



**Fundação Educacional do Município de Assis  
Instituto Municipal de Ensino Superior de Assis  
Campus "José Santilli Sobrinho"**

**NILTON ANTONIO GOMES DA SILVA**

**LGPD - LEI GERAL DE PROTEÇÃO DE DADOS**

**Assis/SP  
2023**



**Fundação Educacional do Município de Assis  
Instituto Municipal de Ensino Superior de Assis  
Campus "José Santilli Sobrinho"**

**NILTON ANTONIO GOMES DA SILVA**

## **LGPD – LEI GERAL DE PROTEÇÃO DE DADOS**

Projeto de pesquisa apresentado ao curso de Bacharelado em Direito do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

**Orientando(a): Nilton Antonio Gomes da Silva**

**Orientador(a): Jesualdo Eduardo de Almeida Junior**

**Assis/SP  
2023**

## FICHA CATALOGRÁFICA

Antônio Gomes da Silva, Nilton.

LGPD – LEI GERAL DE PROTEÇÃO DE DADOS / Nilton Antônio Gomes da Silva.  
Fundação Educacional do Município de Assis –FEMA – Assis, ano 2023

Número de páginas.

1. lei geral proteção de dados. 2. Proteção de dados

CDD:  
Biblioteca da FEMA

# LGPD - LEI GERAL DE PROTEÇÃO DE DADOS

NILTON ANTONIO GOMES DA SILVA

Trabalho de Conclusão do curso de Bacharelado em Direito apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação, avaliado pela seguinte comissão examinadora:

**Orientador:** \_\_\_\_\_  
Jesualdo Eduardo de Almeida Junior

**Examinador:** \_\_\_\_\_

## DEDICATÓRIA

Dedico ao meu pai (in memoriam) que me inspira sempre a nunca desistir, e aos meus filhos Gabriel, João Pedro, Laryssa e Maria Eduarda.

## **AGRADECIMENTOS**

Ao meu orientador Jesualdo Eduardo de Almeida Junior, por me dar total liberdade nas minhas pesquisas e me direcionar na trajetória até aqui.

Sou grato a minha esposa Luciane Regina Gati Gomes Da Silva, que nunca me recusou amor, apoio e incentivo. Obrigado, todo o amor do meu coração, por compartilhar os inúmeros momentos de ansiedade e estresse. Sem você ao meu lado o trabalho não seria concluído. Obrigado por sua gentileza e da nossa família pela compreensão mesmo com minha ausência em diferentes momentos.

## RESUMO

A Lei Nº 13.709 (Lei Geral de Proteção de Dados), vigorou no Brasil em 2020, 18 meses após sua publicação. Apesar de parecer longo esse intervalo, acreditava-se ser o suficiente para que as empresas se adaptassem às novas obrigações referentes ao armazenamento, uso e proteção de dados. O processo é repleto de desafios. Primeiramente, há aqueles relacionados à própria adaptação, que envolve novas demandas, cuidados e tecnologias que devem ser implementadas e bem utilizadas em todo negócio jurídico, sendo ele Físico ou Jurídico. Mas há também as questões resultantes do fato de que a fiscalização da Lei ainda está cercada por dúvidas e pontos em aberto, que alcançam também a população. Nesse contexto, precisamos compreender quais são os desafios nos quais a Pessoa Física ou Pessoa Jurídica deve prestar atenção e, em especial nos processos de implementação da LGPD.

**Palavras-chave: LGPD; Proteção de Dados, Lei 13.13.853/2019.**

## **ABSTRACT**

Law No. 13,709 (General Data Protection Law), came into force in Brazil in 2020, 18 months after its publication. Although this interval seems long, it was believed to be enough for companies to adapt to the new obligations regarding the storage, use and protection of data. The process is fraught with challenges. First, there are those related to the adaptation itself, which involves new demands, care and technologies that must be implemented and well used in all legal business, whether physical or legal. But there are also issues resulting from the fact that enforcement of the Law is still surrounded by doubts and open points, which also reach the population. In this context, we need to understand what are the challenges that the Individual or Legal Entity should pay attention to and, in particular in the implementation processes of the LGPD.

**Keywords: LGPD; Data Protection, Law 13.13.853/2019.**

## **LISTA DE ABREVIATURAS E SIGLAS**

LGPD – Lei geral de Proteção de Dados.

RGPD - Regulamento Geral de Proteção de Dados.

PL – Projeto de Lei.

ANPD - Autoridade Nacional de Proteção de Dados.

DMPS – Data Protection Management System

## SUMÁRIO

<b>INTRODUÇÃO .....</b>	<b>12</b>
<b>1. OS PRINCIPAIS TERMOS E SANSÕES DA LEI GERAL DE PROTEÇÃO DE DADOS.....</b>	<b>14</b>
1.1. CONCEITOS .....	14
1.1.1. DADO PESSOAL .....	14
1.1.2. DADO PESSOAL SENSÍVEL.....	15
1.1.3. DADO ANONIMIZADO .....	15
1.1.4. BANCO DE DADOS .....	15
1.1.5. TITULAR.....	15
1.1.6. CONTROLADOR.....	15
1.1.7. ENCARREGADO.....	16
1.1.8. AGENTES DE TRATAMENTO.....	16
1.1.9. TRATAMENTO .....	16
1.2. PRINCÍPIOS DA LGPD.....	16
1.2.1. PRINCÍPIO DA FINALIDADE .....	17
1.2.2. PRINCÍPIO DA ADEQUAÇÃO .....	17
1.2.3. PRINCÍPIO DA NECESSIDADE.....	17
1.2.4. PRINCÍPIO DO LIVRE ACESSO.....	17
1.2.5. PRINCÍPIO DA QUALIDADE DOS DADOS.....	18
1.2.6. PRINCÍPIO DA TRANSPARÊNCIA.....	18
1.2.7. PRINCÍPIO DA SEGURANÇA.....	18
1.2.8. PRINCÍPIO DE PREVENÇÃO .....	18
1.2.9. PRINCÍPIO DA NÃO DISCRIMINAÇÃO.....	18
1.2.10. PRINCÍPIO DA RESPONSABILIDADE E PRESTAÇÃO DE CONTAS.....	19
1.3. HIPÓTESES DE TRATAMENTO .....	19
<b>2. DO TRATAMENTO DOS DADOS.....</b>	<b>20</b>
2.1. HIPÓTESES DE TRATAMENTO DE DADOS PESSOAIS.....	20
2.1.1. MEDIANTE AUTORIZAÇÃO DO TITULAR .....	20
2.1.2. PARA CUMPRIMENTO DE OBRIGAÇÃO LEGAL OU REGULÁTORIA .....	20
2.1.3. PARA EXECUÇÃO DE POLÍTICAS PÚBLICAS PREVISTAS EM LEI E REGULAMENTOS, OU RESPALDADAS EM CONTRATOS, CONVÊNIOS E OUTROS INSTRUMENTOS.....	21

2.1.4.	PARA REALIZAÇÃO DE ESTUDOS POR ÓRGÃOS DE PESQUISAS.....	21
2.1.5.	PARA EXECUÇÃO DE CONTRATOS OU DE PROCEDIMENTOS PRELIMINARES, DO QUAL SEJA PARTE O TITULAR, A PEDIDO DO TITULAR DOS DADOS.....	22
2.1.6.	PARA EXERCÍCIO REGULAR DE DIREITOS EM PROCESSO JUDICIAL, ADMINISTRATIVO OU ARBITRAL .....	22
2.1.7.	PARA A PROTEÇÃO DA VIDA OU DA INCOLUMIDADE (CONDIÇÃO) FÍSICA DO TITULAR OU DE TERCEIRO .....	22
2.1.8.	PARA A TUTELA DA SAÚDE, EXCLUSIVAMENTE, EM PROCEDIMENTO REALIZADO POR PROFISSIONAIS DE SAÚDE, SERVIÇOS DE SAÚDE OU AUTORIDADE SANITÁRIA .....	23
2.1.9.	QUANDO NECESSÁRIO PARA ATENDER AOS INTERESSES LEGÍTIMOS DO CONTROLADOR OU DE TERCEIRO .....	23
2.1.10.	PROTEÇÃO DO CRÉDITO .....	24
2.2.	HIPÓTESES DE TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS..	24
2.2.1.	MEDIANTE O CONSENTIMENTO .....	24
2.2.2.	SEM O CONSENTIMENTO .....	24
2.3.	HIPÓTESES DE TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES.....	26
<b>3.</b>	<b>DO DIREITO .....</b>	<b>28</b>
3.1.	DIREITOS DOS TITULARES DE DADOS.....	28
3.1.1.	DIREITO A CONFIRMAÇÃO DE EXISTÊNCIA DE TRATAMENTO .....	28
3.1.2.	DIREITO DE ACESSO AOS DADOS.....	29
3.1.3.	DIREITO DE CORREÇÃO DOS DADOS INCOMPLETOS, INEXATOS OU DESATUALIZADOS.....	29
3.1.4.	DIREITO DE ANONIMIZAÇÃO, BLOQUEIO OU ELIMINAÇÃO DE DADOS DESNECESSÁRIOS, EXCESSIVOS OU TRATADOS EM DESCONFORMIDADE COM A LEI.....	29
3.1.5.	DIREITO DE PORTABILIDADE DOS DADOS A OUTRO FORNECEDOR DE SERVIÇO OU PRODUTO .....	29
3.1.6.	DIREITO DE ELIMINAÇÃO DOS DADOS PESSOAIS TRATADOS COM O CONSENTIMENTO DO TITULAR.....	30
3.1.7.	DIREITO DE INFORMAÇÃO DAS ENTIDADES PÚBLICAS E PRIVADAS COM AS QUAIS O CONTROLADOR REALIZOU USO COMPARTILHADO DE DADOS.....	30
3.1.8.	DIREITO DE INFORMAÇÃO SOBRE A POSSIBILIDADE DE NÃO FORNECER CONSENTIMENTO E SOBRE AS CONSEQUÊNCIAS DA NEGATIVA	
	30	
<b>4.</b>	<b>DAS PENALIDADES, DO COMPARTILHAMENTO E DA ADEQUAÇÃO</b>	<b>32</b>

4.1.	DAS PENALIDADES ADMINISTRATIVAS PELO DESCUMPRIMENTO DA LEI	32
4.2.	COMPARTILHAMENTO DE DADOS DE EMPRESAS CONTROLADORAS COM EMPRESAS OPERADORAS E A NECESSIDADE DE ELABORAÇÃO DE CONTRATO .....	34
4.3.	ENCARREGADO DE DADOS, SUA COMUNICAÇÃO COM A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS E O TITULAR DO DADO, E SEU PERFIL .....	36
<b>5.</b>	<b>A ADEQUAÇÃO E A PRIVACIDADE .....</b>	<b>37</b>
5.1.	PASSO A PASSO PARA UM PROGRAMA DE ADEQUAÇÃO À LGPD	37
5.1.1.	A CONSCIENTIZAÇÃO DA EMPRESA PARA SUCESSO DO PLANO DE AÇÃO PARA ADEQUAÇÃO À LGPD .....	37
5.1.2.	O MAPEAMENTO DE DADOS.....	38
5.1.3.	LEVANTAMENTO DE LEIS, REGULAMENTOS, POLÍTICAS, CÓDIGOS E ANÁLISE DE CONTRATOS .....	39
5.1.4.	LEVANTAMENTO DE RISCOS À PRIVACIDADE E MITIGAÇÃO DE RISCOS, COM ADOÇÃO DE MEDIDAS NECESSÁRIAS E ATENDIMENTO DAS SOLICITAÇÕES DOS USUÁRIOS .....	40
5.1.5.	MANTENDO A ADEQUAÇÃO .....	42
	<b>CONSIDERAÇÕES FINAIS .....</b>	<b>43</b>
	<b>REFERÊNCIAS BIBLIOGRÁFICAS .....</b>	<b>45</b>

## INTRODUÇÃO

A LGPD – Lei Geral de Proteção de Dados, foi criada pelo ex-presidente Michel Temer através da Lei 13.709 em 14 de agosto de 2018, posteriormente alterada pela Medida Provisória – MP 869/2018 e atualmente com novas disposições trazidas pela Lei 13.853 de 8 de julho de 2019, sendo as recentes na gestão do presidente Jair Messias Bolsonaro.

Proteção de dados é um assunto relativamente novo no Brasil, mas na Europa o tema é discutido desde 1940. Na década de 1970, surgiu a primeira geração de normas de proteção de dados na Europa, com a Lei de Dados da Suécia (1973) e a Lei Federal de Proteção de Dados da Alemanha (1977).

As leis europeias foram evoluindo nas últimas quatro décadas em busca de devolver ao titular do dado o poder da autodeterminação informativa, que concede a ele o controle sobre o compartilhamento ou não de seus dados pessoais. Essa evolução culminou na recente lei europeia de proteção de dados, conhecida como RGPD: Regulamento Geral de Proteção de Dados, que entrou em Vigor em maio de 2018.

No Brasil, a Constituição de 1988 tem previsto no artigo 5, inciso X, o direito fundamental à intimidade e à vida privada. Há também leis ordinárias que tutelam a privacidade e proteção de dados, das quais podemos citar o Código de Defesa do Consumidor (lei nº 8.078/90), Código Civil (lei nº 10.406/2002), a Lei do Cadastro Positivo (lei nº 12.414/2011), Lei de Acesso a Informação Pública (lei nº 12.527/2011), Marco Civil da Internet (lei nº 12.965/2014) dentre outras.

Somente em 2012 foi proposto na Câmara o projeto de lei nº 4.060, o qual regulou especificamente o tratamento de dados pessoais. Em 2013, é proposto no Senado o projeto de Lei nº 330/2013, que tinha como tema a proteção, tratamento e o uso de dados pessoais. Em 2016, após consulta pública feita pelo Ministério da Justiça e, impulsionado pela aprovação do Regulamento Geral de Proteção de Dados europeu, é instaurado o PL nº 5.276/2016 na Câmara, que acaba sendo apensado ao PL nº 4.060/2012.

Em 2017, estavam em tramitação no Congresso Nacional dois projetos relativos a privacidade e proteção de dados: o PL 5.276/2016 na Câmara e o PLS 330/2013 no Senado.

Os Projetos de Lei foram unificados no Projeto de Lei Complementar nº 53/2018 que resultou na Lei Geral de Proteção de Dados Pessoais. A lei recebeu o nº de 13.709/2018 e entrou em vigor em 16 de agosto de 2020.

# **1. OS PRINCIPAIS TERMOS E SANSÕES DA LEI GERAL DE PROTEÇÃO DE DADOS**

A lei 13.709/2018 será aplicada às empresas e também às pessoas naturais que realizem operações de tratamento de dados pessoais, quando o tratamento destes dados tiver por objetivo o fornecimento de bens e serviços, e ocorra no território nacional.

Importante salientar que a lei Geral de Proteção de Dados não se aplica a pessoas naturais que tem como objetivo o tratamento para fins exclusivamente particulares e não econômicos. Não se aplica, ainda, se o uso for para fins jornalísticos, artísticos, acadêmicos ou de segurança pública, além dos dados provenientes e destinados a outros países, que apenas transitem pelo Brasil.

A inadequação à Lei 13.709/2018 pode resultar na aplicação das penalidades que podem variar desde uma advertência até multas no valor de R\$ 50.000.000,00 (cinquenta milhões de reais), além de bloqueio e eliminação dos dados pessoais tratados em desconformidade da lei, suspensão ou proibição do exercício da atividade de tratamento por período de até 6 (seis) meses.

## **1.1. CONCEITOS**

Para entender a LGPD é necessário, também, entender alguns termos, que serão explicados a seguir.

### **1.1.1. DADO PESSOAL**

É toda informação através da qual seja possível identificar uma pessoa física. Como já é de se imaginar, são os dados que detém o nome, números dos documentos pessoais como CPF e Cédula de Identidade, endereço, estado civil, data de nascimento, e-mail, telefone pessoal, comercial, ou seja, toda fonte de informação, localização e identificação direta do indivíduo. Também se admite como dado pessoal o conjunto de informações através do qual uma pessoa seja identificável, e isso sem que nenhum dado pessoal comum tenha sido fornecido. Senão vejamos.

Imagine e considere essas três informações sobre uma pessoa e, mesmo sem especificar nenhum dado pessoal direto, facilmente identificaremos a pessoa que estou sugerindo: Jogador de futebol, negro, considerado o Rei do Futebol.

Acreditando que todos nos pensaríamos no Pelé, exatamente o que eu sugeri sem indicar nenhum dado direto. Portanto, a Lei considera também a informação indireta como dado pessoal, pois analisadas em conjunto indicam a pessoa.

### **1.1.2. DADO PESSOAL SENSÍVEL**

É um dado pessoal que pode gerar discriminação ou preconceito, tais como: origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato, organização religiosa, filosófica e política, referente a saúde, vida sexual, tudo vinculado a uma pessoa natural.

### **1.1.3. DADO ANONIMIZADO**

Dados anonimizados são os dados que pertencem a um indivíduo, contudo não é possível identificar seu titular, como, por exemplo, os dados eleitorais.

### **1.1.4. BANCO DE DADOS**

São os dados estruturados e armazenados em vários locais, tanto eletronicamente quanto fisicamente.

### **1.1.5. TITULAR**

É a pessoa física a que se refere o dado objeto de tratamento.

### **1.1.6. CONTROLADOR**

Pessoa natural ou jurídica indicada pelo controlador ou operador para ser a ligação entre o titular do dado e a autoridade de proteção de dados.

### **1.1.7. ENCARREGADO**

É a pessoa natural ou jurídica indicada pelo controlador ou operador para ser a ligação entre o titular do dado e a autoridade nacional de proteção de dados.

### **1.1.8. AGENTES DE TRATAMENTO**

É a pessoa natural ou jurídica que trata os dados pessoais, ou seja, o controlador e o operador.

### **1.1.9. TRATAMENTO**

É toda e qualquer ação ou operação realizada com os dados pessoais, como, por exemplo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle da informação, modificação, comunicação, ou seja, toda ação ou atividade seja realizada com um dado pessoal para que seja considerado um tratamento.

## **1.2. PRINCIPIOS DA LGPD**

Tão importante quanto a previsão da obrigação do registro das atividades de tratamento de dados é a definição de quais deveriam ser seus componentes. Na medida em que a LGPD não chegou a tal nível de detalhes, do ponto de vista prático resta aguardar futura regulamentação da Autoridade Nacional de Proteção de Dados/ANPD, a qual deveria precisar quais são os componentes de um inventário de dados, levando-se em consideração as particularidades entre controladores e processadores que podem resultar numa documentação igualmente distinta. Considerar eventual exceção a tal obrigação legal, considerando-se o porte da organização e se a sua atividade de tratamento de dados seria de alto risco de acordo com as suas competências e de forma similar ao que fez o Regulamento Europeu.

A Lei Geral de Proteção de Dados pessoais trouxe no artigo 6º. Dez princípios que precisam obrigatoriamente ser atendidos quando se realiza o tratamento de dados: “Art. 6º. – As atividades de tratamento de dados pessoais deverão observar a boa fé e os seguintes princípios [...] (BRASIL, 2018, p.1). Tais princípios serão abordados a seguir.

### **1.2.1. PRINCÍPIO DA FINALIDADE**

O tratamento deve atender uma finalidade específica, deve ter um propósito, ser motivado, deve ser claro e informado ao titular de dado.

No caso de o dado ser utilizado de forma diferente e equivocada, será considerada uma violação da Lei, um exemplo claro e prático é a coleta de informações através da obtenção de e-mail para fins de envio de nota fiscal e, posteriormente, o e-mail é indevidamente utilizado para enviar mensagens de marketing. Neste caso, o controlador está infringindo a Lei Geral de Proteção de Dados.

### **1.2.2. PRINCÍPIO DA ADEQUAÇÃO**

É necessário existir relação adequada entre a finalidade informada pela empresa que está tratando dos dados com os dados pessoais tratados, simplesmente por ser plausível e adequado.

Imaginemos que determinada empresa que venda artigos de variedades solicita sua opinião política para envio de produtos, vê-se que não há razoabilidade na coleta de um dado pessoal sensível para a finalidade de remessa de um produto. Assim, a coleta está em desconformidade com a Lei.

### **1.2.3. PRINCÍPIO DA NECESSIDADE**

Os dados pessoais tratados devem se limitar ao mínimo necessário para atingir a finalidade do tratamento, deve ser pertinente e proporcional à necessidade, evitando o excessivo.

Suponhamos que em uma compra feita pela Plataforma conhecida como Mercado Livre, o comprador opte por retirar o produto na loja física ou no próprio endereço da plataforma, e lhe é requerido o endereço de entrega. Não parece razoável a exigência diante da forma de retirada do produto, sendo evidente que tal prática extrapola a necessidade do dado.

### **1.2.4. PRINCÍPIO DO LIVRE ACESSO**

A LGPD garantiu aos titulares de dados a consulta facilitada e gratuita sobre a forma de tratamento do dado, e sua integridade, isto é dizer que as empresas deverão ter formas

facilitadas para que os titulares dos dados entrem em contato e solicitem informações sobre os dados pessoais deles que podem ter sido tratados pela empresa. Não atender à solicitação é uma infração à LGPD.

#### **1.2.5. PRINCÍPIO DA QUALIDADE DOS DADOS**

Este princípio busca garantir ao titular que os dados pessoais que a empresa possui a seu respeito sejam verdadeiros, exatos, claros e atualizados.

#### **1.2.6. PRINCÍPIO DA TRANSPARÊNCIA**

Este princípio consiste em informar ao titular dos dados pessoais como eles serão tratados e com quais agentes de tratamento e empresas esses dados são compartilhados.

#### **1.2.7. PRINCÍPIO DA SEGURANÇA**

Este princípio contempla a garantia do titular de que seus dados pessoais serão tratados mediante utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acesso não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Isto é, medidas de segurança como procedimentos, meios e tecnologias.

#### **1.2.8. PRINCÍPIO DE PREVENÇÃO**

Aos agentes de tratamento cabe adotar medidas técnicas administrativas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais por ele realizados.

#### **1.2.9. PRINCÍPIO DA NÃO DISCRIMINAÇÃO**

Este princípio traz ao titular a garantia de que seus dados pessoais não podem ser tratados com finalidade discriminatória, ilícita ou abusiva.

### **1.2.10. PRINCÍPIO DA RESPONSABILIDADE E PRESTAÇÃO DE CONTAS**

Cabe aos agentes de tratamento provar que as normas de proteção de dados pessoais são cumpridas, que as medidas por eles adotadas são eficazes e que podem demonstrar essa conduta diligente em uma eventual fiscalização.

Essa comprovação pode ser feita demonstrando que a equipe de colaboradores foi treinada, que uma consultoria especializada foi contratada para revisar os documentos e processos da empresa e pela implantação de processos e protocolos de segurança, por exemplo.

Conforme demonstrado, com a previsão dos dez princípios do Artigo 6º da Lei Geral de Proteção de Dados, espera-se dos agentes de tratamento que suas condutas sejam éticas, sérias e responsáveis.

### **1.3. HIPÓTESES DE TRATAMENTO**

Para realizar qualquer operação de tratamento de dados pessoais, os agentes de tratamento, que são os controladores e operadores, precisam respeitar todos os princípios da lei. Além disso, precisam enquadrar a finalidade do tratamento que estão realizando a pelo menos uma das hipóteses de tratamento dispostas pela lei, também chamadas de bases legais, dando legitimidade ao tratamento realizado. A LGPD apresenta hipóteses de tratamento específicas para dado pessoal (artigo 7º), para dado pessoal sensível (artigo 11) e para dados pessoais de crianças e adolescentes (artigo 14).

## **2. DO TRATAMENTO DOS DADOS**

### **2.1. HIPOTESES DE TRATAMENTO DE DADOS PESSOAIS**

#### **2.1.1. MEDIANTE AUTORIZAÇÃO DO TITULAR**

O consentimento do titular do dado é a permissão que ele dá para que o tratamento de seus dados pessoais ocorra. Contudo, para que o consentimento seja válido, ele deve ter sido fornecido de forma livre, inequívoca e específica.

Caso haja mudança quanto à finalidade para a qual o consentimento para tratamento de dado foi concedido, o titular deve ser informado para que novamente expresse se aceita ou não o tratamento.

O devido consentimento pode ser dado por qualquer meio, seja eletrônico, físico, em áudio/vídeo ou verbal, cabendo inclusive ao agente de tratamento a prova do livre consentimento por cláusula destacada que esclareça a finalidade, a forma, a duração do tratamento, a identificação do controlador e seus dados de contato, se há compartilhamento de dados com outros agentes, as responsabilidades de cada agente que fará o tratamento e os direitos que assistem ao titular do dado.

Vale ainda salientar que pode o titular revogar o consentimento a qualquer momento de forma simples, fácil e gratuita, inclusive se outros agentes de tratamento tiverem a detenção do mesmo dado.

#### **2.1.2. PARA CUMPRIMENTO DE OBRIGAÇÃO LEGAL OU REGULÁTORIA**

Outra base legal que justifica o tratamento de dados é o cumprimento de uma obrigação legal ou regulatória. O tratamento do dado poderá ser justificado com essa base legal todas as vezes que o dado tiver de ser tratado em razão da exigência de uma lei ou de um órgão regulador.

Como exemplo, tem-se a necessidade de se solicitar ao consumidor, titular do dado, seu nome, CPF e endereço com finalidade de emissão de nota fiscal.

A emissão de nota fiscal para compra de um produto é uma obrigação legal para o vendedor. Assim, bastará que o agente de tratamento informe com clareza ao titular do dado quais dados pessoais dele serão tratados em razão da necessidade de cumprimento da obrigação de emissão de nota fiscal.

### **2.1.3. PARA EXECUÇÃO DE POLÍTICAS PÚBLICAS PREVISTAS EM LEI E REGULAMENTOS, OU RESPALDADAS EM CONTRATOS, CONVÊNIOS E OUTROS INSTRUMENTOS**

A solicitação de dados pessoais para fins de execução de políticas públicas é outra base legal que legitima o tratamento de dados. Assim, o tratamento é justificado para atender o interesse público em promover alguma política prevista em lei ou regulamento, ou ainda baseada em contratos, convênios e outros instrumentos, em benefício da sociedade. Como exemplo dessa hipótese temos o tratamento para fins de cadastro no programa bolsa família, o qual exige dos participantes que forneçam dados como nome, CPF, endereço, data de nascimento, estado civil, dentre outros.

### **2.1.4. PARA REALIZAÇÃO DE ESTUDOS POR ÓRGÃOS DE PESQUISAS**

A realização de estudos por órgãos de pesquisa também é uma hipótese de tratamento de dados pessoais que pode ser utilizada. Assim, os órgãos de pesquisa não precisarão obter o consentimento de cada um dos titulares de dados.

É importante contextualizar que, para a Lei Geral de Proteção de Dados, “órgão de pesquisa” é o 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, conforme definido no inciso XVIII do artigo 5º da LGPD. Cabe destacar a proibição da lei para que pessoas jurídicas de direito privado, com fins lucrativos, se utilizem dessa hipótese de tratamento.

Ademais, deverá o órgão de pesquisa, sempre que possível, realizar a anonimização dos dados pessoais, bem como deverá esclarecer o titular do dado, antes da pesquisa, a respeito da finalidade, adequação e necessidade da coleta dos dados para a pesquisa. Um exemplo de aplicação dessa base legal é a pesquisa de intenção de voto.

### **2.1.5. PARA EXECUÇÃO DE CONTRATOS OU DE PROCEDIMENTOS PRELIMINARES, DO QUAL SEJA PARTE O TITULAR, A PEDIDO DO TITULAR DOS DADOS**

A execução de um contrato ou procedimento preliminar a pedido do titular ou no qual ele seja parte é uma base legal para tratamento de dados pessoais. Nesse caso, o tratamento de dados se dará a pedido do próprio titular, o que se assemelha a uma forma de consentimento prévio para elaboração do contrato, sendo que o tratamento dos dados deverá estar justificado, com informação da finalidade, adequação e necessidade diretamente ao titular do dado, atendendo, assim, aos princípios da LGPD. Um exemplo é o fornecimento de seus dados a um corretor de imóveis para que seja feita a proposta de compra de um imóvel e, se aceita, o contrato de compra e venda em si.

### **2.1.6. PARA EXERCÍCIO REGULAR DE DIREITOS EM PROCESSO JUDICIAL, ADMINISTRATIVO OU ARBITRAL**

Outra hipótese de tratamento de dados que a LGPD trouxe é para exercício regular de direitos em processo judicial, administrativo ou arbitral. Ter que buscar o consentimento da parte adversária para poder usar os dados dela em um processo seria um contrassenso.

Assim, legitimado estará o tratamento de dados feito através dessa hipótese desde que usando os dados exclusivamente para a finalidade estabelecida, qual seja, exercício regular de direitos em processo judicial, administrativo ou arbitral.

### **2.1.7. PARA A PROTEÇÃO DA VIDA OU DA INCOLUMIDADE (CONDIÇÃO) FÍSICA DO TITULAR OU DE TERCEIRO**

Trata-se de legitimação de tratamento de dados pessoais excepcional, quando o titular do dado ou terceiro precisar de proteção para sua vida ou sua condição física, e não for possível obter deles qualquer consentimento (por se tratar de uma situação emergencial, por exemplo).

Assim, por força desta base legal, atendimentos para proteção da vida do titular do dado, com tratamento de seus dados pessoais, estão legitimados. Pode-se citar como exemplo uma pessoa acidentada e inconsciente, que tenha sua carteira coletada para que dados pessoais que a identifiquem sejam tratados com a finalidade de preencher sua ficha de atendimento médico. Ainda não estamos falando de dados pessoais sensíveis.

### **2.1.8. PARA A TUTELA DA SAÚDE, EXCLUSIVAMENTE, EM PROCEDIMENTO REALIZADO POR PROFISSIONAIS DE SAÚDE, SERVIÇOS DE SAÚDE OU AUTORIDADE SANITÁRIA**

Esta é uma base legal que legitima o tratamento de dados pessoais para proteção da saúde do titular, desde que realizado por profissionais da saúde ou autoridade sanitária, sendo um desdobramento da hipótese de tratamento do item anterior. O diferencial é que, nesta hipótese, estamos falando de tratamento solicitado ou buscado pelo próprio titular. Veja que ainda não estamos falando de dados sensíveis relacionados à saúde do titular, que possuiu outra base de tratamento e será visto logo mais, mas sim de dados pessoais diretos, dados simples, tais como dados cadastrais necessários para a tutela da saúde.

### **2.1.9. QUANDO NECESSÁRIO PARA ATENDER AOS INTERESSES LEGÍTIMOS DO CONTROLADOR OU DE TERCEIRO**

A hipótese de tratamento do legítimo interesse é aquela que, por ser mais flexível, poderá ser utilizada para justificar o tratamento de muitos dados pessoais. Contudo, para que tal hipótese seja usada de forma válida, é necessário que, além do legítimo interesse do controlador em efetivar o tratamento de dados, o tratamento seja realizado para situações de apoio e promoção da atividade do controlador e em respeito às legítimas expectativas do titular do dado, observando seus direitos e liberdades individuais, em situações que beneficiem o titular do dado.

Ou seja, apesar de flexível, a base legal do legítimo interesse requer o equilíbrio entre o interesse do controlador em promover sua atividade e a expectativa do titular com essa promoção.

Se o titular tem a expectativa da promoção ou se o tratamento dos dados ferir alguns de seus direitos e liberdades fundamentais, os interesses dele vão se sobrepor ao interesse do controlador de tratamento de dados, não sendo válida a base legal do legítimo interesse para o caso específico.

Ademais, a LGPD, que em seu artigo 5º esclarece o sentido de vários termos usados pelo legislador, não trouxe a definição do que seria o legítimo interesse, não havendo referência para se estabelecer até que ponto o legítimo interesse do controlador ou do terceiro poderia se sobrepor ao do titular do dado. Assim, caberá a Autoridade Nacional de Proteção de Dados preencher as várias lacunas existentes na LGPD.

### **2.1.10. PROTEÇÃO DO CRÉDITO**

O processamento de dados pessoais para fins de proteção do crédito também é uma das bases legais da LGPD. Ela justifica o tratamento de dados pessoais relativos ao inadimplemento (maus pagadores) e adimplemento (cadastro positivo) dos titulares dos dados, visando a realização de operações de crédito, por exemplo.

## **2.2. HIPÓTESES DE TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS**

Os dados pessoais sensíveis são objeto de proteção mais específica pela LGPD, já que, além de serem dados relativos à privacidade dos titulares, são dados que retratam a esfera íntima do indivíduo e que podem ser utilizados para fins discriminatórios.

A LGPD estabeleceu oito bases legais aptas a serem utilizadas pelos agentes de tratamento, que serão abordadas a seguir.

### **2.2.1. MEDIANTE O CONSENTIMENTO**

A base legal do consentimento para tratamento de dados pessoais sensíveis, além de ter que observar todos os requisitos da hipótese de consentimento de dados da hipótese pessoais não sensíveis, isto é, o consentimento tem que ser dado de forma livre, inequívoca e específica. Deverá ser, ainda, específico e destacado, seguindo as demais obrigações que constam na lei, como indicar a finalidade específica do tratamento, o prazo de duração, o compartilhamento de dados, dentre outros. O consentimento para autorização dado de forma genérica é considerado nulo.

### **2.2.2. SEM O CONSENTIMENTO**

O artigo 11 da LGPD previu a possibilidade de tratamento de dados pessoais sensíveis, sem consentimento do titular do dado. Tal tratamento se dará nas seguintes hipóteses: 1) Cumprimento de obrigação legal ou regulatória pelo controlador; 2) Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; 3) Realização de estudos por órgão de pesquisa; 4) Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral; 5) Proteção da vida ou da incolumidade física do titular ou de

terceiros; 6) Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

As seis hipóteses listadas acima foram analisadas individualmente no tópico 4.1, relativo ao tratamento de dados pessoais e, por essa razão, não será feita outra abordagem neste momento. Tudo que foi detalhado no referido tópico se aplica às mesmas hipóteses, mas agora relacionadas ao tratamento dos dados pessoais sensíveis.

O que deve ficar claro é que a utilização de qualquer uma dessas bases legais para tratamento de dados pessoais sensíveis só deve ocorrer se realmente for indispensável para a empresa tratar o dado sensível e deve ser analisado em conjunto com a necessidade de tratamento, com como observados os princípios da finalidade e adequação.

A hipótese de tratamento que foi acrescida para tratamento de dados pessoais sensíveis foi para garantia da prevenção à fraude e a segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, constante no artigo 11, alínea "g" da LGPD, e estando diretamente relacionada ao tratamento de dados biométricos.

No caso da garantia da prevenção à fraude é tutelado o interesse do agente de tratamento e de terceiros, que visam a utilização de dados pessoais sensíveis do titular, como a impressão digital, para prevenirem uma fraude.

Como exemplo podemos citar o acesso a um aplicativo bancário por meio de impressão digital.

É importante dizer que o tratamento de dados pessoais sensíveis deve respeitar e atender aos demais requisitos impostos pela LGPD, em especial os princípios insertos no artigo 6º e os direitos dos titulares de dados, dispostos no artigo 8º, §5º, e nos artigos 9º, 17, 18 e 20.

Merece destaque, ainda, que é proibido o compartilhamento de dados pessoais sensíveis relativos à saúde entre controladores, com objetivo de obter vantagem econômica. A lei estipulou exceção à essa regra nas hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, quando realizados em benefício do titular do dado, ou para realizar a portabilidade do contrato entre planos de saúde, por exemplo, e relativo a transações financeiras e administrativas resultantes do uso e da prestação do serviço em si.

Por fim, deve ser mencionado que as operadoras de planos privados de saúde estão proibidas de realizar tratamento de dados pessoais com objetivo de fazer seleção de risco, seja na contratação ou exclusão dos seus clientes (os titulares de dados).

O legislador se preocupou em inserir tal proibição para que os planos de saúde, após analisarem os dados pessoais sensíveis de seus pacientes, não pudessem excluir os que tivessem doenças que gerariam custos maiores para os planos de saúde, ou para negar a contratação de seus planos de saúde a titulares de dados que têm doenças graves.

### 2.3. HIPÓTESES DE TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES

A possibilidade de tratamento de dados pessoais de crianças e adolescentes está prevista no artigo 14 da Lei Geral de Proteção de Dados Pessoais e conta com apenas uma hipótese. O consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal (tutor, curador ou guardião), sendo que o tratamento deverá ser realizado visando o interesse da criança e do adolescente.

A lei trouxe uma exceção para que o tratamento de dado do menor seja feito sem o consentimento, que se dá exclusivamente para que seja possível utilizar o dado para contatar um dos pais ou o responsável legal, só podendo ser utilizado uma única vez, sem possibilidade de armazenamento, não podendo ser compartilhado com terceiro sem consentimento.

Ademais, a lei estabelece a obrigação do controlador em manter de forma pública as informações sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos dos titulares de dado. Cabe ao controlador, também, realizar esforços razoáveis para se certificar de que o consentimento recebido para tratamento do dado do menor foi dado por um dos pais, ou por responsável legal, o que pode ser feito através de um mecanismo de autorização enviado para o e-mail de um dos pais do menor, por exemplo.

Além disso, os controladores devem cuidar para que processem o mínimo de dados pessoais de menores possível, ou seja, o estritamente necessário, quando necessários para participação ou acesso de crianças e adolescentes a jogos, aplicações de internet e outras atividades, devendo as informações sobre o tratamento de dados realizado ser fornecida de maneira simples, clara e acessível, tanto para o menor quanto para os pais ou

para o responsável legal, buscando facilitar o entendimento da criança sobre o tratamento em si, podendo ser usado nessa explicação recursos audiovisuais, se necessário, ou outros meios lúdicos.

## **3. DO DIREITO**

### **3.1. DIREITOS DOS TITULARES DE DADOS**

Os titulares de dados possuem um numeroso rol de direitos assegurados pela LGPD que são estabelecidos em vários artigos da lei, como os artigos 8º (§5º), 9º, 17, 18 e 20.

No parágrafo 5º do artigo 8º temos o direito à revogação do consentimento dado para tratamento de dados pessoais. Neste caso, o titular poderá entrar em contato com o controlador para dizer que não mais permitirá o tratamento, devendo o mesmo ser interrompido.

No artigo 9º temos o direito de acesso facilitado às informações sobre o tratamento dos dados pessoais, cabendo aos agentes de tratamento disponibilizar de forma clara, adequada e ostensiva a finalidade do tratamento, bem como sua forma e duração, além da identificação do controlador e seu contato, informações sobre o compartilhamento de dados, sua finalidade, a responsabilidade dos agentes de tratamento e os direitos constantes no artigo 18 da LGPD.

O direito à titularidade do dado pessoal está assegurado no artigo 17, não podendo o titular do dado renunciar, ceder ou transferir a terceiros seus direitos por força do artigo 112 do Código Civil, tendo em vista que o dado pessoal inclui a identidade de um indivíduo e por isso é um direito da personalidade.

No artigo 18 da LGPD estão dispostos vários direitos, que serão mencionados e explicados nas subseções a seguir:

#### **3.1.1. DIREITO A CONFIRMAÇÃO DE EXISTÊNCIA DE TRATAMENTO**

É garantido ao titular do dado o direito de obter dos agentes de tratamento a confirmação de que seus dados pessoais são tratados pela empresa. Caso a solicitação seja em formato simplificado, um mero sim ou não sobre a existência do tratamento deverá ser respondido ao titular de forma imediata. Caso haja solicitação, os agentes de tratamento terão o prazo de 15 dias para responder.

### **3.1.2. DIREITO DE ACESSO AOS DADOS**

Aos titulares do dado é garantido o direito de acesso aos seus dados pessoais, obtendo dos agentes de tratamento uma cópia deles, que deverá ser disponibilizada por meio eletrônico ou de forma impressa, à escolha do titular do dado.

### **3.1.3. DIREITO DE CORREÇÃO DOS DADOS INCOMPLETOS, INEXATOS OU DESATUALIZADOS**

O titular do dado tem o direito de solicitar a correção de seus dados incompletos, inexatos ou desatualizados. Assim, além de um direito, trata-se do respeito aos princípios da qualidade dos dados e da transparência.

### **3.1.4. DIREITO DE ANONIMIZAÇÃO, BLOQUEIO OU ELIMINAÇÃO DE DADOS DESNECESSÁRIOS, EXCESSIVOS OU TRATADOS EM DESCONFORMIDADE COM A LEI**

É garantido ao titular do dado o direito de anonimização, bloqueio ou eliminação dos dados tratados, desde que seja constatado que os dados tratados são excessivos ou desnecessários para a finalidade para a qual foram coletados, ou se estiverem sendo tratados com finalidade diversa. Caso o titular solicite a anonimização, bloqueio ou eliminação, o controlador deverá comunicar aos agentes de tratamento com os quais compartilhou os dados para que também executem a operação.

### **3.1.5. DIREITO DE PORTABILIDADE DOS DADOS A OUTRO FORNECEDOR DE SERVIÇO OU PRODUTO**

O titular do dado tem o direito de solicitar a portabilidade de seus dados pessoais para outro controlador. Tal solicitação precisa ser expressa e, havendo base legal que justifique a permanência dos dados com o antigo controlador, como por exemplo cumprimento de obrigação legal ou regulatória, os dados permanecerão com ele.

A Autoridade Nacional de Proteção de Dados poderá estabelecer padrões de capacidade de diversos sistemas para fins de portabilidade e ainda regulará o assunto.

### **3.1.6. DIREITO DE ELIMINAÇÃO DOS DADOS PESSOAIS TRATADOS COM O CONSENTIMENTO DO TITULAR**

É garantido ao titular do dado o direito de ter seus dados pessoais eliminados quando a base legal utilizada para tratamento tenha sido o consentimento. Contudo, não serão eliminados dados que tenham outras bases legais em suas finalidades, como cumprimento de obrigação legal ou regulatória pelo controlador, estudo por órgãos de pesquisas, para uso exclusivo do controlador, desde que anonimizado e vedado acesso por terceiro.

Dados coletados para finalidade de marketing e meramente cadastrais serão eliminados. Caso o titular solicite a eliminação, deverá o controlador comunicar aos demais agentes de tratamento com os quais compartilhou os dados para que também executem a operação.

### **3.1.7. DIREITO DE INFORMAÇÃO DAS ENTIDADES PÚBLICAS E PRIVADAS COM AS QUAIS O CONTROLADOR REALIZOU USO COMPARTILHADO DE DADOS**

O titular do dado tem o direito de saber com quais agentes de tratamento e quais de seus dados pessoais foram compartilhados, inclusive sendo informado sobre qual finalidade.

Além de ser um direito do titular, é um dever dos agentes de tratamento em decorrência do princípio da transparência. As informações genéricas de que os dados são compartilhados com terceiros não atendem as exigências da LGPD.

### **3.1.8. DIREITO DE INFORMAÇÃO SOBRE A POSSIBILIDADE DE NÃO FORNECER CONSENTIMENTO E SOBRE AS CONSEQUÊNCIAS DA NEGATIVA**

É direito do titular do dado ter informações sobre as consequências de não dar o seu consentimento para tratamento de seus dados pessoais. Para isso, o controlador deverá informar ao titular quais as limitações ou impedimentos ele terá em decorrência da negativa, prejuízos na navegação do site, por exemplo, ou impossibilidade de elaboração de uma proposta, facultando ao titular conceder ou não seu consentimento.

Agindo dessa maneira o controlador está garantindo que o consentimento fornecido pelo titular tenha sido realmente livre.

Direito de revogação do consentimento: poderá o titular, a qualquer momento, revogar, desde que de forma expressa, o consentimento dado para tratamento de seus dados

personais, através de procedimento gratuito e facilitado. Os tratamentos realizados até a data de solicitação continuam válidos.

No artigo 20 da LGPD está disposto o direito à revisão unicamente de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais. Com a utilização de inteligência artificial em muitos setores, inclusive para aprovação de crédito com base em análise de perfis, é importante que tal direito tenha sido consagrado na lei. Assim, poderá o titular do dado solicitar que a decisão que afete seus interesses seja revisada, devendo o controlador fornecer, quando solicitado, informações claras e adequadas a respeito do critério e procedimentos utilizados para a realização da decisão automatizada, resguardado o segredo comercial e industrial.

A lei também dispõe sobre o direito do titular do dado de apresentar reclamação aos agentes de tratamento relativamente ao tratamento de seus dados.

## 4. DAS PENALIDADES, DO COMPARTILHAMENTO E DA ADEQUAÇÃO

### 4.1. DAS PENALIDADES ADMINISTRATIVAS PELO DESCUMPRIMENTO DA LEI

O tratamento de dados pessoais realizado em desconformidade com a LGPD sujeitará os agentes de tratamento às penalidades administrativas que estão dispostas no artigo 52 da lei, que somente poderão ser aplicadas pela autoridade nacional de proteção de dados após o devido processo administrativo, no qual deverá ser oportunizada a ampla defesa.

As penalidades que poderão ser aplicadas são:

- I - advertência, com indicação de prazo para adoção de medidas corretivas;
- II - 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 a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- III - multa diária, observado o limite total de R\$ 50.000.000,00 (cinquenta milhões de reais);
- IV - publicação da infração após devidamente apurada e confirmada a sua ocorrência;
- V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- VI - eliminação dos dados pessoais a que se refere a infração;
- X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
- XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
- XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (BRASIL, 2018, p.1)

As penalidades que poderão ser aplicadas pelo descumprimento da lei são pesadas. A possibilidade de multa de até 2% do faturamento bruto da empresa (podendo aqui ser considerado todo o grupo ou conglomerado no Brasil), por infração cometida e por dia, pode alcançar valores altíssimos e está limitada a R\$ 50.000.000,00 (cinquenta milhões de reais).

Em comparação ao limite de multa estabelecido no Código de Defesa do Consumidor, por exemplo, que é de aproximadamente R\$ 9,7 milhões de reais atualmente, percebe-se que o legislador realmente buscou ser rigoroso com a aplicação da sanção pecuniária.

A penalidade de publicização da infração é, também, consideravelmente danosa, uma vez que ao dar publicidade ao descumprimento da lei a empresa poderá sofrer um grande dano reputacional, reduzindo seu valor de mercado e da marca e levando à perda de clientes, que, inseguros quanto a política de tratamento de dados pessoais da empresa, buscarão os concorrentes dela no mercado para terem os mesmos produtos ou serviços.

As penalidades de bloqueio e suspensão parcial do banco de dados e suspensão ou proibição do exercício da atividade de tratamento dependente da atividade da empresa, também poderão ser muito prejudiciais para ela, já que que podem inviabilizar a continuidade da atividade da empresa.

A legislação também estabeleceu que as penalidades serão aplicadas de forma gradativa, podendo ser isoladas ou cumulativas e devem ser levados em consideração para a aplicação da pena:

- I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
  - II - a boa-fé do infrator;
  - III - a vantagem auferida ou pretendida pelo infrator;
  - IV - a condição econômica do infrator;
  - V - a reincidência;
  - VI - o grau do dano;
  - VII - a cooperação do infrator;
  - VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
  - IX - a adoção de política de boas práticas e governança;
  - X - a pronta adoção de medidas corretivas; e
  - XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.
- (BRASIL, 2018, p.1)

Assim, apesar do vultoso valor máximo da multa por descumprimento da LGPD saltar aos olhos, as demais penalidades que poderão ser impostas, após o devido processo administrativo, também são pesadas, o que deve ser levado em consideração pelos agentes de tratamento para que busquem se adequar à lei, realizando o tratamento de dados respeitando a legislação.

Por fim, destacamos que a LGPD não afastou ou substituiu a aplicação de sanções administrativas, civis ou penais, dispostas no Código de Defesa do Consumidor ou em outras legislações específicas, e que poderão ser propostas ações judiciais, individuais ou coletivas, para proteção dos direitos dos titulares de dados, o que significa que podem ser aplicadas penalidades por outros órgãos administrativos, como PROCON, Ministério

Público e Secretaria Nacional do Consumidor, sem prejuízo de propositura de demandas judiciais para buscar reparação de danos.

A lei geral de proteção de dados só entrou em vigor em agosto de 2020, mas é possível observar toda uma movimentação, principalmente do Ministério Público e da Secretaria Nacional do Consumidor, no sentido de buscar a proteção de direitos dos consumidores, que inevitavelmente são titulares de dados pessoais.

#### 4.2. COMPARTILHAMENTO DE DADOS DE EMPRESAS CONTROLADORAS COM EMPRESAS OPERADORAS E A NECESSIDADE DE ELABORAÇÃO DE CONTRATO

O controlador é a pessoa, natural ou jurídica, com a qual o titular do dado tem o primeiro contato, ao ter interesse em obter algum produto ou serviço. Então, é com essa pessoa (normalmente empresa) que o titular do dado se relaciona e, após esclarecer sobre a atividade de tratamento que será realizada com seus dados pessoais (o que pode ter sido informado através de uma política de uso do site, por exemplo, na qual o controlador buscou atender todos os princípios do artigo 6º da LGPD e deu transparência para toda a atividade de tratamento de dados), o controlador informa ao titular com quais empresas operadoras os dados pessoais do titular serão compartilhados, explicando a necessidade, finalidade.

Difícilmente encontraremos controladores que não precisam compartilhar os dados pessoais com empresas operadoras, já que para a realização de um serviço certamente o controlador terá que contratar algumas empresas para executar serviços que ele, por si só, não consegue fazer.

Vejamos o exemplo de uma loja de vendas on-line. A loja é o controlador. É ela que recebe o contato inicial do titular do dado e que trata seus dados. Contudo, a loja não tem condições de ter um departamento interno de contabilidade e, para isso, contratou uma empresa para realizar os serviços contábeis. Essa empresa, que é uma operadora, terá acesso aos dados pessoais dos clientes da controladora, vez que precisará deles para atender a obrigações legais ou regulatórias, por exemplo.

A loja de vendas on-line pode precisar contratar uma empresa de publicidade para fazer marketing de seus produtos e essa empresa poderá ter acesso a dados pessoais de clientes para mandar e-mails com produtos ou promoções que possam ser de interesse do cliente (titular do dado).

Para que o site fique no ar, é necessário contratar um serviço de hospedagem, que poderá fornecer o servidor no qual estarão dados pessoais dos titulares de dados, ou seja, dos clientes da empresa.

Em um exemplo simples, identificamos três empresas distintas que podem ter acesso aos dados pessoais coletados pela controladora. Isso é compartilhamento de dados. Todas essas empresas agiram na qualidade de operadoras ao realizarem um tratamento a pedido da controladora.

O titular tem o direito de saber quais são essas outras pessoas (físicas ou jurídicas) que estão tendo acesso aos seus dados pessoais, e o controlador tem que se preocupar com a maneira que o operador cuida dos dados pessoais que ele coletou, uma vez que há responsabilidades e obrigações a serem atendidas.

A lei geral de proteção de dados pessoais permite que os dados pessoais sejam compartilhados entre controlador e operador. Para tanto, é necessário observar os direitos dos titulares de dados, em especial o de transparência para que ele saiba quem são as outras pessoas que tratarão seus dados, a finalidade e tempo de duração do tratamento, dentre outros, assim como as obrigações impostas pela LGPD para os agentes de tratamento.

Tanto o controlador como os operadores devem manter registros das operações de tratamento de dados pessoais que realizam.

E extremamente necessário que exista um contrato escrito entre controlador e operador no qual conste: os direitos e obrigações de cada um deles; o tratamento de dados pessoais que será realizado; a relação dos tipos de dados que serão tratados e sua finalidade; a vedação para tratamento diverso do que foi estabelecido pelo controlador; as instruções para realização do tratamento; a exigência de que o operador adote medidas de segurança, técnicas e administrativas para proteger os dados pessoais que serão tratados por ele de acesso não autorizado, perdas acidentais ou ilícitas, destruição, alteração ou qualquer forma de tratamento inadequado; a responsabilidade pela segurança dos dados e que defina direito de regresso do controlador contra o operador em caso de dano; a possibilidade do controlador de realizar auditorias para verificar se a afirmação de que o operador está em adequação com a LGPD é verdadeira; a obrigação do operador em colaborar com o controlador no cumprimento do exercício dos direitos dos titulares; a obrigação de informar ao controlador sobre a ocorrência de violação aos dados pessoais,

dispor sobre eliminação ou devolução dos dados após o encerramento do contrato, dentre outros.

Assim, conclui-se que é de extrema importância e relevância ter um bom e claro contrato entre controlador e operador, Vale lembrar que a lei estabelece hipóteses em que os dois responderão solidariamente, razão pela qual um contrato bem escrito tratando das obrigações e responsabilidades de cada um dos agentes é medida necessária.

Por fim, considera-se ser bem provável que as empresas controladoras, ao contratarem empresas operadoras para executarem atividades que necessitem de tratamento de dados pessoais, passarão a exigir não somente um contrato bem elaborado, mas também solicitarão as políticas de uso e de segurança para verificarem as medidas técnicas e organizacionais que são praticadas pela empresa operadora, com fim de reduzir os riscos na contratação de fornecedores.

#### 4.3. ENCARREGADO DE DADOS, SUA COMUNICAÇÃO COM A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS E O TITULAR DO DADO, E SEU PERFIL

O encarregado de dados é uma pessoa, física ou jurídica, contratada pelo controlador e que terá uma atuação de intermediador entre o titular do dado e a empresa controladora, e entre ela e a Autoridade Nacional de Proteção de Dados. Isto é, o encarregado é o canal de comunicação com ambos, sendo obrigatória a divulgação pública da identidade e meios de contato com ele (e-mail, telefone, ou formulário on-line, por exemplo).

A princípio, a indicação de um encarregado por uma empresa controladora é obrigatória. Contudo, o §3º do artigo 41 prevê a possibilidade da Autoridade Nacional estabelecer normas complementares sobre as atribuições do encarregado ou da possibilidade de ser dispensada sua indicação, de acordo com a natureza e porte da empresa controladora.

Espera-se que o profissional que vai desempenhar a função de encarregado de dados tenha conhecimentos de privacidade e proteção de dados.

## **5. A ADEQUAÇÃO E A PRIVACIDADE**

### **5.1. PASSO A PASSO PARA UM PROGRAMA DE ADEQUAÇÃO À LGPD**

Existem no mercado vários modelos e metodologias para elaboração e implantação de um programa de adequação da empresa à Lei Geral de Proteção de Dados.

Alguns apresentam duas fases (preparatória e execução), outros são mais detalhados, podendo ser divididos em até cinco fases, tal qual como sugerido pelo DMPS – Data Protection Management System (preparação, organização, implementação, governança e avaliação).

Independentemente da metodologia a ser utilizada ou do nome dado ao programa, o que realmente importa é que seja feita uma análise séria e criteriosa dos dados pessoais e processos utilizados pela empresa e que o programa desenvolvido passe a fazer parte da rotina da empresa, com uma mudança cultural, com fim de efetivamente proteger o uso os dados pessoais contra o uso em desconformidade com a Lei.

#### **5.1.1. A CONSCIENTIZAÇÃO DA EMPRESA PARA SUCESSO DO PLANO DE AÇÃO PARA ADEQUAÇÃO À LGPD**

É certo que todas as empresas que realizam tratamento de dados pessoais no Brasil, ou que o tratamento tenha por objetivo a oferta ou fornecimento de bens ou serviços para pessoas localizadas no Brasil, ou cujo tratamento de dados tenha ocorrido no território nacional, terão que se adequar à LGPD.

O trabalho de adequação deve começar com a mudança de pensamento da alta gerência da empresa, que deve compreender que a minimização de dados pessoais que são coletados em suas atividades representa respeito e transparência com os seus clientes, os titulares dos dados, e também que quanto menos dados pessoais forem tratados, mais fácil será para a empresa exercer o controle sobre eles.

A partir do momento que a alta gerência está engajada em buscar a adequação da empresa à lei geral de proteção de dados pessoais, passa-se a conscientizar todos os colaboradores e funcionários da empresa.

Trata-se, assim, de uma mudança cultural dentro da empresa, que passará a ter um olhar mais atento quanto à proteção dos dados pessoais que são ali tratados. Os próprios funcionários e colaboradores podem ajudar a identificar quais dados pessoais são processados na empresa e onde estão armazenados, podendo, ainda, esclarecer a necessidade ou não da coleta de determinados dados.

Assim, conscientizar os colaboradores da empresa é um passo chave no processo de adequação à LGPD. Um funcionário despreparado é uma ameaça interna constante à segurança da empresa, que poderá compartilhar dados pessoais sem qualquer intenção de prejudicar a corporação, mas, mesmo assim, estará causando um vazamento de dados, repassando a um terceiro, sem autorização, acesso aos dados pessoais, descumprindo a legislação e colocando a empresa em situação de risco.

### **5.1.2. O MAPEAMENTO DE DADOS**

Para realizar o mapeamento dos dados é possível comprar softwares que farão uma varredura nos sistemas da empresa. Existem muitas soluções disponíveis no mercado, contudo, a conformidade e adequação com a LGPD não é apenas o mapeamento dos dados. Esta talvez seja apenas a etapa mais demorada.

Sugere-se que o mapeamento dos dados pessoais tratados na empresa seja realizado de forma manual e individualizada em cada departamento. Entrevistas com os gestores de cada divisão (recepção, jurídico, compras, vendas, contabilidade, marketing, administrativo, financeiro, TI, recursos humanos, por exemplo) são necessárias para identificar quais dados pessoais são coletados naquela seção, e a necessidade daqueles dados para os processos que são realizados.

O mapeamento de dados pessoais identificará os dados em si, se são dados sensíveis ou não, bem como a forma de entrada deles na organização, quais pessoas têm acesso àqueles dados, por quanto tempo esses dados estão armazenados, onde estão armazenados e a necessidade de uma coleta, se são dados físicos, dados de aplicativos, de páginas da internet ou dados de terceiros.

Realizado o mapeamento, você terá em mãos o fluxo de entrada dos dados pessoais na empresa, o ciclo de vida daquele dado, o motivo pelo qual os dados foram tratados e, assim, terá melhores condições de analisar as bases legais que podem justificar o tratamento dos dados coletados e o período de armazenamento necessário de acordo com a base legal

utilizada. É importante estabelecer no mapeamento o prazo de armazenamento do dado pessoal, haja vista que o titular do dado poderá solicitar a exclusão dos seus dados pessoais, e a empresa precisará justificar a impossibilidade de fazê-lo, caso o tratamento tenha sido justificado em base legal distinta do consentimento.

Até pouco tempo era comum que as empresas coletassem o máximo de dados pessoais. Contudo, com a publicação da LGPD e a responsabilização da empresa pela segurança dos dados pessoais coletados, buscar minimizar a quantidade de dados coletados é uma boa prática, processando apenas os dados que efetivamente sejam necessários para a finalidade do tratamento.

Por fim, os dados tratados não poderão ficar em poder dos agentes de tratamento por prazo indeterminado. Eles deverão ser eliminados após o término do tratamento, de acordo com a finalidade e prazo estipulados, ou quando deixarem de ser necessários ou pertinentes para a finalidade para o qual foram tratados, ou ainda quando determinado pela Autoridade Nacional de Proteção de Dados, em razão de violação da LGPD, e, também, mediante solicitação do titular, caso haja revogação do consentimento dado.

### **5.1.3. LEVANTAMENTO DE LEIS, REGULAMENTOS, POLÍTICAS, CÓDIGOS E ANÁLISE DE CONTRATOS**

Outro ponto importante em um programa de adequação à LGPD é o levantamento de leis e regulamentos que podem ser aplicáveis à atividade da empresa, e buscar o diálogo deles com a Lei Geral de Proteção de Dados Pessoais, isto é, identificar seus princípios e obrigações, para que se verifique as normas às quais a empresa esteja submetida por força de alguma regulamentação e que deverão ser absorvidas nas políticas da empresa.

É nesse momento, também, que a empresa entrega sua política de privacidade, seu código de conduta e sua política de segurança da informação para serem analisados.

Isso deve ser feito para que se verifique as adequações que precisarão ser implementadas em atendimento à LGPD, em atenção à atividade e ao processamento de dados realizada pela empresa e o que necessitará ser criado.

A análise de todos os contratos da empresa também é necessária. Nessa análise, será verificado quais dados pessoais são tratados, seja contrato com o cliente, contrato de trabalho com colaboradores ou prestadores de serviços, contratos com empresas que serão operadoras de dados pessoais coletados pela empresa controladora, etc.

Feito esse levantamento nos contratos, deverão ser apontadas as alterações que deverão ser implementadas, seja para restringir a coleta de dados, esclarecer a finalidade do tratamento de dado ou, ainda, para estabelecer com as demais empresas operadoras como os dados pessoais que foram transferidos para elas deverão ser tratados.

Assim, são estabelecidas regras claras que deverão ser seguidas pelo operador e sua responsabilidade pelo não cumprimento de suas obrigações.

#### **5.1.4. LEVANTAMENTO DE RISCOS À PRIVACIDADE E MITIGAÇÃO DE RISCOS, COM ADOÇÃO DE MEDIDAS NECESSÁRIAS E ATENDIMENTO DAS SOLICITAÇÕES DOS USUÁRIOS**

Com a realização das entrevistas e o mapeamento de dados feito, já tendo ciência de todos os processos de tratamento de dados que são realizados na empresa, conhecendo as leis e regulamentos que a empresa precisa cumprir, as políticas e códigos de conduta da própria empresa e quem são as empresas que fazem tratamento de dados a pedido da controladora, haverá clareza para fazer um levantamento de riscos à privacidade em cada um dos processos.

Além disso, poderão ser adotadas medidas para acabar ou reduzir os riscos encontrados. Ou seja, a empresa estará apta a desenhar e executar seu projeto de adequação à LGPD através de mudança do processo, sistemas e métodos, sendo recomendado:

- 1) Criação ou ajuste dos processos de tratamento de dados pessoais;
- 2) Criação de processo para resposta de incidentes com dados pessoais;
- 3) Criação ou ajuste do processo de atendimento aos direitos dos titulares dos dados;
- 4) Criação ou ajuste de políticas para as hipóteses que autorizam o tratamento de dados pessoais, de acordo com a atividade desempenhada e o tipo de dados e a finalidade do tratamento;
- 5) Criação ou ajuste de cláusulas contratuais nos contratos com terceiros (fornecedores processadores de dados), nos contratos com clientes (titulares de dados) e com empregados;
- 6) Criação de um roteiro de boas práticas e de proteção de dados com a elaboração e implantação de um conjunto de medidas para fazer cumprir as normas legais, regulamentares e políticas, processos;

- 7) Estabelecimento de medidas técnicas e organizacionais adequadas para proteção dos dados pessoais tratados na empresa, como políticas de senha, de acesso a arquivos, definições de usuários na rede, política de backup;
- 8) Avaliação de aquisição de soluções de segurança de dados e tecnologia, bem como de equipamentos que podem ser necessários;
- 9) Avaliação da possibilidade e necessidade de contratação de seguro de riscos cibernéticos para resguardar a empresa no caso de um incidente de segurança como uma invasão ao sistema com sequestro de dados, vírus ou malware, acesso não autorizado à rede ou vazamento de dados, no qual ela seja responsabilizada;
- 10) Outras necessidades que serão identificadas quando da elaboração do plano de ação para implementação.

Caberá à alta gerência da empresa acompanhar e autorizar a modificação e implementação do processo de adequação à LGPD. Ela também deverá deliberar sobre a necessidade e possibilidade de se realizar investimentos financeiros para aquisição de soluções de segurança e tecnologia, por exemplo, para adequação à lei.

Após a implementação de todo o projeto de adequação a LGPD, no qual foram redefinidos os dados pessoais processados pela empresa controladora e empresas operadoras, os sistemas e processos de tratamento de dados, estruturado o banco de dados, elaboradas ou revisadas as políticas (de privacidade e segurança da informação) e códigos de conduta e, também, alterando ou redigindo novos contratos (com clientes, empregados e fornecedores), e criado o processo para atendimento da demanda dos titulares de dados, deverá ser feito novo treinamento e conscientização dos colaboradores, para que as novas práticas, em especial de proteção de dados e privacidade, sejam internalizadas.

As empresas terceiras, operadoras de dados pessoais para a empresa controladora, deverão ser advertidas de suas responsabilidades com o tratamento de dados pessoais que são compartilhados com elas para determinada finalidade, assinando novo contrato de prestação de serviços ou um aditivo em que conste as regras de tratamento, obrigações e responsabilidades.

Por fim, a empresa terá que ter um departamento que atenda às demandas dos titulares de dados, devendo o funcionário responsável por esse atendimento passar por treinamento específico.

### **5.1.5. MANTENDO A ADEQUAÇÃO**

O programa de adequação a Lei Geral de Proteção de Dados normalmente requer vários meses para ser implementado e para, efetivamente, estar atendendo à lei. Não basta passar por esse processo, adequar as políticas, aos sistemas e processos e não acompanhar a manutenção do programa.

É aconselhável que periodicamente seja feito um levantamento de atualizações que podem interferir na efetiva adequação da empresa. Legislações podem ter sido alteradas ou criadas, processos internos da empresa podem ter sido criados ou descontinuados, estando a empresa coletando dados pessoais que não mais são necessários, ou tendo começado a coletar dados que não estavam catalogados. Isso resultará na necessidade de readequação dos processos e documentos da empresa.

Assim, a manutenção do processo de adequação à LGPD é contínua e serve também para que a própria empresa possa ter provas, caso eventualmente passe por uma auditoria ou seja requisitado pela Autoridade Nacional de Proteção de Dados de que possuiu condições de prestar contas ou esclarecimentos sobre os tratamentos realizados.

## CONSIDERAÇÕES FINAIS

Em um mundo em que praticamente qualquer informação está a apenas alguns cliques de distância, os dados inclusive, e os dados pessoais tornam-se um recurso de valor imensuráveis para as empresas de todos os setores, a LGPD busca regulamentar o que deveria ser ético de quem trata e manipula os dados dentro das empresas e dos dados compartilhados por ela.

A edição da lei nº 13.709/2018 trata da proteção de dados. A LGPD cria regras para o armazenamento e coleta de dados buscando oferecer segurança nas informações que são fornecidas e recebidas a todo momento. O trabalho abordou sobre a LGPD- Lei Geral de proteção de dados e seus impactos e formas de implantação nas empresas.

Como resultado da pesquisa, conclui-se que a maioria das empresas precisaram adaptar-se através de mudanças no contrato com os clientes, saneamento dos dados no sistema no sentido de solicitar dados realmente necessários, determinar um tempo para manter os dados armazenados e atualizar constantemente, contratar profissionais da área jurídica e incentivar os colaboradores a cumprirem o disposto na lei.

Através da pesquisa, pode-se observar que as empresas precisaram se adequar e adotar novos protocolos em suas atividades, pois necessitam revisar a maneira como os dados são tratados, armazenados e fornecidos quando solicitados.

Ao fim do trabalho pode-se concluir que a pesquisa realizada ampliou o conhecimento a respeito do que a Lei Geral de proteção dados coloca e formas das empresas se adequarem. Conclui-se que a privacidade de dados é de grande relevância e deve ser tratada de forma séria e com cuidado.

A Lei Geral de Proteção de Dados (LGPD) representa um marco importante na proteção da privacidade e dos direitos dos cidadãos em relação ao tratamento de seus dados pessoais. Desde sua promulgação no Brasil em 2018, a LGPD tem impactado significativamente a forma como empresas e instituições lidam com as informações pessoais de seus clientes e usuários.

Uma conclusão sobre a LGPD é que ela veio para elevar os padrões de transparência, segurança e responsabilidade no uso dos dados pessoais. Ao regulamentar o tratamento dessas informações, a legislação busca garantir que os indivíduos tenham maior controle

sobre seus dados e que as organizações sejam mais responsáveis ao coletar, armazenar, processar e compartilhar essas informações.

Com a LGPD, as empresas são incentivadas a adotar práticas mais éticas e seguras no tratamento de dados, o que pode fortalecer a confiança do público em suas atividades. Além disso, a lei estabelece regras claras e adequadas em caso de violação, o que deve atuar como um fator dissuasório contra o uso inadequado ou negligente dos dados pessoais.

No entanto, a implementação e conformidade com a LGPD podem ser desafiadoras para muitas organizações, especialmente as de menor porte. Por isso, é fundamental que as empresas se adaptem às exigências da legislação e invistam em programas de capacitação e conscientização para seus funcionários.

A LGPD está em constante evolução e, com o passar do tempo, podem surgir ajustes e entendimentos jurisprudenciais que refinem a aplicação da lei. Portanto, é essencial que empresas e indivíduos estejam sempre atualizados em relação às suas disposições e às melhores práticas em matéria de privacidade de dados.

Em resumo, a Lei Geral de Proteção de Dados representa um passo significativo para a proteção da privacidade e o fortalecimento dos direitos dos cidadãos brasileiros no crescente contexto da era digital. Seu cumprimento e entendimento são essenciais para que a sociedade alcance um equilíbrio entre a inovação tecnológica e o respeito aos direitos individuais.

## REFERÊNCIAS BIBLIOGRÁFICAS

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais, A função e os limites do consentimento**. Rio de Janeiro: Ed Forense, 2019.

BRASIL. **Lei 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/ato2015-2018/2018/lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/L13709.htm)> Acesso em: 27 jul. 2023.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção da Dados Pessoais Comentada**. São Paulo: Ed. Thomson Reuters Brasil, 2018.

MENDES, Laura Schertel Mendes. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Ed. Saraiva, 2014.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais: Comentários à Lei 13.709/2018**. São Paulo: Ed. Saraiva Educação, 2018.

UFSC. **Proteção de dados pessoais – UFSC**. Disponível em: <<https://lgpd.ufsc.br/duvidas-frequentes/>> Acesso em: 14 jul. 2023.