as disposições da legislação já em vigor trouxeram a obrigação de as empresas investirem em novas tecnologias.

A adequação à LGPD, portanto, exsurge num momento ideal para começar ou avançar na transformação digital numa organização – seja na adoção de novas ferramentas que permitam a segurança da informação, na digitalização do negócio, na leitura e ciência de dados, organização negocial etc.

**Evolução das relações sociais e proteção à democracia**
Através da LGPD o direito e a tecnologia se agrupam com promessas significativas de efetividade, que estabelecerão mudanças necessárias, contribuintes para a proteção e segurança a coleta de dados pessoais, pautadas no respeito a privacidade, direitos de personalidade, intimidade e dignidade, fomentando e harmonizando o uso da tecnologia, almejando negócios pautados em boas práticas de governança e de responsabilidade ao tratamento dessas informações.

A LGPD pretende proteger direitos como privacidade, intimidade, imagem, honra e dignidade. Logo, podemos afirmar que a LGPD não deixa de ser um mecanismo de proteção a democracia.

São numerosos os riscos decorrentes do uso de dados pessoais em massa, precipuamente quando impróprios, isto é, quando utilizados para fins diversos daqueles inicialmente divulgados e consentidos. A possível deterioração de instituições democráticas tornou-se evidente com os escândalos da *Cambridge Analytica* e *Brexit*, e obteve atenção mundial de governos nas eleições que seguiram. É certo que um dos pilares do Estado Democrático de Direito é a limitação dos seus poderes, bem como os direitos e garantias fundamentais da pessoa humana. Os conceitos da LGPD, portanto, coadunam-se com os mecanismos implícitos ao princípio democrático. **Relações transparentes e melhora no relacionamento com o cliente através da confiabilidade e respeito à privacidade.**

Em razão do desenvolvimento tecnológico, o compartilhamento de dados é massivo atualmente, e muitas vezes o destino dos dados pessoais é totalmente desconhecido. Um dos objetivos da LGPD é possibilitar a transparência perante os consumidores sobre a utilização de seus dados, o que faz com que a implementação da LGPD seja uma oportunidade de ouro para as empresas se aproximarem dos consumidores e futuros investidores. Com a maior transparência pela LGPD pregada, os usuários/titulares podem saber exatamen-

te o que ocorre com os seus dados, tendo muito mais segurança e confiança na utilização de um site/serviço.

Pela necessidade do consentimento para *captação e tratamento de dados pessoais*, além de deixar clara a finalidade da coleta de dados, o cliente terá conhecimento integral sobre o uso de suas informações de forma transparente, o que contribui para uma maior credibilidade social e alcance positivo do público-alvo.

**Reputação da Empresa e fator concorrencial**

A implementação da LGPD numa organização automaticamente demonstra para os clientes a atuação transparente e ética da empresa – atitude vai construir e contribuir para a reputação da organização e ajudar a fidelizar cliente. É, também nesse aspecto, um importante fator concorrencial perante as demais empresas.

**Contratação entre Empresas: fortalecimento das relações comerciais**

Além da transparência perante os clientes, a adequação à LGPD também trará vantagem competitiva em relação à contratação entre empresas, o que decorre da possibilidade de responsabilização solidária e dos riscos rela-

cionados ao tratamento indevido dos dados. É evidente que toda organização que implementar a LGPD também questionará se os seus fornecedores estão igualmente de acordo com suas determinações. Nesse sentir, cada vez mais a empresa garantirá uma reputação de ambiente seguro para o pleno tratamento e uso de dados pessoais.

A maior segurança jurídica em relação ao tratamento de dados pessoais possibilitará o fechamento de novos contratos, haja vista que nem todas as empresas estarão de acordo com a lei. Essas últimas, sem dúvida alguma, perderão negócios.

**Valorização do marketing e aumento de sua produtividade.** Eliminar informações pessoais irrelevantes ao negócio (a chamada "minimização"), propiciará aumento na qualidade das informações realmente decisivas e necessárias às empresas, com bancos de dados alimentados com informações de clientes verdadeiros e relevantes.

Além disso, a navegação nos sites deverá ser mais prazerosa devido à redução de publicidade e anúncios não solicitados.

Um outro benefício da LGPD, por conseguinte, é aumentar consideravelmente a probabilidade de proximi-

dade dos clientes com as organizações que sejam do seu real interesse. Com abordagens menos invasivas, e melhorando a experiência do cliente, o interesse do consumidor tende a crescer naturalmente para determinada marca ou produto.

**Segurança cibernética aprimorada, organização e saneamento de vulnerabilidades.**
Devido às altas sanções, a preocupação das companhias com a infraestrutura de tecnologia de informação e segurança de dados pessoais passará a vir em primeiro lugar, trazendo consideráveis mudanças no processo de proteção cibernética. Ataques nunca cessarão, é claro, mas o nível de segurança das empresas deve aumentar cada vez mais. Como decorrência lógica, as empresas serão mais organizadas e haverá um aprimoramento e otimização de rede, com liberação de espaço em servidores e nuvens, além de uma exponencialmente melhor organização e identificação dos dados.

Muitas empresas possuem excesso de dados pessoais desnecessários ou incorretos para o exercício de sua atividade. Além de se traduzir em desconformidade com a legislação, isso aumenta os riscos de eventuais incidentes de segurança e influenciar na organização das informações, comprometendo inclusive a relação com consumidores e parceiros econômicos.

Durante o processo de adequação à LGPD a empresa começará a detectar as vulnerabilidades (físicas e digitais), identificar as lacunas de segurança, bem como aprender a corrigi-las.

**Nível de consciência dos empregados**

Muito embora muitos empresários pensem que as falhas de segurança ocorrem por conta de problemas com *software* ou sistema operacional, pesquisas apontam que  o fator humano tem enorme peso na ocorrência de vazamentos de dados. Num processo de adequação à LGPD, a responsabilidade dos colaboradores é intimamente enfrentada de modo que todos possam ter ciência de suas responsabilidades e da importância da proteção dos dados para muito além de evitar sanções.

**Da responsabilidade pelo Tratamento de Dados Pessoais**

A responsabilidade do agente de tratamento de dados é disciplinada nos artigos 42 a 45 da Lei 13.709/18 (LGPD) estabelecendo, logo de início (Art. 42), que o controlador ou operador de dados pessoais que causar dano a outrem é obrigado a repara-lo.

O legislador preocupou-se ainda em assegurar a possibilidade de inversão do ônus da prova em favor do

titular dos dados tratados, sempre que se verificar ser verossimilhante  a alegação do mesmo; houver hipossuficiência para fins de produção da prova; ou quando a produção da prova resultar-lhe excessivamente onerosa (§2º, art. 42).

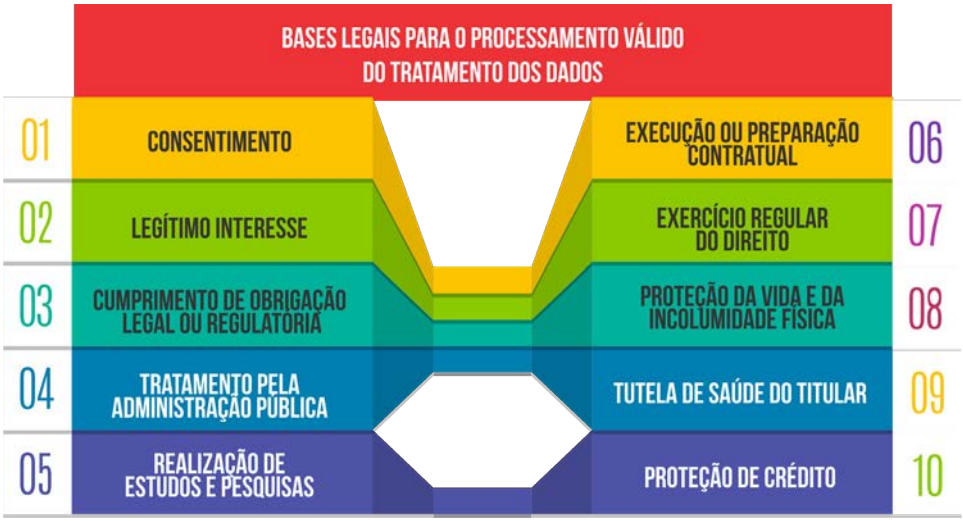
Assim, é muito importante para o exercício da atividade de tratamento de dados pessoais a observância ao disposto no art. 6º da LGPD, que estabelece, juntamente com a boa-fé, os 10 princípios norteadores da atividade de tratamento, sendo eles: Finalidade, Adequação, Necessidade, Livre acesso, Qualidade dos dados, Transparência, Segurança, Prevenção, Não discriminação, Responsabilização e Prestação de contas. Ao lado dos Princípios o Agente de Tratamento deve atender os Requisitos para o tratamento de dados pessoais (art.7º e ss), que devem ser preenchidos para o regular exercício da atividade.

Portanto, existindo alegação por parte do Titular de Dados da ocorrência de dano, compete ao agente de Tratamento a prova da ocorrência das excludentes do art. 43, ou seja, que não realizou o tratamento; realizou sem violação a legislação ou que o dano se deu por culpa exclusiva do Titular dos Dados, afastando dessa forma o dever de reparação.

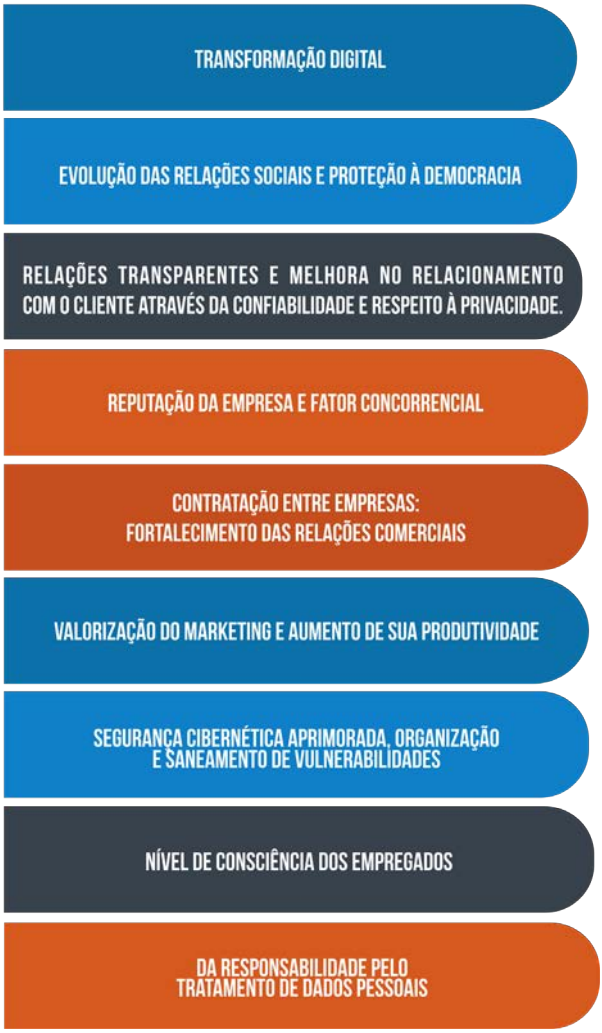
Medidas como a implementação de um Código de Governança através de um departamento de *Compliance*(artº50), bem como de medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessonão autorizados (art. 46), mostram-se bastante relevantes na medida que podem influenciar no resultado reduzindo o patamar de aplicação de sanções administrativas (art. 52§1º).

Por fim, importante registrar que a responsabilização administrativa prevista na LGPD, não afasta a aplicação das regras de responsabilidade previstas no Código Civil (arts. 186, 187 e 927) e no Código de Defesa do Consumidor.

# CONTEÚDO LGPD


BASES LEGAIS PARA O PROCESSAMENTO VÁLIDO DO TRATAMENTO DOS DADOS
01
CONSENTIMENTO
02
LEGÍTIMO INTERESSE
03
CUMPRIMENTO DE OBRIGAÇÃO LEGAL OU REGULATÓRIA
04
TRATAMENTO PELA ADMINISTRAÇÃO PÚBLICA
05
REALIZAÇÃO DE ESTUDOS E PESQUISAS
06
EXECUÇÃO OU PREPARAÇÃO CONTRATUAL
07
EXERCÍCIO REGULAR DO DIREITO
08
PROTEÇÃO DA VIDA E DA INCOLUMIDADE FÍSICA
09
TUTELA DE SAÚDE DO TITULAR
10
PROTEÇÃO DE CRÉDITO

## ALGUMAS VANTAGENS EXTRAS PARA A IMPLEMENTAÇÃO DA LEI:



# DIREITOS DE TITULARES


Esta obra foi composta em Calibri
em agosto de 2021.

Vivemos a era da revolução digital, na qual quem não se digitalizar a médio e longo prazo dificilmente permanecerá no mercado.

Já é impossível estabelecer modelos de negócios ou inovação tecnológica sem considerar o conceito de Privacy by Design.

Toda e qualquer empresa precisa incorporar salvaguardas de privacidade e proteção de dados pessoais em todos os projetos desenvolvidos.

Não há solução mágica, tampouco um caminho único para adequar uma organização à Lei Geral de proteção de Dados - LGPD. Cada modelo de negócio demanda um olhar específico. Um especialista poderá auxiliar a encontrar o melhor caminho.

Tenha em mente, porém, que a adequação à LGPD é fundamental para a sobrevivência do seu negócio e que somente trará resultados satisfatórios se for entendida como uma jornada multidisciplinar – com benefícios diretos na relação com empregados, clientes, fornecedores e terceiros – e não um projeto com data para iniciar e terminar.

Assim como um empresário precisa sempre cumprir a legislação trabalhista numa relação de trabalho, ou o CDC numa relação de consumo, todo e qualquer agente que tratar dados sempre terá de cumprir a LGPD para evitar passivos e que sejam aplicadas punições judiciais ou administrativas.

LIFE EDITORA

OAB MATO GROSSO DO SUL

ISBN 978-65-5887-136-1