

**CENTRO UNIVERSITÁRIO PARA O DESENVOLVIMENTO DO ALTO VALE DO  
ITAJAÍ – UNIDAVI**

**STEFANY KRIEGER PADILHA**

**BREVES APONTAMENTOS SOBRE AS IMPLICAÇÕES JURÍDICAS DA LEI  
GERAL DE PROTEÇÃO DE DADOS NA GESTÃO EMPRESARIAL**

**RIO DO SUL**

**2023**

**CENTRO UNIVERSITÁRIO PARA O DESENVOLVIMENTO DO ALTO VALE DO  
ITAJAÍ – UNIDAVI**

**STEFANY KRIEGER PADILHA**

**BREVES APONTAMENTOS SOBRE AS IMPLICAÇÕES JURÍDICAS DA LEI  
GERAL DE PROTEÇÃO DE DADOS NA GESTÃO EMPRESARIAL**

Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Direito, pelo Centro Universitário para o Desenvolvimento do Alto Vale do Itajaí - UNIDAVI

Orientador(a): Prof. Doutor Daniel Mayerle

**RIO DO SUL**

**2023**

**CENTRO UNIVERSITÁRIO PARA O DESENVOLVIMENTO DO ALTO VALE DO  
ITAJAÍ – UNIDAVI**

A monografia intitulada “BREVES APONTAMENTOS SOBRE AS IMPLICAÇÕES JURÍDICAS DA LEI GERAL DE PROTEÇÃO DE DADOS NA GESTÃO EMPRESARIAL “, elaborada pelo(a) acadêmico(a) STEFANY KRIEGER PADILHA, foi considerada

APROVADA

REPROVADA

por todos os membros da banca examinadora para a obtenção do título de BACHAREL EM DIREITO, merecendo nota \_\_\_\_\_.

\_\_\_\_\_, \_\_\_\_ de \_\_\_\_\_ de \_\_\_\_\_.

---

Profa. M.<sup>a</sup> Vanessa Cristina Bauer  
Coordenadora do Curso de Direito

Apresentação realizada na presença dos seguintes membros da banca:

Presidente: \_\_\_\_\_

Membro: \_\_\_\_\_

Membro: \_\_\_\_\_

## **TERMO DE ISENÇÃO DE RESPONSABILIDADE**

Declaro, para todos os fins de direito, que assumo total responsabilidade pelo aporte ideológico conferido ao presente trabalho, isentando o Centro Universitário para o Desenvolvimento do Alto Vale do Itajaí, a Coordenação do Curso de Direito, a Banca Examinadora e o Orientador de toda e qualquer responsabilidade acerca do mesmo.

Rio do Sul, 05 de novembro de 2023.

**STEFANY KRIEGER PADILHA**  
**Acadêmico(a)**

Este trabalho dedico a minha família, que ao meu lado sempre estiveram e me apoiaram, sem eles não estaria hoje aqui.

## **AGRADECIMENTOS**

Primeiramente, quero agradecer aos meus pais e a minha irmã pelo apoio incondicional ao longo desta jornada. Suas palavras de incentivo e compreensão foram fundamentais para minha motivação e sucesso no curso.

Agradeço a meu noivo, da mesma forma por me auxiliar desde o início, e entender quando fora necessário abdicar de certos momentos para a realização deste trabalho.

À meu orientador Daniel Mayerle, pela orientação precisa, e conhecimentos compartilhados para o desenvolvimento deste projeto.

## RESUMO

O trabalho científico intitulado "Implicações Legais da LGPD na Gestão Empresarial" tem como principal objetivo abordar as ramificações da Lei Geral de Proteção de Dados (LGPD) no contexto da administração de empresas. O enfoque central do estudo é a demonstração das responsabilidades e limitações enfrentadas pelos agentes de proteção de dados, juntamente com as complexidades e desafios associados à implementação da LGPD nas organizações. Os objetivos específicos incluem a análise da aplicação prática da LGPD, a discussão das dificuldades encontradas para garantir a conformidade com a legislação e a exposição das limitações impostas às empresas que manipulam informações pessoais. O cerne do problema investigado reside na identificação dos principais desafios e impactos que a LGPD impõe à gestão empresarial. A hipótese formulada sugere que a conformidade à LGPD envolve desafios significativos relacionados à segurança de dados, custos operacionais, gestão de reputação e conformidade legal, impactando diretamente a confiança dos clientes e a prevenção de sanções. Além disso, supõe-se que a adaptação efetiva à LGPD pode criar oportunidades para a inovação e o desenvolvimento de estratégias empresariais centradas na proteção de dados pessoais. A metodologia adotada baseia-se em uma abordagem indutiva com um método de procedimento monográfico, com ênfase na pesquisa bibliográfica como técnica de coleta de dados. A relevância desse tema é respaldada pela crescente importância da proteção de dados pessoais em um mundo digitalmente interconectado, bem como pela necessidade de empresas compreenderem e se ajustarem à LGPD para garantir a segurança e privacidade das informações dos titulares de dados. Este estudo visa contribuir para um melhor entendimento das implicações da LGPD nas empresas, fornecendo insights cruciais para profissionais, gestores e pesquisadores que buscam garantir a conformidade com a legislação e aprimorar a gestão empresarial em um ambiente regulamentado. Cada capítulo do trabalho aborda aspectos específicos, culminando em considerações finais que sintetizam os principais pontos explorados no estudo.

**Palavras-chave:** Lei Geral de Proteção de Dados. Dados pessoais. Conformidade. Empresarial.

## **ABSTRACT**

The scientific work titled "Legal Implications of LGPD in Business Management" aims to address the ramifications of the General Data Protection Law (LGPD) in the context of corporate administration. The central focus of the study is to demonstrate the responsibilities and limitations faced by data protection agents, along with the complexities and challenges associated with the implementation of LGPD in organizations. Specific objectives include the analysis of the practical application of LGPD, the discussion of difficulties encountered in ensuring compliance with the law, and the exposure of limitations imposed on companies handling personal information. The core issue investigated lies in identifying the main challenges and impacts that LGPD imposes on business management. The formulated hypothesis suggests that LGPD compliance involves significant challenges related to data security, operational costs, reputation management, and legal compliance, directly impacting customer trust and sanction prevention. Furthermore, it is assumed that effective adaptation to LGPD can create opportunities for innovation and the development of business strategies centered on the protection of personal data. The methodology adopted is based on an inductive approach with a monographic procedure, with an emphasis on bibliographical research as the data collection technique. The relevance of this topic is supported by the growing importance of personal data protection in an increasingly interconnected digital world, as well as the need for companies to understand and adjust to LGPD to ensure the security and privacy of data subjects' information. This study aims to contribute to a better understanding of the implications of LGPD in companies, providing crucial insights for professionals, managers, and researchers seeking to ensure legal compliance and enhance business management in a regulated environment. Each chapter of the work addresses specific aspects, culminating in final considerations that synthesize the main points explored in the study.

**Keywords:** General Data Protection Law. Personal data. Conformity. Business.

## **LISTA DE ABREVIATURAS E SIGLAS**

AIPD - Avaliação de Impacto sobre Proteção de Dados;

ANPD - Autoridade Nacional de Proteção de Dados;

DID - Defesa em profundidade;

DPO - Data Protection Officer (Encarregado dos Dados);

GDPR - General Protection Data Regulation (Regulamento Geral sobre a Proteção de Dados);

LGPD - Lei Geral de Proteção de Dados.

## SUMÁRIO

<b>1. INTRODUÇÃO.....</b>	<b>12</b>
<b>CAPÍTULO 1: FUNDAMENTOS E IMPACTOS DA LGPD NA GESTÃO EMPRESARIAL... 16</b>	<b>16</b>
1.1. Origem, objetivos e princípios da Lei Geral de Proteção de Dados.....	16
1.2. Direitos dos Titulares de Dados.....	20
1.3. Aplicabilidade Empresarial: identificação dos setores e atividades mais afetados pela LGPD.....	22
1.4. Impactos na Coleta e Tratamento de Dados.....	27
1.5. A importância da implementação de políticas e procedimentos para a proteção de dados nas empresas.....	30
<b>CAPÍTULO 2: DESAFIOS NA ADEQUAÇÃO À LGPD.....</b>	<b>34</b>
2.1. Levantamento e classificação dos dados tratados pela empresa, incluindo a identificação de dados sensíveis.....	34
2.2. Identificação das principais vulnerabilidades que podem comprometer a segurança e privacidade dos dados.....	36
2.3. Políticas de Privacidade na empresa.....	39
2.4. Adoção de medidas técnicas e organizacionais para garantir a proteção dos dados pessoais.....	42
2.5 Avaliação regular de conformidade com a LGPD.....	44
<b>CAPÍTULO 3: IMPLICAÇÕES JURÍDICAS DA LGPD NA GESTÃO EMPRESARIAL.....</b>	<b>48</b>
3.1. Responsabilidade dos Controladores e Operadores de Dados.....	48
3.2. Análise das penalidades previstas na LGPD para empresas em não conformidade.....	49
3.3. Revisão e adequação dos contratos com parceiros, fornecedores e clientes, incluindo cláusulas de proteção de dados.....	51
3.4. Procedimentos para notificar titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD) em caso de vazamentos ou violações de dados.....	54
3.5. Critérios para obtenção de consentimento válido dos titulares de dados para o tratamento de suas informações.....	56
<b>CONSIDERAÇÕES FINAIS.....</b>	<b>59</b>
<b>REFERÊNCIAS.....</b>	<b>62</b>

## 1. INTRODUÇÃO

O objeto do presente Trabalho de Curso é prover alguns apontamentos sobre as implicações legais da Lei Geral de Proteção de Dados na Gestão Empresarial.

O seu objetivo institucional é a produção do Trabalho de Curso como requisito parcial à obtenção do grau de Bacharel em Direito pelo Centro Universitário para o Desenvolvimento do Alto Vale do Itajaí – UNIDAVI.

O objetivo geral deste trabalho de curso é demonstrar a responsabilidade e limitações dos agentes de proteção de dados, e com isso as dificuldades para implementação da LGPD em empresas.

Os objetivos específicos são: a) analisar a forma em que a Lei de Proteção de Dados é aplicada; b) discutir a dificuldade para as empresas/ ou organizações se adequarem em meio a tantas regras novas; c) demonstrar as limitações que ela traz para empresas que lidam com dados pessoais.

Na delimitação do tema levanta-se o seguinte problema: Quais são os principais desafios e impactos na gestão impostos pela LGPD em empresas (agentes)?

Para o equacionamento do problema levanta-se a seguinte hipótese:

Supõe-se que a implementação da Lei Geral de Proteção de Dados em empresas resulta em desafios significativos relacionados à conformidade, segurança de dados, custos operacionais e gestão da reputação, tendo impactos diretos na confiança dos clientes e na prevenção de sanções. Além disso, presume-se que a correta adaptação à LGPD pode criar oportunidades para a inovação e o desenvolvimento de estratégias de negócios centradas na proteção de dados pessoais, beneficiando as empresas.

O Método de abordagem a ser utilizado na elaboração desse trabalho de curso será o indutivo; o Método de procedimento será o monográfico. O levantamento de dados será feito através da técnica da pesquisa bibliográfica.

A escolha do tema envolve a análise da responsabilidade e limitações dos agentes de proteção de dados, bem como as dificuldades na implementação da Lei Geral de Proteção de Dados em empresas, é justificada pela crescente importância da proteção da privacidade e dos dados pessoais em um mundo cada vez mais digital e interconectado. A LGPD representa uma legislação crucial para garantir a segurança e a privacidade das informações pessoais dos titulares.

Dessa forma, o tema escolhido é relevante e atual, contribuindo para o entendimento das implicações da LGPD nas empresas e fornecendo informações valiosas para profissionais, gestores e pesquisadores interessados em garantir a conformidade com a legislação de proteção de dados e aprimorar a gestão empresarial em um ambiente cada vez mais regulamentado. Portanto, a pesquisa abordada neste trabalho tem o propósito de esclarecer os desafios e impactos enfrentados pelas empresas em meio a essa mudança legal significativa.

Principia-se, no Capítulo 1, com diversos tópicos fundamentais relacionados à Lei Geral de Proteção de Dados e como ela afeta as práticas de gestão das empresas. As origens da LGPD, seus objetivos e os princípios fundamentais que a norteiam. Isso inclui a discussão sobre a necessidade de proteger a privacidade e os direitos dos titulares de dados, bem como a regulamentação das atividades de tratamento de dados pessoais no contexto empresarial, os direitos conferidos aos indivíduos cujos dados pessoais são processados pelas empresas, a identificação dos setores e atividades mais impactados pela LGPD, destaca-se também a necessidade de empresas implementarem políticas e procedimentos específicos para garantir a conformidade com a LGPD e os riscos e sanções que as empresas enfrentam caso não estejam em conformidade com a LGPD. Este capítulo serve como uma base sólida para a compreensão dos fundamentos da LGPD e seus impactos na gestão empresarial, preparando o terreno para análises mais aprofundadas nos capítulos subsequentes.

O Capítulo 2 trata de aspectos críticos relacionados à implementação da Lei Geral de Proteção de Dados (LGPD) por parte das empresas. É discutido o desafio de identificar e classificar os dados que a empresa coleta, processa e armazena. Isso inclui a identificação de dados sensíveis, que requerem um tratamento especial de acordo com a LGPD, são exploradas as vulnerabilidades que podem comprometer a segurança e a privacidade dos dados, trata da necessidade de as empresas adotarem políticas de privacidade claras e transparentes para informar os titulares de dados sobre como suas informações são tratadas, são discutidas as medidas técnicas e organizacionais necessárias para garantir a proteção dos dados pessoais e aborda-se a importância da avaliação contínua da conformidade com a LGPD. As empresas precisam monitorar e revisar regularmente seus procedimentos e políticas para garantir que estão em conformidade com a legislação. Este capítulo descreve os desafios específicos que as empresas enfrentam ao tentar se adequar à LGPD e a compreensão desses aspectos é fundamental para que as empresas implementem políticas eficazes de proteção de dados e garantam a conformidade com a legislação.

O Capítulo 3 dedica-se às complexidades legais relacionadas à Lei Geral de Proteção de Dados (LGPD) e como essas implicações afetam a gestão empresarial. São discutidas as responsabilidades dos controladores e operadores de dados sob a LGPD, e isso envolve a definição clara de papéis e responsabilidades, bem como a necessidade de garantir que os dados sejam tratados de acordo com os princípios da legislação, são abordadas as penalidades previstas na LGPD para empresas que não estão em conformidade com a legislação, trata da importância de revisar e adequar os contratos com parceiros de negócios, fornecedores e clientes para incluir cláusulas de proteção de dados, também os procedimentos que as empresas devem seguir em caso de vazamento ou violação de dados e são discutidos os critérios necessários para obter um consentimento válido dos titulares de dados para o tratamento de suas informações pessoais. Este capítulo fornece uma visão aprofundada das implicações jurídicas da LGPD e como elas afetam a gestão empresarial. Compreender essas implicações é essencial para garantir a conformidade com a legislação e minimizar o risco de sanções legais e financeiras. Além disso, auxilia na criação de políticas e procedimentos internos que protegem

os direitos dos titulares de dados e a reputação da empresa.

O presente Trabalho de Curso encerrar-se-á com as Considerações Finais nas quais serão apresentados pontos essenciais destacados dos estudos e das reflexões realizados sobre as implicações da LGPD na gestão da empresa.

## **CAPÍTULO 1: FUNDAMENTOS E IMPACTOS DA LGPD NA GESTÃO EMPRESARIAL**

### **1.1. Origem, objetivos e princípios da Lei Geral de Proteção de Dados.**

A Lei Geral de Proteção de Dados (Lei 13.709, de 2018) foi aprovada no Brasil em 2018 e entrou em vigor em setembro de 2020<sup>1</sup>, e tem como objetivo principal proteger os direitos fundamentais de privacidade e de controle dos indivíduos sobre seus dados pessoais. Esta norma estabelece regras para a coleta dos dados, processamento e compartilhamento de informações pessoais, buscando equilibrar o avanço tecnológico com a proteção da privacidade e segurança das informações, visando garantir que os dados pessoais sejam tratados de maneira transparente, justa e segura, preservando a privacidade das pessoas e evitando o uso indevido de suas informações, além de conceder aos indivíduos o controle sobre seus dados pessoais, permitindo que eles saibam como suas informações estão sendo coletadas, usadas e compartilhadas. Portanto, a lei reconhece organizações que não cumprem suas disposições, incluindo multas que podem variar de acordo com a gravidade das violações.

A origem da Lei Geral de Proteção de Dados está relacionada a uma série de eventos globais e uma preocupação crescente com a privacidade e a segurança dos dados pessoais na era digital atual. Com o avanço da tecnologia e o aumento da coleta dos dados pessoais de cada indivíduo, não apenas aos cidadãos brasileiros, mas toda e qualquer pessoa que esteja no Brasil<sup>2</sup>, e o processamento de dados pessoais, preocupava-se sobre como essas informações estavam sendo usadas e protegidas por cada agente. Com o uso indevido de informações pessoais e falta de transparência por parte de empresas levou a uma demanda por regulamentações mais rigorosas.

---

<sup>1</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 15 de out. de 2023.

<sup>2</sup> LIMA, Cíntia Rosa Pereira de. **Comentários à Lei Geral de Proteção de Dados**. Grupo Almedina (Portugal), 2020. E-book. ISBN 9788584935796. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9788584935796/>>. Acesso em: 02 de out. de 2023. p. 84.

O assunto já foi tratado em legislações como o Código de Defesa do Consumidor e a Lei do Cadastro Positivo (Lei nº 12.414/2011) e o Marco Civil da Internet, referente à proteção de dados. Contudo, a importância de se ter uma legislação específica sobre isso colocou em destaque a problemática da proteção de dados, visto que não existia regulamentação que abordasse essa questão. Vale ressaltar que um dos principais catalisadores para a criação de legislações de proteção de dados em diversos países foi o Regulamento Geral de Proteção de Dados (GDPR, na sigla em inglês), implementado pela União Europeia em maio de 2018. O GDPR estabeleceu padrões elevados para a proteção de dados pessoais e direitos dos indivíduos, influenciando o debate global sobre o tema. O Brasil, como parte do cenário internacional, também restringiu para acomodar suas políticas na proteção de dados. Dessa forma, diversos países adotaram leis parecidas com o GDPR, como foi o caso do Brasil, em que a LGPD é claramente inspirada à imagem e semelhança da disciplina normativa europeia.<sup>3</sup>

A inclusão de cláusulas relacionadas à proteção de dados em acordos comerciais, como o acordo entre o Mercosul e a União Europeia, desempenha um papel significativo ao transferir a necessidade de uma legislação sólida sobre proteção de dados no Brasil. Esse tipo de acordo internacional frequentemente envolve uma troca de informações pessoais e comerciais entre países, o que torna diretrizes cruciais claras para o tratamento desses dados. Portanto, a inclusão de cláusulas sobre proteção de dados em acordos comerciais, como o acordo Mercosul-União Europeia, não apenas impulsiona a necessidade de uma legislação sólida no Brasil, mas também contribui para a integração do país em uma rede global de proteção de dados e padrões éticos no tratamento da informação.

O processo para a criação da LGPD no Brasil começou com um projeto de lei que foi apresentado no Congresso Nacional<sup>4</sup>. Sendo discutido e passado por

---

<sup>3</sup> LIMA, Cíntia Rosa Pereira de. **ANPD e LGPD: Desafios e perspectivas**. Grupo Almedina (Portugal), 2021. E-book. ISBN 9786556272764. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9786556272764/>>. Acesso em: 09 de out. de 2023. p. 223.

<sup>4</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm)>. Acesso em: 15 de out. de 2023.

revisões e ajustes para contemplar as realidades brasileiras, os interesses das empresas e os direitos dos cidadãos. Aprovado pelo Congresso e sancionado pelo então presidente Michel Temer em agosto de 2018. A lei foi inspirada no GDPR<sup>5</sup>, mas também considerada como particularidades do Brasil. Originalmente programada para entrar em vigor em fevereiro de 2020, mas esse prazo foi prorrogado para agosto de 2020 devido a solicitação do setor empresarial para mais tempo de preparação.

Assim, a origem está enraizada na necessidade de proteger a privacidade dos cidadãos em um mundo cada vez mais digitalizado, levando em consideração tendências internacionais, demandas sociais e dinâmica do mercado global. A lei estabeleceu um novo marco legal para a proteção de dados pessoais no Brasil, visando equilibrar os interesses dos cidadãos, das empresas e do governo. Levando em conta também que o Brasil tem a necessidade de implementação da LGPD por conta da limitação de relações internacionais, conforme Lara Garcia cita:

[...] a transferência somente pode acontecer para países ou organismos que possuem leis de proteção de dados similares à brasileira. Inclusive, este foi um dos valores da lei nacional: evitar que o Brasil sofresse qualquer embargo comercial por falta de legislação apropriada, especialmente da Europa, após a promulgação por esta da GDPR. Caberá à ANPD definir a lista de países para os quais pode haver transferência de dados.<sup>6</sup>

A Lei Geral de Proteção de Dados representa um marco fundamental na privacidade e proteção de dados no Brasil. Sustentada por uma série de princípios, estabelece diretrizes claras para o tratamento responsável e ético dos dados pessoais, com o objetivo de garantir os direitos dos indivíduos e espalhar uma cultura de privacidade e segurança tanto na sociedade quanto nas práticas dentro de empresas. Especificamente, por exemplo, estipula-se que o tratamento de dados deve ser realizado com propósitos legítimos, específicos, explícitos e informados aos titulares. Isso significa que as organizações devem deixar claro por que estão

---

<sup>5</sup> **General Data Protection Regulation (GDPR)** – official legal text. Disponível em: <<https://gdpr-info.eu/>>. Acesso em: 20 de ago. de 2023.

<sup>6</sup> GARCIA, Lara R. **Lei Geral de Proteção de Dados (LGPD): Guia de implantação**. Editora Blucher, 2020. E-book. ISBN 9786555060164. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9786555060164/>>. Acesso em: 13 de out. de 2023. p.22.

coletando dados e como pretendem utilizá-los, garantindo transparência e confiança entre as partes envolvidas.

A adequação dos dados obtidos é outro princípio-chave. Os dados coletados devem ser relevantes, fornecidos e não excessivos em relação às finalidades do tratamento. Isso evita a coleta indiscriminada e excessiva de informações, promovendo uma abordagem mais focada e responsável.

Com a necessidade de tratamento também é importante na LGPD, ela restringe o tratamento de dados ao mínimo necessário para atingir os objetivos pretendidos, evitando o uso excessivo e não justificado de informações pessoais.

A lei também coloca o titular dos dados no centro do cenário. O acesso livre dos titulares aos seus próprios dados é um direito fundamental. Eles têm o direito de obter informações claras e precisas sobre como seus dados estão sendo tratados e o poder de exercer o controle sobre eles, inclusive para corrigir informações imprecisas.

A segurança, naturalmente, é uma preocupação crucial, e a LGPD exige que sejam adotadas medidas técnicas e organizacionais para proteger os dados contra acesso não autorizado, perda, destruição, alteração ou divulgação proibida. Isso garante que os dados pessoais sejam mantidos em ambiente seguro e confidencial.

Em conjunto, esses elementos específicos da LGPD tem o propósito de não apenas cumprir as normas internacionais, mas também de estabelecer um ambiente confiável para a coleta e uso de dados pessoais no Brasil. Ao priorizar a privacidade, a transparência e a segurança, a lei se configura como um instrumento indispensável de proteção dos direitos dos cidadãos em relação aos seus dados pessoais, impulsionando uma ideia de respeito à privacidade tanto na sociedade quanto no âmbito empresarial.

## 1.2. Direitos dos Titulares de Dados

A Lei Geral de Proteção de Dados confere diversos direitos aos titulares de dados, garantindo-lhes o controle sobre suas informações pessoais e permitindo que exerçam maior autonomia em relação ao tratamento desses dados por parte de organizações.

Ainda, e conforme citado por Peck:

A proteção das pessoas físicas relativamente ao tratamento dos seus dados pessoais é um direito fundamental, garantido por diversas legislações em muitos países. Na Europa, já estava previsto na Carta dos Direitos Fundamentais da União Europeia e no Tratado sobre o Funcionamento da União Europeia<sup>7</sup>

Um dos principais direitos é o acesso às informações. Os titulares têm o direito de obter informações claras e completas sobre como seus dados pessoais estão sendo processados. Isso inclui detalhes especificamente sobre o tratamento, a origem dos dados e a possibilidade de compartilhamento com terceiros. Além disso, os titulares podem corrigir dados imprecisos, incompletos ou desatualizados. Se eles perceberem que suas informações estão erradas, podem solicitar uma retificação ou complementação.

O direito à exclusão, muitas vezes chamado de "direito ao esquecimento"<sup>8</sup>, permite que os titulares partilhem a exclusão de seus dados, a menos que exista uma obrigação legal que exija o tratamento dessas informações.

Portanto, não se trata apenas de conferir ao titular dos dados pessoas o controle de suas informações, mas, sobretudo, de operacionalizar tais possibilidades na medida em que se assegure ao titular dos dados habilidade concreta de tutela sobre suas informações.<sup>9</sup>

---

<sup>7</sup> PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários à Lei n.º 13.709/2018 (LGPD)**. 2. ed. São Paulo: Saraiva Educação, 2020. p. 19.

<sup>8</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 15 de out. de 2023.

<sup>9</sup> LIMA, Cíntia Rosa Pereira de. **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Grupo Almedina (Portugal), 2020. E-book. ISBN 9788584935796. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9788584935796/>>. Acesso em: 02 de out. de 2023. p. 250.

Os titulares também têm o direito de se referir ao tratamento de seus dados em determinadas situações, como quando os dados são usados para marketing direto ou quando o tratamento se baseia em interesses legítimos da organização. E ainda, conforme citado por Lara Garcia:

[...] mesmo que o Titular tenha manifestamente tornado públicos seus dados, o Controlador e o Operador não estão isentos de suas responsabilidades, especialmente no que diz respeito ao livre acesso do Titular às informações baseadas em seus dados, forma e duração do tratamento realizado com eles, e a possíveis compartilhamentos que Controlador e Operador possam ter feito.<sup>10</sup>

Outro direito importante é a portabilidade de dados. Isso significa que os titulares podem solicitar o download de seus dados em um formato que seja facilmente transferível para outro serviço ou empresa, desde que isso não afete os direitos de terceiros. Além disso, os titulares podem revogar sua autorização a qualquer momento. Se o tratamento de seus dados for baseado na autorização deles, eles têm o direito de retirá-los sem consequências negativas. É crucial mencionar que a LGPD também trata do tratamento de dados de crianças e adolescentes, exigindo o consentimento específico e destacado de seus pais ou responsáveis legais.

Para exercer esses direitos, os titulares podem entrar em contato com a organização que trata seus dados, normalmente conhecida como controladora de dados. Geralmente, as empresas disponibilizam canais de comunicação, como e-mails ou formulários, para que os titulares possam exercer seus direitos. Portanto a LGPD busca capacitar os indivíduos, permitindo-lhes tomar decisões informadas sobre suas informações pessoais e promovendo uma cultura de respeito à privacidade e segurança dos dados.

---

<sup>10</sup> GARCIA, Lara R. **Lei Geral de Proteção de Dados (LGPD):** Guia de implantação. Editora Blucher, 2020. E-book. ISBN 9786555060164. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9786555060164/>>. Acesso em: 13 de out. de 2023. p. 20.

### 1.3. Aplicabilidade Empresarial: identificação dos setores e atividades mais afetados pela LGPD.

A Lei Geral de Proteção de Dados representa uma mudança significativa na forma como as organizações coletam, utilizam e protegem os dados pessoais. A aplicabilidade da LGPD é vasta, alcançando setores e atividades empresariais, dada a presença do tratamento de dados pessoais na era digital, até mesmo setores mais tradicionais da economia brasileira, como a agropecuária e a indústria extrativa, estão se digitalizando com uma velocidade grande para não ficar fora dos parâmetros da legislação.<sup>11</sup> A privacidade é uma preocupação fundamental na era da informação, onde a coleta e o uso de dados pessoais estão cada vez mais divulgados. Embora praticamente todas as organizações estejam sujeitas a alguma forma, alguns setores e atividades se destacam devido à natureza sensível das informações que manipulam ou ao volume significativo de dados que coletam e processam.

As empresas de tecnologia desempenham um papel central na coleta e no processamento de dados pessoais, muitas vezes impulsionadas por seus serviços inovadores e soluções tecnológicas avançadas. Desde gigantes da indústria até startups emergentes, essas empresas desenvolvem produtos que dependem da coleta de dados para melhorar a experiência do usuário, personalizar serviços e oferecer insights valiosos. Dessa forma Lima cita que:

Talvez o ponto-chave no processo de adequação de empresas de tecnologia da informação seja exatamente o mapeamento de dados ou data mapping. Esse processo, comum a qualquer outro ramo de atividade, consiste em identificar sempre que, na execução do negócio, dados pessoais são coletados e tratados.<sup>12</sup>

---

<sup>11</sup> LIMA, Ana Paula Moraes Canto de. **LGPD Aplicada**. Grupo GEN, 2021. E-book. ISBN 9788597026931. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9788597026931/>>. Acesso em: 11 de out. de 2023. p. 03.

<sup>12</sup> LIMA, Ana Paula Moraes Canto de. **LGPD Aplicada**. Grupo GEN, 2021. E-book. ISBN 9788597026931. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9788597026931/>>. Acesso em: 11 de out. de 2023. p. 04.

No entanto, a LGPD introduz a necessidade de obter consentimento claro e informado dos usuários antes de coletar seus dados e estabelece limites sobre como esses dados podem ser usados, promovendo assim uma maior transparência nas práticas de coleta e tratamento de dados.

A aplicação da LGPD no contexto da Saúde é especialmente crucial devido à natureza altamente sensível dos dados que são coletados, processados e armazenados por hospitais, clínicas, laboratórios e planos de saúde. Essas entidades coletaram informações pessoais planejadas para prestar serviços médicos de qualidade, permitindo o acompanhamento do histórico de saúde de cada paciente e auxiliar no diagnóstico e tratamento. Esses dados não se limitam apenas a informações básicas, mas também incluem históricos médicos completos, resultados de exames, imagens de diagnóstico e detalhes sobre tratamentos específicos. E essa área pode ser considerada a mais ampla em questão de arquivamento de informações pessoais e sensíveis. Dessa forma:

As organizações de saúde precisam, portanto, investir tempo, capital financeiro e recurso humano para mudar sua perspectiva e abordagem, já que para estar em conformidade com a nova regulamentação de proteção de dados pessoais é essencial aplicar melhores práticas de cibersegurança.<sup>13</sup>

Ainda, os centros de saúde precisam lidar com históricos longos de pacientes para uma melhor precisão no diagnóstico. Trazendo à tona o descarte das informações solicitadas pela LGPD, no artigo 5º, inciso X.<sup>14</sup>

As instituições bancárias desempenham um papel vital na economia, atuando como investidores financeiros e facilitando transações financeiras. Essas instituições não lidam apenas com informações financeiras dos clientes, como também possuem uma grande quantidade de dados pessoais sensíveis, incluindo números de

---

<sup>13</sup> SERPRO-SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS. **LGPD e saúde: os fins justificam os meios?** — LGPD - Lei Geral de Proteção de Dados Pessoais. Disponível em: <<https://www.serpro.gov.br/lgpd/noticias/2019/paciente-no-comando-lgpd-dados-sensiveis-saude>>. Acesso em: 31 out. 2023.

<sup>14</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018.** Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 15 de out. de 2023.

documentos de identidade, endereços, histórico de transações e até mesmo informações biométricas em alguns casos. A necessidade de proteger esses dados não pode ser subestimada, uma vez que qualquer violação de segurança pode levar a sérias consequências, incluindo roubo de identidade, fraude financeira e danos à confiança das instituições envolvidas.

O Comércio Eletrônico, representado pelas lojas online, plataformas de compras e aplicativos de entrega, revolucionou a forma como as pessoas adquirem produtos e serviços. Para oferecer uma experiência personalizada e conveniente, as empresas desse setor coletam informações como histórico de compras, opções de produtos, localização e até mesmo comportamento de navegação. Outro ponto importante são os critérios do algoritmo de score, a capacidade de demonstrar a transparência dos parâmetros e que atenda ao princípio de não discriminação previsto pelo art. 6.º, IX, trazendo ao cliente argumentos válidos e utilizados para análise da venda.<sup>15</sup>

Esses dados são usados para recomendar produtos relevantes, ajustar preços dinamicamente e criar estratégias de marketing direcionadas. No entanto, com a implementação da LGPD, as empresas precisam agora obter consentimento explícito dos clientes para coletar e processar esses dados, além de garantir medidas de segurança robustas para assim evitar qualquer futuro problema.

As agências de marketing e as empresas de publicidade vêm coletando dados de consumidores há anos, entendendo seus comportamentos, preferências e necessidades. Esses dados permitem a criação de perfis detalhados, que por sua vez são usados para segmentar audiências específicas e personalizar campanhas de maneira direcionada. No entanto, a era da LGPD trouxe à tona a necessidade de transparência e consentimento na coleta e uso desses dados. Agora, os consumidores têm o direito de saber quais informações estão sendo coletadas e para quais fins elas serão usadas, além de poderem escolher se desejam ou não compartilhar esses dados.

---

<sup>15</sup> LIMA, Ana Paula Moraes Canto de. **LGPD Aplicada**. Grupo GEN, 2021. E-book. ISBN 9788597026931. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9788597026931/>>. Acesso em: 11 de out. de 2023. p. 112.

A inclusão do Setor Público na esfera de influência da LGPD é um reflexo da crescente digitalização das operações governamentais e da necessidade de equilibrar o fornecimento eficiente de serviços com a proteção dos direitos de privacidade dos cidadãos. Nesse sentido Lima cita:

Tanto o setor público quanto à iniciativa privada no Brasil antecipam muita dificuldade de percorrer caminhos como esses que aqui são apontados, passos essenciais para a conformidade com relação à LGPD que envolvem a adoção de processos organizacionais que são relativamente complexos.<sup>16</sup>

O governo coleta e processa uma grande quantidade de dados pessoais em diversas áreas, incluindo saúde, educação, serviços sociais, segurança e administração pública. Esses dados variam desde informações básicas de identificação até detalhes mais sensíveis, como históricos médicos, registros criminais e informações financeiras. No Setor Público na abrangência da LGPD tem várias implicações importantes. Em primeiro lugar, ela visa garantir que os cidadãos tenham confiança de que suas informações pessoais estão sendo tratadas com respeito e protegidas contra abuso ou vazamento. Isso é essencial para manter a legitimidade e a transparência do governo aos olhos da população.

No setor de Transporte e Logística, a coleta de dados se tornou fundamental para otimizar as operações, rastrear mercadorias e garantir que as entregas realizadas sejam realizadas de maneira eficiente. Empresas que atuam nesse campo coletam informações de rastreamento, como localização e status das encomendas, a fim de fornecer atualizações precisas aos clientes sobre o andamento de suas entregas. No entanto, com a LGPD, surge a necessidade de que essas empresas obtenham o consentimento dos clientes para coleta e uso desses dados, além de garantir que medidas de segurança estejam em vigor para proteger essas informações contra acessos não autorizados.

---

<sup>16</sup> LIMA, Ana Paula Moraes Canto de. **LGPD Aplicada**. Grupo GEN, 2021. E-book. ISBN 9788597026931. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9788597026931/>>. Acesso em: 11 de out. de 2023. p. 128.

Independentemente do setor, a LGPD exige que as organizações compreendam suas responsabilidades legais, implementem políticas de conformidade e apliquem medidas de segurança adequadas. Ao proteger os direitos dos titulares de dados e garantir a privacidade, a LGPD não reflete apenas uma evolução nas práticas de tratamento de dados, mas também fortalece a confiança entre as organizações e um público.

A implementação da Lei Geral de Proteção de Dados pode apresentar várias dificuldades para as empresas. Em primeiro lugar, a mudança de cultura organizacional e a conscientização dos colaboradores sobre a importância da proteção de dados podem ser desafiadoras. Isso requer treinamento e educação para garantir que todos compreendam os princípios e saibam como aplicá-los em suas atividades diárias. Outro obstáculo é a revisão e adaptação dos processos internos. As empresas precisam identificar quais dados pessoais são coletados, como são usados e com quem são compartilhados. Isso pode envolver revisar contratos com fornecedores e parceiros para garantir que todos estejam em conformidade com a lei. Além disso, exige medidas técnicas e organizacionais para garantir a segurança dos dados. Isso pode envolver investimentos em sistemas de segurança, criptografia e outras tecnologias que protejam os dados contra acesso não autorizado.

Conforme citado inicialmente a LGPD é uma legislação muito ampla, deixando brechas e espaços para a aplicações específicas em organizações, trazendo uma grande dificuldade para a implementação, e por essa razão é muito comum no princípio dos trabalhos o time operacional se sentir perdido e não saber por onde começar. Especialmente quando se fala de um ambiente consideravelmente grande, o volume de análises e avaliações é tamanho que dificulta até identificar quais controles atendem quais processos.<sup>17</sup>

Em resumo, a implementação da LGPD envolve mudanças culturais, revisões de processos, investimentos em segurança, concessão de autorização válida e

---

<sup>17</sup> LIMA, Ana Paula Moraes Canto de. **LGPD Aplicada**. Grupo GEN, 2021. E-book. ISBN 9788597026931. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9788597026931/>>. Acesso em: 11 de out. de 2023. p. 14.

ajustes legais. Embora seja um desafio, é fundamental para garantir a proteção dos dados pessoais e a conformidade com os critérios legais.

#### 1.4. Impactos na Coleta e Tratamento de Dados

A evolução digital e o crescente papel dos dados na tomada de decisões e no desenvolvimento de produtos e serviços transformaram profundamente a maneira como as empresas coletam, armazenam, tratam e utilizam informações. Com a implementação da Lei Geral de Proteção de Dados, esses processos sofreram um impacto significativo.

A LGPD redefiniu fundamentalmente a forma como as organizações podem coletar e utilizar dados pessoais. Antes, o processo muitas vezes ocorria sem a clara ciência dos titulares dos dados, o que gerava preocupações em relação à privacidade e ao controle sobre suas informações pessoais. Agora, a concessão do consentimento explícito e informado tornou-se uma âncora central nas operações que envolvem dados pessoais. As empresas são obrigadas a comunicar, de maneira clara e acessível, como os dados serão utilizados, garantindo que os titulares tenham um entendimento completo dos propósitos do tratamento. Conforme cita Bittar e Tomaschewski:

A LGPD se tornou uma lei necessária no cenário atual, tendo em vista a crescente preocupação no que diz respeito ao uso das informações pessoais das pessoas, bem como a sua comercialização e uso indevido.<sup>18</sup>

Essa mudança trouxe à tona uma nova era de transparência, responsabilidade e compromisso com a privacidade. A coleta de dados não é mais obscura ou sigilosa, mas sim um processo que promove uma interação honesta entre as organizações e seus clientes ou usuários. Particularmente relevante é a mudança no tratamento de dados sensíveis, como informações de saúde, orientação

---

<sup>18</sup> BITTAR, C. A. C.; TOMASCHEWSKI, T. A Lei Geral de Proteção de Dados Pessoais e sua aplicação prática nas empresas. In: **CONGRESSO INTERNACIONAL DE ADMINISTRAÇÃO**, XXVI., 2021, Rio de Janeiro-RJ.

sexual e origem racial. A LGPD distribui requisitos mais específicos para o processamento desses dados, garantindo que sejam utilizados apenas dados específicos e legítimos, com um cuidado especial em conformidade com a natureza sensível dessas informações.

Nesse novo cenário, as empresas se veem obrigadas a considerar a ética e a privacidade em todas as etapas do uso de tecnologias de análise de dados. Isso se torna especialmente relevante na coleta e análise de dados para a criação de perfis de consumidores.

A LGPD também fez nascer a grande necessidade de uma infraestrutura de segurança de dados maior. As empresas não podem mais subestimar a importância de proteger os dados contra acesso não autorizado, perda ou vazamento. A lei exige a adoção de medidas técnicas e organizacionais que mantêm a integridade dos dados, o que se refere a investimentos em tecnologias de segurança avançadas. E neste mesmo sentido, de acordo com Almeida e Santos, a aplicação da LGPD exige que as organizações estabeleçam ações para salvaguardar os dados pessoais e assegurar a privacidade e a integridade dos usuários. Isso implica a necessidade de implementar estratégias técnicas e administrativas, como a utilização de criptografia, a realização de cópias de segurança e o controle de acessos, além de adotar políticas e procedimentos transparentes e moralmente aceitáveis no tocante ao tratamento de informações pessoais.<sup>19</sup>

Um destaque notável trazido pela LGPD é o processo de anonimização de dados no artigo 5º, III da lei nº 13.709<sup>20</sup>. A lei promove o uso dessa técnica como forma de proteção à identificação dos titulares dos dados, permitindo que as empresas utilizem informações de maneira anônima. Isso demonstra uma abordagem equilibrada que visa a proteção da privacidade, ao mesmo tempo que permite o aproveitamento dos dados oferecidos. No geral, a anonimização traz à tona duas abordagens diferentes para as empresas: a primeira tem por base a

---

<sup>19</sup> ALMEIDA, N. N.; SANTOS, S. L. F. Gestão de dados pessoais em conformidade com a LGPD. In: **ENCONTRO DE ADMINISTRAÇÃO**, 8., 2020, Joinville-SC. INESUL, 2020. p. 7.

<sup>20</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 15 de out. de 2023.

aleatorização, enquanto a segunda baseia-se na generalização.<sup>21</sup> A abordagem de aleatorização envolve uma introdução de ruído ou alterações evocadas nos dados pessoais, de modo que seja difícil ou impossível associar esses dados a uma pessoa específica. E uma abordagem de generalização envolve a substituição de dados pessoais por categorias mais amplas ou informações menos específicas. Isso preserva a utilidade dos dados, mas torna mais difícil identificar indivíduos.

Além dos impactos internos, a implementação da LGPD também forçou uma mudança nas relações comerciais entre as empresas e seus parceiros de negócios. Os contratos e acordos agora deverão incluir cláusulas explícitas de proteção de dados, garantindo que todas as partes envolvidas estejam em conformidade com as disposições da lei. Essa mudança é crucial para garantir que todos respeitem os padrões rigorosos de tratamento de dados pessoais, criando um sistema mais seguro e confiável para todos os envolvidos.

Enquanto a LGPD impõe restrições e regulamentações mais rigorosas, também abre portas para oportunidades específicas. Empresas que adotam práticas de coleta e tratamento de dados que respeitam a privacidade e a segurança, não apenas cumprem as exigências legais, mas também conquistam a confiança dos clientes e usuários. Isso leva a relacionamentos mais sólidos e duradouros, pois os consumidores se sentem mais confortáveis em compartilhar suas informações pessoais com empresas que demonstram um compromisso genuíno com a proteção desses dados.

Em resumo, a LGPD trouxe uma mudança grande na maneira como as empresas abordam a coleta e o tratamento de dados. Desde a importância do consentimento até a necessidade de práticas éticas na análise de dados, passando por medidas de segurança e proteção rigorosas, a lei exige uma abordagem consciente, responsável em relação às informações pessoais.

---

<sup>21</sup> LIMA, Cíntia Rosa Pereira de. **Comentários à Lei Geral de Proteção de Dados**. Grupo Almedina (Portugal), 2020. E-book. ISBN 9788584935796. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9788584935796/>>. Acesso em: 02 de out. de 2023. p. 107.

## **1.5. A importância da implementação de políticas e procedimentos para a proteção de dados nas empresas.**

No cenário atual, onde a coleta, o processamento e o compartilhamento de dados são elementos cruciais para o funcionamento de empresas em diversos setores, a implementação de políticas e procedimentos para a proteção de dados tornou-se uma prioridade incontestável. A crescente conscientização sobre a privacidade e a segurança dos dados, bem como a implementação da Lei Geral de Proteção de Dados no Brasil e regulamentações semelhantes em outros países, destaca a relevância de disposições sólidas para a gestão responsável de informações pessoais. A implementação eficaz de políticas e procedimentos para a proteção de dados oferece uma série de vantagens inegáveis para as empresas. Em primeiro lugar, a adoção dessas políticas é essencial para cumprir as exigências legais. A LGPD e outras regulamentações obrigam as empresas a proteger os dados pessoais dos indivíduos, estabelecendo deliberações significativas em caso de não conformidade, conforme artigo 34º, § 3º da lei nº 13.709.<sup>22</sup> E dessa forma implementar políticas e procedimentos adequados ajuda a mitigar riscos legais e evitar multas onerosas.

Além disso, a proteção de dados é um aspecto vital para a construção de confiança entre as empresas e seus clientes e parceiros. Quando as pessoas veem que suas informações pessoais são tratadas com responsabilidade e segurança, estão mais inclinadas a se envolver com a empresa e compartilhar seus dados. A implementação de medidas de segurança maiores, como criptografia, autenticação de dois fatores, ajuda a prevenir a proteção de dados e ciberataques.

As políticas de proteção de dados permitem uma avaliação mais eficiente dos riscos relacionados ao tratamento de informações pessoais. Isso permite que a empresa identifique áreas de vulnerabilidade e tome medidas proativas para mitigar esses riscos, garantindo a continuidade dos negócios. A implementação de políticas

---

<sup>22</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 15 de out. de 2023.

sólidas demonstra o comprometimento da empresa com a privacidade dos dados, contribuindo para uma imagem positiva.

Políticas básicas e procedimentos claros e transparentes mostram que uma empresa está comprometida em agir de forma ética e responsável em relação aos dados pessoais. Isso não apenas atende às expectativas dos clientes, mas também demonstra responsabilidade corporativa. Ter políticas bem definidas para coleta, armazenamento e processamento de dados podem melhorar os processos internos. Isso pode levar a um gerenciamento mais eficaz de informações, resultando em decisões mais informadas e eficientes. Evitando situações de emergência que possam surgir devido à transparência de dados. A prevenção de tais incidentes pode resultar na redução de custos associados a investigações, ações judiciais e recuperação pós-violação, conforme citado na Lei nº 13.709:

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

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; [...]<sup>23</sup>

Em resumo, a implementação de políticas e procedimentos para a proteção de dados é uma iniciativa estratégica essencial para empresas em todos os setores. Além de garantir a conformidade legal, esta abordagem promove a construção de confiança, a prevenção de detecção de dados, a gestão de riscos e a melhoria da eficiência operacional. Com a privacidade e a segurança dos dados sendo um foco crescente tanto para consumidores quanto para reguladores, as empresas que priorizam a proteção de dados estão melhor posicionadas para prosperar em um ambiente digital cada vez mais complexo.

Nesse contexto abrangente e crucial, ganhar a confiança do público para o compartilhamento de dados emerge como uma tarefa de extrema importância. Para atingir esse objetivo, é importante estabelecer níveis de segurança que estejam em

---

<sup>23</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 03 de nov. de 2023.

sintonia com as demandas da empresa, em relação tanto ao volume de dados pessoais quanto aos dados sensíveis que manejam. Nesse cenário, vale a pena destacar a metodologia estratégica conhecida como “Defesa em Profundidade” (DID).

Importante ressaltar a citação de Lima:

Esse conceito é antigo e já era aplicado desde a Idade Média (ou talvez até antes). Num castelo, como o representado a seguir, talvez a “Torre de Homenagem” fosse seu ponto mais sensível e, para tanto, precisaria ter o máximo de segurança.<sup>24</sup>

E essa abordagem se fundamenta na proteção abrangente dos dados, valendo-se da identificação criteriosa das necessidades de segurança e da implementação de medidas em múltiplas camadas.

Esse processo é iniciado com a identificação minuciosa dos ativos que mantêm segurança, ao mesmo tempo em que são determinados os níveis de segurança obrigatórios para parar ou evitar qualquer tentativa de ataque. A etapa subsequente consiste na aplicação de medidas de segurança customizadas para se alinharem com os objetivos específicos da organização. O objetivo primordial é construir uma rede defensiva em multicamadas que amplifique a capacidade do sistema de lidar com as ameaças existentes em potencial.

À luz dessa explicação, torna-se evidente a urgência de estabelecer várias barreiras de proteção, capazes de lidar com vastas formas de ataque. Esse princípio, embora inicialmente concebido para ambientes físicos e estratégicos, é igualmente aplicável ao âmbito dos sistemas digitais. Em conformidade com essa linha de pensamentos, podem ser inovadoras uma série de práticas e protocolos, tais como políticas de procedimentos e conscientização, salvaguardas físicas dentro das organizações, fortificações no perímetro, medidas de segurança na rede interna, proteções em nível alto, resguardos na camada de aplicação e, por sequência, na segurança dos próprios dados.

---

<sup>24</sup> LIMA, Ana Paula Moraes Canto de. **LGPD Aplicada**. Grupo GEN, 2021. E-book. ISBN 9788597026931. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9788597026931/>>. Acesso em: 13 de out. de 2023.

Através dessa abordagem abrangente e exemplificada em camadas, as organizações podem estabelecer um ambiente de confiança, que não apenas protege os dados sensíveis, mas também fortalece a capacidade geral do sistema de resistência a ataques. Conforme citado por Ana Paula Moraes Canto de Lima:

Uma vez que todas essas camadas estão totalmente operacionais, é preciso garantir que as pessoas que vão realizar essa operação estejam capacitadas para mantê-las em funcionamento e conforme os parâmetros previamente estabelecidos. Aqui é que criamos as políticas, os códigos de conduta e os procedimentos.<sup>25</sup>

Nessa mesma linha de raciocínio, pode-se dizer que, apesar de todos os avanços tecnológicos e das sofisticadas estratégias de proteção de dados que uma empresa possa implementar, de nada adianta se não houver uma conduta correta e comprometida por parte de seus funcionários. Afinal, são eles que estão no frente, utilizando diariamente os sistemas e interagindo com os dados.

Portanto, a conscientização e a capacitação dos colaboradores são de suma importância. Compreender as políticas de segurança, adotar práticas seguras no uso diário dos recursos digitais e seguir os procedimentos estabelecidos são ações que podem determinar a mudança da rede de defesa de uma empresa. Capacitar os funcionários para lidar com os dados é um componente crítico para a segurança da empresa.

Em resumo, a conexão entre as camadas de defesa de dados, as políticas organizacionais, os códigos de conduta e a capacitação dos funcionários é o que confere força e reforço a qualquer estratégia de segurança. O sucesso não é apenas medido pelo quão robustas são as barreiras de proteção, mas também pela consciência coletiva da importância de preservação da integridade dos dados.

---

<sup>25</sup> LIMA, Ana Paula Moraes Canto de. **LGPD Aplicada**. Grupo GEN, 2021. E-book. ISBN 9788597026931. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9788597026931/>>. Acesso em: 29 de ago. de 2023. p. 11.

## CAPÍTULO 2: DESAFIOS NA ADEQUAÇÃO À LGPD

### 2.1. Levantamento e classificação dos dados tratados pela empresa, incluindo a identificação de dados sensíveis

O levantamento e classificação dos dados tratados por uma empresa desempenham um papel fundamental na gestão eficaz da informação e na conformidade com as regulamentações de proteção de dados. Esse processo envolve a identificação, organização e categorização dos dados de acordo com sua natureza e importância. Uma etapa crítica desse processo é a identificação de dados sensíveis. Esses dados são informações que, se expostas, podem causar danos significativos à empresa ou às partes envolvidas. O artigo 5º, II dispõe que os dados pessoais sensíveis correspondem aos:

[...] 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.<sup>26</sup>

E a classificação dos dados permite que a empresa estabeleça políticas e medidas de segurança apropriadas para proteger essas informações sendo elas sensíveis ou não. Isso inclui a implementação de controles de acesso restrito, criptografia de dados, monitoramento de atividades suspeitas e a elaboração de planos de resposta a incidentes de segurança. Em conformidade com as leis, a identificação precisa de dados sensíveis é de suma importância. Isso se deve ao fato de que tanto o GDPR quanto a LGPD impõem requisitos rigorosos para o tratamento responsável e seguro desses tipos de informações.

---

<sup>26</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 15 de out. de 2023.

Tais regulamentações requerem que as empresas adotem medidas específicas para proteger informações sensíveis, incluindo a implementação de técnicas e organizacionais robustas, a nomeação de um Encarregado de Proteção de Dados (DPO), onde desloca-se a exclusividade de responsabilidade de uma pessoa específica, como o oficial de proteção de dados ou qualquer outra pessoa, para o cumprimento da LGPD, com o intuito de manter em conformidade, tornando-se um objetivo coletivo de toda a organização, compartilhando em todos os seus níveis.<sup>27</sup> Portanto, a identificação correta dos dados não é apenas uma formalidade, mas uma ação estratégica para garantir que a empresa esteja em total conformidade com as exigências legais, mitigando, assim, o risco de sanções significativas.

Dessa forma, um passo importante é identificar e coletar todos os dados que a empresa trata. Isso envolve não apenas os dados estruturados (como informações em bancos de dados), mas também os dados não estruturados (como documentos, e-mails e registros em sistemas diversos). Esse processo de levantamento deve ser abrangente e incluir todas as áreas e departamentos da empresa. Após o levantamento, é crucial classificar os dados, atribuindo a cada conjunto de dados um nível de importância e sensibilidade. Os dados podem ser classificados em categorias, como:

- **Dados Pessoais:** Informações que identificam ou podem identificar uma pessoa, como nome, endereço, CPF, número de telefone, etc.
- **Dados Sensíveis:** Informações mais delicadas que podem causar danos significativos se forem mal utilizadas, como informações médicas, religiosas, étnicas, dados biométricos, etc.
- **Dados Empresariais:** Informações sobre a empresa, seus clientes, fornecedores, e operações internas.
- **Dados Públicos:** Informações que estão disponíveis publicamente, como dados em sites ou informações que não são sensíveis.

---

<sup>27</sup> GARCIA, Lara R. **Lei Geral de Proteção de Dados (LGPD):** Guia de implantação. Editora Blucher, 2020. E-book. ISBN 9786555060164. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9786555060164/>>. Acesso em: 13 de out. de 2023.

Portanto, a classificação apropriada de dados, especialmente dos sensíveis, não é apenas uma obrigação legal, mas uma estratégia empresarial sensata que fortalece a posição da empresa cada vez mais focada na privacidade, permitindo-lhe não só cumprir regulamentações, mas também estabelecer uma reputação de integridade aos dados, o que, por sua vez, traz a confiança dos clientes, conforme citado no artigo 50, § 2º, e), que tenha o propósito de criar um vínculo de confiança com o indivíduo em questão, através de uma atuação que seja clara e que garanta a inclusão de mecanismos que permitam a participação do titular.<sup>28</sup>

Em resumo, o processo de coleta e classificação de dados está relacionado à conformidade regulatória e à redução de riscos para as empresas que manejam dados pessoais. Portanto, a implementação eficaz desse processo não é apenas uma escolha estratégica, mas uma necessidade urgente em um cenário empresarial onde a gestão responsável de dados é um elemento importante para se manter dentro da legislação, e evitar sanções por vazamento de dados pessoais e sensíveis.

## **2.2. Identificação das principais vulnerabilidades que podem comprometer a segurança e privacidade dos dados**

A Lei Geral de Proteção de Dados (LGPD) representa um marco fundamental na regulamentação da privacidade e segurança de dados no Brasil. Nesse contexto, a identificação das principais vulnerabilidades que podem comprometer a segurança e privacidade dos dados assume uma importância ainda maior, uma vez que a legislação impõe rigorosos requisitos de proteção de dados pessoais.

E neste mesmo sentido Marinho propõe que:

[...] o risco jurídico das empresas vai aumentar exponencialmente, na medida em que já existem grupos, associações, empresas e pessoas se preparando para ingressar com ações coletivas contra empresas

---

<sup>28</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 15 de out. de 2023.

que coletam grande quantidade de dados pessoais, com a finalidade de angariar indenizações.<sup>29</sup>

Ainda que cumprindo com os requisitos, um dos principais desafios sob a LGPD é a identificação de vulnerabilidades na infraestrutura de rede e armazenamento. A lei exige que as organizações adotem medidas para proteger os dados pessoais de acessos não autorizados, e vulnerabilidades na rede podem ser exploradas por invasores cibernéticos ou até mesmo de indivíduos da própria empresa. Garantir a segurança da rede é crucial para proteger os dados.

Falhas de segurança em software, sistemas operacionais e hardware são igualmente críticas sob a LGPD. A lei exige que as organizações implementem medidas para proteger os dados pessoais contra perda, uso não autorizado e vazamento, conforme artigo 46 da Lei nº 13.709.<sup>30</sup> Falhas de software podem ser exploradas para obter acesso não autorizado aos sistemas que armazenam dados pessoais, comprometendo a privacidade.

Erros humanos são uma fonte significativa de vulnerabilidades sob a LGPD. A lei impõe a necessidade de conscientização e treinamento em segurança de dados. Funcionários mal-informados ou desatentos podem expor informações pessoais, resultando em violações de privacidade. Trazendo a conscientização dos funcionários para evitar falhas humanas que futuramente possam comprometer a segurança dos dados armazenados na empresa.<sup>31</sup> As ameaças internas, como funcionários insatisfeitos ou mal-intencionados, também são uma preocupação sob a LGPD. A lei exige o controle de acesso a dados pessoais, mas colaboradores com acesso privilegiado podem abusar dessas permissões, por isso identificar essas ameaças internas é de suma importância para a conformidade com a lei.

---

<sup>29</sup> MARINHO, Fernando. Os 10 Mandamentos da LGPD - **Como Implementar a Lei Geral de Proteção de Dados em 14 Passos**. Grupo GEN, 2020. E-book. ISBN 9788597026009. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9788597026009/>>. Acesso em: 13 de out. de 2023.

<sup>30</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 15 de out. de 2023.

<sup>31</sup> FERREIRA, D. C. (2020). Lei Geral de **Proteção de dados pessoais**: a implementação e seus desafios para a administração pública e privada no Brasil. Revista de Direito, 18(32). p. 108.

O armazenamento inadequado de dados é uma vulnerabilidade que a LGPD aborda especificamente, conforme artigo 46 da Lei nº 13.709, os agentes devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados.<sup>32</sup> A lei requer que os dados pessoais sejam armazenados de forma segura, incluindo medidas como criptografia e controles de acesso. O armazenamento inadequado pode resultar em vazamentos de dados que violem a privacidade dos indivíduos.

A não conformidade com a LGPD é, por si só, uma vulnerabilidade de grande magnitude. A lei estabelece penalidades substanciais para as organizações que não atenderem aos seus requisitos, e a falta de conformidade pode acarretar prejuízos financeiros e danos à reputação, além de potenciais violações à privacidade dos titulares de dados. Neste mesmo sentido Garrido reforça:

[...] um programa de gestão de dados pessoais bem implementado pode ajudar na redução das penas, na hipótese de ocorrência de um tipo de infração que enseje a aplicação de alguma penalidade.<sup>33</sup>

Além disso, a LGPD aborda a importância da cooperação com terceiros e parceiros de negócios. A legislação impõe às organizações a responsabilidade de assegurar que essas entidades sigam os mesmos padrões rigorosos de segurança e privacidade ao lidar com dados pessoais<sup>34</sup>. Parceiros de negócios que não garantem adequadamente a segurança dos dados podem representar um sério risco à privacidade das informações.

Dessa forma, a evolução das ameaças cibernéticas é uma constante sob a LGPD, se medidas de segurança cibernética não forem inovadoras, seus dados pessoais permanecerão desprotegidos e suscetíveis a possíveis particularidades,

---

<sup>32</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 15 de out. de 2023.

<sup>33</sup> GARRIDO, Patricia P. **Proteção de dados pessoais: comentários à lei n. 13.709/2018 (LGPD)**. Editora Saraiva, 2023. E-book. ISBN 9786555599480. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9786555599480/>>. Acesso em: 20 de out. de 2023.

<sup>34</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 15 de out. de 2023.

resultando em uma ilusão de estar em conformidade com as normas de segurança.<sup>35</sup> A lei exige que as organizações estejam constantemente preparadas para identificar e mitigar novas ameaças à segurança dos dados pessoais, tornando a atualização contínua das defesas de segurança uma necessidade premente. Isso significa que a segurança de dados não é uma tarefa pontual, mas um processo contínuo de adaptação e aprimoramento para garantir o cumprimento da LGPD e a proteção dos dados pessoais de forma eficaz.

Portanto, é importante ressaltar que a conformidade com a LGPD transcende o mero cumprimento de uma obrigação legal. Ela se manifesta como uma demonstração tangível de responsabilidade e respeito pela privacidade das pessoas, posicionando as organizações em um patamar mais elevado de governança e ética empresarial. Além disso, a conformidade com a LGPD reflete um compromisso com a transparência, a integridade e a confiança, fatores cruciais para manter a lealdade dos clientes e parceiros comerciais em um mundo cada vez mais consciente da importância da proteção de dados. A implementação de robustas políticas de segurança e a promoção da conscientização sobre a privacidade são pilares estratégicos para empresas que buscam não apenas cumprir a lei, mas também estabelecer um padrão elevado de excelência na proteção dos dados pessoais.

### **2.3. Políticas de Privacidade na empresa**

As políticas de privacidade desempenham um papel crucial no contexto da Lei Geral de Proteção de Dados no Brasil. A LGPD é uma legislação que estabelece regras rigorosas para a coleta, uso e tratamento de dados pessoais, com o objetivo de proteger a privacidade dos indivíduos. Nesse cenário, as políticas de privacidade são essenciais para que as empresas estejam em conformidade com a legislação e protejam os direitos dos titulares de dados.

Essas políticas têm diversas funções essenciais para adequação de uma empresa quanto a LGPD. Primeiro, elas garantem a transparência no tratamento de

---

<sup>35</sup> LIMA, Ana Paula Moraes Canto de. **LGPD Aplicada**. Grupo GEN, 2021. E-book. ISBN 9788597026931. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9788597026931/>>. Acesso em: 20 de out. de 2023.

dados pessoais, e isso significa que as políticas devem fornecer informações claras e acessíveis aos titulares de dados sobre como suas informações serão coletadas, utilizadas e protegidas pela empresa, incluindo detalhes sobre a finalidade do tratamento, o período de retenção dos dados e os direitos dos titulares.

Vide artigo 39 da Lei Geral de Proteção de Dados Pessoais:

Art. 39. 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.<sup>36</sup>

Além disso, as políticas abordam a obtenção de consentimento dos titulares de dados. De acordo com a LGPD, o consentimento deve ser obtido de forma clara e inequívoca, e os titulares têm o direito de revogá-lo a qualquer momento.<sup>37</sup> As políticas devem explicar como os titulares podem exercer esse controle sobre seus dados. E ainda, o consentimento para o tratamento dos dados pessoais sensíveis deverá ocorrer por meio de consentimento específico à atividade, nos termos do artigo 11, inciso I.<sup>38</sup>

As políticas também refletem o compromisso da empresa com a segurança dos dados pessoais. Com medidas técnicas e organizacionais para proteger os dados contra acessos não autorizados, vazamentos ou perdas. Assim, Santos afirma que o desenvolvimento e a revisão desses aspectos nas instituições necessitam ser efetivos, não bastando apenas um regulamento, código ou regras internas.<sup>39</sup>

---

<sup>36</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 15 de out. de 2023.

<sup>37</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 15 de out. de 2023.

<sup>38</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 15 de out. de 2023.

<sup>39</sup> SANTOS, Fernando de A. **Ética Empresarial: Políticas de Responsabilidade Social em 5 Dimensões**. Grupo GEN, 2023. E-book. ISBN 9786559775163. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9786559775163/>>. Acesso em: 23 de out. de 2023. p. 28.

Os agentes devem indicar quem é o Encarregado de Proteção de Dados (DPO), um papel fundamental na conformidade com a LGPD, podendo ser também pessoa física ou jurídica, sendo indicada pelo controlador dos dados em questão. Acerca do papel do “Responsável”, sua atividade envolve comunicação e manutenção do programa de conformidade, conforme artigo 41 da Lei Geral de Proteção de Dados Pessoais:

Art. 41. [...]

§ 2º As atividades do encarregado consistem em:

I – aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II – receber comunicações da autoridade nacional e adotar providências;

III – orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV – executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.<sup>40</sup>

Em casos em que a empresa compartilha dados pessoais com terceiros, as políticas de privacidade devem detalhar esse processo. O consentimento deve ser claro e de fácil acesso, usando linguagem objetiva.<sup>41</sup> Trazendo aos titulares sobre quem são esses terceiros, a finalidade do compartilhamento e as medidas de segurança adotadas para proteger os dados durante essa transferência.

A LGPD estabelece que os dados pessoais devem ser mantidos apenas pelo tempo necessário para cumprir a finalidade para a qual foram coletados e as políticas de privacidade devem indicar os períodos de retenção específicos e explicar como a empresa destruirá ou anonimiza os dados após o término desse prazo. Pestana, ainda reforça:

[...] que o titular seja cientificado da duração do tratamento, ou seja, não só do tempo a ser despendido para a sua realização, como,

---

<sup>40</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 15 de out. de 2023.

<sup>41</sup> TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei Geral de Proteção de dados pessoais: comentada artigo por artigo**. 2. Ed. rev. Atual. e ampl. Salvador: Editora JusPodivm, 2020 p. 56.

também, para o período em que os dados tratados estarão sendo utilizados para a finalidade correspondente ser atingida.<sup>42</sup>

Por fim, é importante compreender que as políticas de privacidade não devem ser percebidas como documentos inflexíveis, e devem ser consideradas como instrumentos dinâmicos, com revisão e atualização regular. Essa adaptação contínua é necessária para assegurar que as políticas permaneçam alinhadas com as mudanças nas práticas da empresa e nas regulamentações de privacidade em constante evolução.

Em resumo, as políticas de privacidade desempenham um papel central na garantia da conformidade com a Lei Geral de Proteção de Dados e na proteção dos direitos dos titulares de dados. Elas constituem um elemento fundamental da estratégia de conformidade com a LGPD de qualquer organização, contribuindo para assegurar que os dados pessoais sejam coletados, utilizados e protegidos de maneira ética e legal. Isso ocorre em estrita observância das obrigações legais, ao mesmo tempo que demonstra respeito pelos direitos e a privacidade dos indivíduos. As políticas de privacidade não apenas atendem aos requisitos regulatórios, mas também fortalecem a confiança do público e promovem uma cultura organizacional de respeito pela privacidade e pela proteção de dados. Portanto, sua criação e manutenção cuidadosas são fundamentais para o sucesso de qualquer empresa no ambiente legal.

#### **2.4. Adoção de medidas técnicas e organizacionais para garantir a proteção dos dados pessoais.**

A adoção de medidas técnicas e organizacionais para garantir a proteção dos dados pessoais é um pilar fundamental da conformidade com a legislação de privacidade. Essas medidas têm o objetivo de assegurar que os dados pessoais sejam tratados com o máximo de cuidado e responsabilidade, garantindo a privacidade e a segurança das informações dos indivíduos. Marcondes enfatiza a

---

<sup>42</sup> PESTANA, Márcio. **Os princípios no tratamento de dados na LGPD**. Consultor jurídico, 25 de maio de 2020. Disponível em: <<https://www.conjur.com.br/dl/artigo-mar-cio-pestanalgpd.pdf>>. Acesso em: 10 de out. de 2023. p. 02.

relevância de medidas técnicas e organizacionais, como a criptografia, a gestão de acesso e a realização periódica de cópias científicas de segurança, bem como a aplicação de diretrizes de segurança da informação a fim de fomentar a segurança das informações pessoais mantidas.<sup>43</sup>

As medidas técnicas referem-se à implementação de tecnologias e práticas específicas para proteger os dados pessoais. Conforme Almeida e Santos, no âmbito da LGPD, as organizações estão obrigadas a estabelecer precauções com vistas à proteção das informações pessoais e à garantia da confidencialidade e proteção dos usuários. Isso compreende a incorporação de procedimentos técnicos e administrativos, tais como a criptografia, as explicitamente de segurança e as estratégias de controle de acesso, adicionalmente com a adoção de princípios e diretrizes transparentes e moralmente justas em relação ao tratamento de informações.<sup>44</sup> Além disso, medidas como autenticação de dois fatores, monitoramento de segurança em tempo real e proteção contra malware são exemplos de práticas técnicas que contribuem para a proteção dos dados pessoais.

As medidas organizacionais, por outro lado, se concentram na criação de uma cultura de privacidade e segurança dentro da organização. Isso envolve a definição de políticas claras de privacidade e segurança de dados, e a promoção da conscientização e treinamento dos funcionários em relação às melhores práticas de proteção de dados. A elaboração de um plano de resposta a incidentes de segurança também faz parte das medidas organizacionais, permitindo que a empresa saiba como agir em caso de violações de dados. A resposta eficiente a incidentes contribui para minimizar os danos e demonstra o compromisso da empresa em proteger os dados pessoais<sup>45</sup>

A conformidade com a LGPD e outras regulamentações de privacidade exige uma abordagem holística que combine medidas técnicas e organizacionais. Essas

---

<sup>43</sup> MARCONDES, F. R. S. **A Nova Lei Geral de Proteção de Dados Pessoais** : Comentários à Lei n. 13.709/18. São Paulo: Thomson Reuters Brasil, 2021. MEDIDA PROVISÓRIA nº 954/2020. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_Ato2019-2022/2020/Mpv/mpv954.htm](http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Mpv/mpv954.htm)>. Acesso em: 15 set. 2023. p. 68.

<sup>44</sup> ALMEIDA, N. N.; SANTOS, S. L. F. Gestão de dados pessoais em conformidade com a LGPD. In: **ENCONTRO DE ADMINISTRAÇÃO**, 8., 2020, Joinville-SC. Joinville-SC: INESUL, 2020. p. 7.

<sup>45</sup> PEREIRA, L. S. **A Lei Geral de Proteção de Dados (LGPD)** : Seus Aspectos Fundamentais. São Paulo: Novo Século Editora, 2019. p.45.

medidas não apenas protegem os dados pessoais contra acessos não autorizados, mas também garantem que as organizações estejam em conformidade com as regulamentações, evitando multas substanciais e danos à reputação. Além disso, a proteção eficaz dos dados pessoais fortalece a confiança dos clientes e parceiros de negócios, demonstrando um compromisso com a privacidade e a segurança das informações confidenciais.

Em última análise, a adoção de medidas técnicas e organizacionais é essencial para enfrentar os desafios crescentes no cenário de proteção de dados e para garantir que os direitos dos indivíduos sejam preservados em um mundo digital em constante evolução.

## 2.5 Avaliação regular de conformidade com a LGPD

A Lei Geral de Proteção de Dados é a legislação brasileira que regula o tratamento de dados pessoais por organizações e estabelece obrigações em relação à privacidade e proteção de dados. Para garantir a conformidade com a LGPD, é fundamental realizar avaliações regulares e implementar medidas adequadas.

Primeiramente, é importante nomear um Encarregado de Proteção de Dados (DPO), que será responsável por supervisionar a conformidade com a LGPD e orientar a organização em relação às práticas de proteção de dados. Esse profissional desempenha um papel crucial na garantia de conformidade. Lima esclarece:

O DPO pode ser um elemento do pessoal da entidade responsável pelo tratamento, por exemplo, um funcionário do controlador, ou exercer as suas funções com base em um contrato de prestação de serviços, isto é, o controlador contrata uma empresa especializada em proteção de dados para dar esse suporte.<sup>46</sup>

---

<sup>46</sup> LIMA, Cíntia Rosa Pereira de. **Comentários à Lei Geral de Proteção de Dados**. Grupo Almedina (Portugal), 2020. E-book. ISBN 9788584935796. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9788584935796/>>. Acesso em: 17 de out. de 2023.

E na organização deve realizar um mapeamento abrangente dos dados pessoais que coleta, armazena, processa e compartilha. Isso inclui a identificação de dados de clientes, funcionários e outras partes envolvidas. Garrido reforça em seu estudo:

É imprescindível para que a organização possua um “mapa” de todas as atividades de tratamento de dados pessoais que realizam, auxiliando, ainda, no cumprimento das demais obrigações trazidas pela LGPD, como atendimento aos direitos dos titulares de dados pessoais e registros de eventuais incidentes.<sup>47</sup>

Nesta parte é essencial avaliar se a organização possui bases legais para o processamento de dados pessoais, como o consentimento dos titulares, a execução de contratos ou o cumprimento de obrigações legais. A LGPD exige que o tratamento de dados pessoais seja respaldado por uma base legal.

Ao desenvolver políticas internas e procedimentos alinhados com os princípios da LGPD é crucial adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas<sup>48</sup>, trazendo como os dados pessoais são coletados, tratados, armazenados e compartilhados, bem como as medidas de segurança obrigatórias. A conscientização e o treinamento de toda a equipe são igualmente importantes, trazendo a compreensão da importância da LGPD e conhecendo suas responsabilidades em relação à proteção de dados.

Manter um registro das atividades de tratamento de dados pessoais é uma exigência da LGPD, incluindo documentar as operações de processamento de dados realizadas pela organização. E inclusive a realização de Avaliações de Impacto sobre a Proteção de Dados (AIPD) é necessária sempre que uma atividade de processamento de dados possa ter um impacto significativo na privacidade dos titulares dos dados trazendo ajuda para identificar e mitigar riscos.

---

<sup>47</sup> GARRIDO, Patricia P. **Proteção de dados pessoais: comentários à lei n. 13.709/2018 (LGPD)**. Editora Saraiva, 2023. E-book. ISBN 9786555599480. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9786555599480/>>. Acesso em: 17 de out. de 2023.

<sup>48</sup> GARCIA, Lara R. **Lei Geral de Proteção de Dados (LGPD): Guia de implantação**. Editora Blucher, 2020. E-book. ISBN 9786555060164. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9786555060164/>>. Acesso em: 17 de out. de 2023.

A organização deve implementar medidas de segurança rigorosas para proteger os dados pessoais, como criptografia, controle de acesso e monitoramento de segurança. Em caso de violação de dados pessoais, é essencial ter procedimentos com vigor para notificar as autoridades e os titulares de dados afetados. Inclusive, nestes casos os titulares de dados, bem como o direito de acesso, podem solicitar exclusão e portabilidade de dados, e devem ser respeitados e atendidos pela organização.

Neste mesmo sentido Garrido afirma:

[...] as organizações são responsáveis no caso de incidentes – como vazamentos – no tratamento dos dados, devem aplicar medidas de prevenção e proteção à segurança dos dados que manuseiam, como anonimização e encriptação das informações. Ainda assim, no caso de qualquer incidente é obrigação da organização notificar as autoridades imediatamente.<sup>49</sup>

É necessário realizar auditorias regulares internas, sendo uma prática recomendada para garantir que todas as políticas e procedimentos sejam seguidos e que a conformidade com a LGPD seja mantida, conforme cita o artigo 50, § 2º.<sup>50</sup> Dessa forma é importante manter-se atualizado sobre as mudanças na legislação e nas melhores práticas de proteção de dados e ajustar as políticas e procedimentos conforme necessário. Além disso, a organização deve avaliar a conformidade dos parceiros de negócios e abordar os serviços que têm acesso aos dados pessoais. Para evitar que os requisitos impostos não sejam preenchidos.

A empresa deverá manter-se em contato com todos os titulares de dados, ou manter uma linha de contato fácil e direto para lidar com reclamações de titulares de dados e obrigações relacionadas à LGPD, além do objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure

---

<sup>49</sup> GARRIDO, Patricia P. **Proteção de dados pessoais: comentários à lei n. 13.709/2018 (LGPD)**. Editora Saraiva, 2023. E-book. ISBN 9786555599480. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9786555599480/>>. Acesso em: 17 de out. de 2023.

<sup>50</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 18 de out. de 2023.

mecanismos de participação do titular conforme explícito no artigo 50<sup>51</sup>. E ainda cita que é de suma importância manter uma documentação detalhada de todas as atividades relacionadas à proteção de dados, incluindo documentos de consentimento<sup>52</sup>, AIPDs, políticas e auditorias, para demonstrar a conformidade com a LGPD.

Dessa forma a conformidade com a LGPD é um processo contínuo que exige compromisso constante com a proteção de dados pessoais. Consultar profissionais jurídicos e especialistas em privacidade de dados é fundamental para garantir uma abordagem sólida e atualizada de acordo com as mudanças na legislação e nas melhores práticas.

---

<sup>51</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 18 de out. de 2023.

<sup>52</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 18 de out. de 2023.

## CAPÍTULO 3: IMPLICAÇÕES JURÍDICAS DA LGPD NA GESTÃO EMPRESARIAL

### 3.1. Responsabilidade dos Controladores e Operadores de Dados

A Lei Geral de Proteção de Dados é uma legislação que estabelece regras e diretrizes para o tratamento de dados pessoais no Brasil, com o objetivo principal de proteger a privacidade e os direitos dos titulares desses dados. No âmbito da LGPD, há uma distinção importante entre os controladores e operadores de dados, e ambos têm responsabilidades específicas no que diz respeito à gestão de informações pessoais.

Os controladores de dados são as entidades ou organizações que decidem como e para que os dados pessoais são processados. Eles determinam os fins para quais dados serão usados e têm a responsabilidade primária pela conformidade com a LGPD conforme cita o artigo 50 da Lei Geral de Proteção de Dados Pessoais:

Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.<sup>53</sup>

Algumas das responsabilidades dos controladores incluem a concessão de consentimento, garantia de bases legais, transparência nas práticas de coleta, uso e compartilhamento de dados, implementação de medidas adequadas de segurança de dados e resposta a cláusulas válidas de titulares de dados.

---

<sup>53</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 18 de out. de 2023.

Já os operadores de dados são empresas ou organizações que realizam o processamento de dados em nome dos controladores, de acordo com suas instruções. Embora não tenham o controle final sobre as decisões de tratamento de dados, os operadores também têm responsabilidades sob a LGPD, incluindo o cumprimento das instruções específicas dos controladores, a implementação de medidas de segurança, a prestação de assistência aos controladores em relação ao cumprimento da LGPD, notificação imediata de dados divulgados aos controladores, e realizar o controle de probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.<sup>54</sup>

A LGPD estabelece uma estrutura clara de responsabilidades para controladores e operadores, com o objetivo de proteger a privacidade e os direitos dos titulares de dados. Cumprir essas responsabilidades é essencial para garantir a conformidade com a legislação e evitar prejuízos.

Portanto, as organizações devem investir tempo e recursos para entender e cumprir suas obrigações sob a LGPD. Além disso, a conformidade com a LGPD não é estática e requer uma revisão contínua das práticas de proteção de dados à medida que a legislação evolui e as situações mudam. A fim de evitar problemas futuros com fiscalizações, é necessário se adequar de acordo com as mudanças solicitadas na legislação.

### **3.2. Análise das penalidades previstas na LGPD para empresas em não conformidade**

A Lei Geral de Proteção de Dados estabelece um conjunto de decisões e avaliações que podem ser aplicadas a empresas que não estejam em conformidade com suas disposições. Essas decisões visam garantir o cumprimento da lei, bem como proteger a privacidade e os direitos dos titulares de dados. E a análise das previsões previstas na LGPD para empresas em não conformidade revela a

---

<sup>54</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 18 de out. de 2023.

seriedade com que a legislação aborda a proteção de dados pessoais. Dessa forma, Lima diz que:

No âmbito da LGPD, o art. 44 assevera que o tratamento de dados será tido por irregular ao não se observar o que dispõe a lei ou por não fornecer a segurança que o titular pode esperar do tratamento dos dados pessoais.<sup>55</sup>

Uma das principais deliberações da LGPD é uma multa, que pode ser aplicada em casos de violação das disposições da lei. As multas podem variar de 2% do faturamento anual da empresa no Brasil, limitadas a um total de 50 milhões de reais por infração, a 2% do faturamento global da empresa, caso a empresa não tenha presença no Brasil, conforme artigo 52 da Lei Geral de Proteção de Dados Pessoais.<sup>56</sup> Essas multas podem ser aplicadas em casos de coleta ou tratamento de dados sem consentimento, não fornecidas informações sobre o tratamento de dados, falta de medidas de segurança adequadas, entre outras específicas. Além das multas, a LGPD também prevê outras avaliações que podem ser aplicadas às empresas em não conformidade. Entre elas, estão a publicação da infração após devidamente apurada e confirmada, a suspensão parcial ou total do tratamento de dados pessoais e a eliminação dos dados pessoais relacionados à infração. Dessa forma:

Ainda, visando concretizar a indenização ao titular, o inc. II do § 1º do art. 42 da LGPD descreve que, havendo dois ou mais controladores, os que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados responderão solidariamente (salvo excludentes do art. 43).<sup>57</sup>

---

<sup>55</sup> LIMA, Cíntia Rosa Pereira de. **Comentários à Lei Geral de Proteção de Dados**. Grupo Almedina (Portugal), 2020. E-book. ISBN 9788584935796. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9788584935796/>>. Acesso em: 02 de out. de 2023. p. 310.

<sup>56</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 18 de out. de 2023.

<sup>57</sup> LIMA, Cíntia Rosa Pereira de. **Comentários à Lei Geral de Proteção de Dados**. Grupo Almedina (Portugal), 2020. E-book. ISBN 9788584935796. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9788584935796/>>. Acesso em: 02 de out. de 2023. p. 315.

A LGPD também permite que os titulares de dados afetados pela violação de seus direitos busquem indenização por danos morais e materiais<sup>58</sup>, o que pode resultar em custos adicionais para as empresas não conformes. É importante ressaltar que a fiscalização e a aplicação das recomendações da LGPD são de responsabilidade da Autoridade Nacional de Proteção de Dados (ANPD), órgão criado pela legislação. A ANPD tem o poder de conduzir investigações, aplicar deliberações e monitorar o cumprimento das leis pelas empresas. Nesse mesmo sentido Garrido afirma:

Não obstante as atividades de fiscalização, a ANPD poderá realizar atividades repressivas, mediante a aplicação de sanção, através de um processo administrativo sancionador.<sup>59</sup>

Portanto, a análise das previsões previstas na LGPD para empresas em não conformidade destaca a importância da conformidade com a legislação de proteção de dados. A não conformidade das obrigações da LGPD não apenas expõe as empresas a riscos financeiros, mas também pode prejudicar sua confiança e a confiança dos clientes. Como resultado, as empresas devem investir recursos adequados na implementação de medidas de conformidade com a LGPD, como políticas de privacidade robustas, treinamento de pessoal e medidas de segurança de dados, a fim de evitar as diversas decisões previstas pela legislação.

### **3.3. Revisão e adequação dos contratos com parceiros, fornecedores e clientes, incluindo cláusulas de proteção de dados.**

A revisão e conformidade dos contratos com parceiros, fornecedores e clientes, incluindo cláusulas de proteção de dados, é uma etapa essencial para garantir a conformidade com as regulamentações de privacidade de dados, como a Lei Geral de Proteção de Dados no Brasil, e para proteger a privacidade dos titulares

---

<sup>58</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 18 de out. de 2023.

<sup>59</sup> GARRIDO, Patricia P. **Proteção de dados pessoais: comentários à lei n. 13.709/2018 (LGPD)**. Editora Saraiva, 2023. E-book. ISBN 9786555599480. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9786555599480/>>. Acesso em: 23 de out. de 2023.

de dados. A proteção de dados tornou-se uma preocupação crítica nas relações comerciais, uma vez que as empresas coletam e processam informações pessoais com uma grande frequência.

Com a entrada em vigor da LGPD e outras regulamentações de privacidade em todo o mundo, as empresas têm obrigações legais específicas em relação ao tratamento de dados pessoais. É importante que os contratos reflitam essas obrigações e requisitos legais. Tal ainda reforça que deve-se alinhar todos os contratos com clientes e fornecedores (operadores) garantindo o atendimento aos requisitos da lei.<sup>60</sup>

Quando os dados pessoais são compartilhados com parceiros, fornecedores ou clientes, há uma responsabilidade compartilhada de proteção dessas informações. As cláusulas contratuais podem definir claramente quem é responsável pelo quê em relação à proteção de dados. Garcia ressalta a importância da legislação nas cláusulas contratuais:

Além da exigência de legislação no país de destino, requer-se também que o Controlador garanta que todos os direitos do Titular estejam sendo respeitados, principalmente em cláusulas contratuais, sejam elas específicas ou padrão, normas corporativas e até selos, certificados e códigos de conduta. Nesse sentido, a área de Compliance pode ter papel importante nessa discussão, como um validador do trabalho realizado pela Organização.<sup>61</sup>

Os titulares de dados têm direitos específicos sob a LGPD, como o direito de acesso, retificação, exclusão e portabilidade de seus dados.<sup>62</sup> Os contratos devem incluir disposições que permitam o exercício desses direitos pelos titulares de dados e que estabeleçam procedimentos claros para isso. Além disso, os contratos devem abordar medidas de segurança de dados que devem ser inovadoras para proteger

<sup>60</sup> MARINHO, Fernando. **Os 10 Mandamentos da LGPD - Como Implementar a Lei Geral de Proteção de Dados em 14 Passos**. Grupo GEN, 2020. E-book. ISBN 9788597026009. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9788597026009/>>. Acesso em: 25 de out. de 2023. p. 82.

<sup>61</sup> GARCIA, Lara R. **Lei Geral de Proteção de Dados (LGPD): Guia de implantação**. Editora Blucher, 2020. E-book. ISBN 9786555060164. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9786555060164/>>. Acesso em: 25 de out. de 2023.

<sup>62</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 18 de out. de 2023.

as informações pessoais, incluindo criptografia, controle de acesso e outras medidas de segurança adequadas.

Os contratos devem definir os períodos de retenção de dados e como os dados pessoais serão excluídos ou devolvidos após o término da relação comercial. As partes também podem incluir disposições que permitem auditorias e monitoramento para garantir que as práticas de proteção de dados sejam cumpridas. Vale ressaltar a citação de Vigliar:

[...] deve considerar um especialista para avaliar a implementação e para analisar os riscos, além de proceder com auditorias e treinamentos de todos da empresa.<sup>63</sup>

Por fim, é essencial que as empresas revejam seus contratos existentes e atualizem os novos contratos de acordo com as regulamentações de proteção de dados aplicáveis. Oliveira explica:

É extremamente importante que o operador também crie ciclos de vida de dados pessoais recebidos do controlador, ainda que seja um ciclo de vida bastante simples, como por exemplo, a vigência do contrato com o mesmo.<sup>64</sup>

Isso não apenas ajuda a garantir a conformidade legal, mas também demonstra um compromisso com a proteção da privacidade e a transparência nas relações comerciais, construindo confiança entre as partes envolvidas. E neste mesmo sentido a ANPD também será responsável por verificar se nas cláusulas contratuais os direitos do Titular estão presentes.<sup>65</sup> Por isso é essencial consultar um advogado especializado em privacidade de dados para garantir que as cláusulas contratuais sejam específicas e práticas na proteção de dados pessoais.

---

<sup>63</sup> VIGLIAR, José Marcelo M. **LGPD e a Proteção de Dados Pessoais na Sociedade em Rede**. Grupo Almedina (Portugal), 2022. E-book. ISBN 9786556276373. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9786556276373/>>. Acesso em: 25 de out. de 2023. p. 240.

<sup>64</sup> OLIVEIRA, Ricardo. **LGPD: Como evitar as avaliações administrativas**. Editora Saraiva, 2021. E-book. ISBN 9786553623262. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9786553623262/>>. Acesso em: 25 de out. de 2023.

<sup>65</sup> GARCIA, Lara R. **Lei Geral de Proteção de Dados (LGPD): Guia de implantação**. Editora Blucher, 2020. E-book. ISBN 9786555060164. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9786555060164/>>. Acesso em: 25 de out. de 2023. p. 23.

### 3.4. Procedimentos para notificar titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD) em caso de vazamentos ou violações de dados

Quando ocorrerem vazamentos ou violações de dados, é essencial seguir procedimentos específicos para notificar tanto os titulares de dados quanto a Autoridade Nacional de Proteção de Dados (ANPD) de acordo com as regulamentações de privacidade de dados, como a Lei Geral de Proteção de Dados no Brasil.<sup>66</sup> Esses procedimentos são importantes para garantir a transparência, a responsabilidade e o cumprimento das obrigações legais.

A primeira etapa é identificar e confirmar se ocorreu um vazamento ou violação de dados. Isso pode envolver a detecção de atividades suspeitas, relatórios de funcionários ou outros mecanismos de monitoramento de segurança. Assim que o incidente for identificado, é importante isolar a causa e tomar medidas imediatas para mitigar os danos. Isso pode incluir suspensão de acesso não autorizado, correção de vulnerabilidades e outras ações para conter o incidente. Avaliar o impacto do incidente, determinando quais dados foram afetados, o número de titulares envolvidos e o impacto potencial sobre a privacidade e os direitos dos titulares. Dessa forma Oliveira reforça:

Para a apuração de responsabilidades, especialmente a penal, é essencial identificar a pessoa natural que agiu gerando o dano à empresa, atestando-se tecnologicamente que ela acessou determinado dado.<sup>67</sup>

De acordo com a LGPD, os titulares de dados devem ser notificados em caso de vazamento ou violação de dados que possam resultar em riscos ou danos

---

<sup>66</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 18 de out. de 2023.

<sup>67</sup> OLIVEIRA, Ricardo. **LGPD: Como evitar as avaliações administrativas**. Editora Saraiva, 2021. E-book. ISBN 9786553623262. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9786553623262/>>. Acesso em: 25 de out. de 2023.

significativos para eles.<sup>68</sup> A notificação deve ser feita de forma clara e transparente, informando sobre os detalhes do incidente, o tipo de dados afetados, as medidas tomadas e os próximos passos que os titulares podem tomar.

Em casos de incidentes de segurança que envolvam riscos significativos para os titulares de dados, a LGPD exige que a ANPD seja notificada no momento.<sup>69</sup> Essa notificação deve ser feita sem demora indevida e deve incluir informações sobre o incidente, como sua natureza, impacto e medidas tomadas para remediar a situação.

Manter registros de todos os incidentes de vazamento ou violação de dados, incluindo detalhes sobre a detecção, investigação, notificação aos titulares e comunicação com a ANPD. É de suma importância colaborar com a ANPD e outras autoridades competentes, conforme necessário, para investigar e remediar a violação de dados conforme cita o artigo 48 da LGPD.<sup>70</sup> Isso pode incluir o fornecimento de informações adicionais e cooperação total durante as investigações.

Após o incidente, é importante realizar uma análise detalhada para entender as causas subjacentes e identificar áreas onde a segurança de dados pode ser aprimorada na empresa.

Cumprir rigorosamente os procedimentos é crucial para cumprir as obrigações da LGPD e outras regulamentações de privacidade de dados. Além disso, demonstrar um compromisso com a proteção da privacidade dos titulares de dados ajuda a evitar prejuízos graves por não conformidade. Consultar um advogado especializado em privacidade de dados pode ser benéfico para garantir que os procedimentos de envio sejam preenchidos em conformidade com a lei e as melhores práticas.

---

<sup>68</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 18 de out. de 2023.

<sup>69</sup> GARRIDO, Patricia P. **Proteção de dados pessoais: comentários à lei n. 13.709/2018 (LGPD)**. [Digite o Local da Editora]: Editora Saraiva, 2023. E-book. ISBN 9786555599480. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9786555599480/>>. Acesso em: 25 de out. de 2023.

<sup>70</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 18 de out. de 2023.

### 3.5. Critérios para obtenção de consentimento válido dos titulares de dados para o tratamento de suas informações.

A concessão de consentimento válido dos titulares de dados é um dos princípios fundamentais da proteção de dados pessoais. No contexto da era digital, em que a coleta e o tratamento de informações pessoais são presentes, estabelecer critérios sólidos para garantir o registro adequado tornou-se uma preocupação crucial. Afinal, os indivíduos têm o direito fundamental de controlar suas informações e decidir como elas serão usadas.

Para que um consentimento seja considerado válido e em conformidade com os regulamentos de privacidade, como o Regulamento Geral de Proteção de Dados na União Europeia ou a Lei de Proteção de Dados Pessoais no Brasil, vários critérios precisam ser atendidos.

Os titulares de dados devem ser informados de maneira clara e explicativa sobre como seus dados serão coletados e usados. Isso inclui detalhes sobre as finalidades do tratamento, os tipos de dados encontrados, a duração do tratamento e qualquer compartilhamento de dados com terceiros. Assim, Oliveira cita:

A ausência de informação clara e precisa ao titular sobre o tratamento de dados pessoais realizado é uma das mais graves e flagrantes da LGPD. Isso porque impossibilita o exercício dos direitos relacionados e torna incerta a base legal de tratamento de dados pessoais.<sup>71</sup>

Após, o consentimento deve ser dado de forma voluntária e livre de pressão ou coerção. Os titulares de dados não devem ser obrigados a consentir para acessar serviços essenciais ou produtos.

Vale lembrar que os titulares de dados devem ser informados sobre qualquer alteração específica no tratamento dos dados e ter a opção de consentir novamente,

---

<sup>71</sup> OLIVEIRA, Ricardo. **LGPD: Como evitar as sanções administrativas**. Editora Saraiva, 2021. E-book. ISBN 9786553623262. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9786553623262/>>. Acesso em: 25 de out. de 2023. p. 17.

e ainda têm o direito de cancelar a utilização a qualquer momento.<sup>72</sup> E as empresas e organizações devem garantir que esse processo seja simples e eficiente para o titular.

E as empresas precisam manter registros que comprovem que o consentimento foi recebido de acordo com os requisitos legais. Essa questão é essencial para a prestação de contas e para comprovar a conformidade com as regulamentações de privacidade. No mesmo sentido, as empresas devem adotar medidas técnicas e organizacionais para garantir a conformidade com os critérios de consentimento, e se manterem dentro dos padrões exigidos pela legislação.

Vale reforçar a citação de Oliveira em sua obra:

Desta forma, recomendo que qualquer insumo produzido no processo de adequação, tais como políticas, regulamentos, planos de trabalho, análise de gaps, relatórios de incidentes, entre outros, devem ser preservados para comprovação futura, no caso de necessidade.<sup>73</sup>

Outro ponto de suma importância, os titulares de dados têm o direito de receber informações contínuas sobre como seus dados são tratados, e como estão sendo utilizados pela empresa.<sup>74</sup> Incluindo notificações sobre qualquer violação de dados que possa afetá-los ou até mesmo acompanhamento por meio de aplicativos disponibilizados pela empresa.

Em resumo, os critérios para concessão de autorização válida dos titulares de dados são fundamentais para garantir a privacidade e a proteção dos direitos individuais no mundo, cada vez mais orientados por dados. É responsabilidade das organizações e das autoridades reguladoras garantir que esses critérios sejam

---

<sup>72</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 18 de out. de 2023.

<sup>73</sup> OLIVEIRA, Ricardo. **LGPD: Como evitar as sanções administrativas**. Editora Saraiva, 2021. E-book. ISBN 9786553623262. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9786553623262/>>. Acesso em: 25 de out. de 2023.

<sup>74</sup> BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 18 de out. de 2023.

rigorosamente seguidos para proteger os dados pessoais e a privacidade das pessoas.

## CONSIDERAÇÕES FINAIS

A Lei Geral de Proteção de Dados, declarou ter um impacto significativo nas práticas de gestão empresarial. Através da análise dos vários aspectos dessa regulamentação ao longo deste estudo, ficou evidente que a LGPD tem o potencial de redefinir a maneira como as empresas coletam, tratam e protegem os dados pessoais.

No início deste trabalho, explorou-se a origem, os objetivos e os princípios da LGPD. A lei foi inspirada em regulamentações semelhantes, como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, refletindo uma tendência global em direção à proteção dos direitos dos titulares de dados. Os princípios da LGPD, como o consentimento, a especificamente e a transparência, estabelecem a base para uma abordagem mais ética e transparente no tratamento de dados.

Em seguida, examinou-se os direitos dos titulares de dados, enfatizando o empoderamento que a LGPD oferece aos indivíduos na relação com seus dados pessoais. Os titulares de dados agora têm o direito de acessar, concordar e excluir suas informações pessoais, bem como saber como seus dados estão sendo usados. Isso implica que as empresas devem implementar sistemas que permitam uma fácil gestão desses direitos pelos titulares. Além disso, aborda a aplicabilidade empresarial da LGPD, identificando os setores e atividades mais afetados pela regulamentação. E assim, constatou-se que a LGPD abrange uma ampla gama de organizações, desde pequenas empresas até grandes corporações, independentemente do setor de atuação. Portanto, a conformidade com a LGPD tornou-se uma prioridade para uma vasta parte das atividades empresariais brasileiras. E no contexto dos impactos na coleta e tratamento de dados, destacou-se como a LGPD exige um nível alto de responsabilidade no gerenciamento das informações pessoais dos clientes e colaboradores. As empresas devem estar cientes de que a coleta e o processamento de dados devem ser feitos de forma justa e transparente, com a necessidade de identificar os dados sensíveis e garantir medidas de segurança adequadas.

Uma descoberta fundamental deste estudo foi a importância da implementação de políticas e procedimentos para a proteção de dados nas empresas. Essas políticas servem como orientações para funcionários e parceiros de negócios, estabelecendo práticas sólidas para garantir a conformidade com a LGPD, e a falta de tais políticas pode resultar em riscos significativos para as empresas. E neste mesmo sentido o presente trabalho explorou os riscos e avaliações para as empresas que não se adequam à LGPD, constatando que as deliberações são substanciais e podem incluir muitas significativas, o que pode ter um impacto devastador nas finanças de uma empresa.

As políticas de privacidade desempenham um papel fundamental na conformidade com a LGPD, conforme discutido no item 2.3. As empresas devem fornecer informações claras e acessíveis aos titulares de dados sobre como seus dados serão usados, sendo incluídos na política da empresa. A adoção de medidas técnicas e organizacionais para garantir a proteção de dados pessoais é um aspecto crítico da conformidade com a LGPD, conforme citado nos itens acima. Isso inclui implementação de criptografia, controles de acesso, auditorias regulares para garantir que os dados permaneçam seguros, além de outras implementações que ajudam a se manter regular com a legislação.

Finalmente, na última parte deste trabalho, discutiu-se as implicações jurídicas da LGPD na gestão empresarial. As responsabilidades dos controladores e operadores de dados, conforme detalhado, destacam a necessidade de esclarecer as atribuições e responsabilidades dentro de uma organização para não haver riscos e sanções para a área empresarial. A LGPD deixa claro que todos os envolvidos no tratamento de dados pessoais têm um papel crucial na conformidade com a lei, e nos cuidados com todos os dados pessoais que são utilizados e manuseados.

A revisão e conformidade dos contratos com parceiros, fornecedores e clientes, incluindo cláusulas de proteção de dados é uma parte vital da conformidade com a LGPD, talvez uma das mais importantes. Isso garante que todas as partes envolvidas estejam comprometidas com a proteção dos dados pessoais. Além disso, os procedimentos para notificar os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD) em caso de vazamento ou divulgação de dados

também são fundamentais para evitar maiores transtornos para a empresa que vazou os dados e para o titular dos dados.

Em resumo, a LGPD impõe desafios significativos às empresas brasileiras, que agora precisam reavaliar e aprimorar suas práticas de coleta, tratamento e proteção de dados pessoais. As implicações da LGPD na gestão empresarial são inegáveis, e a não conformidade com essa regulamentação pode resultar em sérias consequências legais e financeiras. Portanto, a hipótese inicial de que a LGPD é altamente relevante para a gestão empresarial foi totalmente comprovada. As empresas precisam agir rapidamente para garantir a conformidade e a proteção eficaz dos dados pessoais, respeitando os direitos dos titulares de dados e evitando as consequências e sanções da LGPD. Em um mundo cada vez mais orientado por dados, a conformidade com a LGPD é uma prioridade incontestável e primordial em empresas que manuseiam dados.

## REFERÊNCIAS

ALMEIDA, N. N.; SANTOS, S. L. F. Gestão de dados pessoais em conformidade com a LGPD. In: **ENCONTRO DE ADMINISTRAÇÃO**, 8., 2020, Joinville-SC. Joinville-SC: INESUL, 2020. p. 7.

BITTAR, C. A. C.; TOMASCHEWSKI, T. A Lei Geral de Proteção de Dados Pessoais e sua aplicação prática nas empresas. In: **CONGRESSO INTERNACIONAL DE ADMINISTRAÇÃO**, XXVI., 2021, Rio de Janeiro-RJ.

BRASIL. Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em: 18 de out. de 2023.

FERREIRA, D. C. (2020). Lei Geral de **Proteção de dados pessoais**: a implementação e seus desafios para a administração pública e privada no Brasil. Revista de Direito, 18(32). p. 108.

GARCIA, Lara R. **Lei Geral de Proteção de Dados (LGPD)**: Guia de implantação. Editora Blucher, 2020. E-book. ISBN 9786555060164. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9786555060164/>>. Acesso em: 25 de out. de 2023. p. 23.

GARRIDO, Patricia P. **Proteção de dados pessoais**: comentários à lei n. 13.709/2018 (LGPD) . [Digite o Local da Editora]: Editora Saraiva, 2023. E-book. ISBN 9786555599480. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9786555599480/>>. Acesso em: 25 de out. de 2023.

**General Data Protection Regulation (GDPR)** – official legal text. Disponível em: <<https://gdpr-info.eu/>>. Acesso em: 20 de ago. de 2023.

LIMA, Ana Paula Moraes Canto de. **LGPD Aplicada**. Grupo GEN, 2021. E-book. ISBN 9788597026931. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9788597026931/>>. Acesso em: 13 de out. de 2023.

LIMA, Cíntia Rosa Pereira de. **Comentários à Lei Geral de Proteção de Dados**. Grupo Almedina (Portugal), 2020. E-book. ISBN 9788584935796. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9788584935796/>>. Acesso em: 02 de out. de 2023. p. 315.

MARCONDES, F. R. S. **A Nova Lei Geral de Proteção de Dados Pessoais** : Comentários à Lei n. 13.709/18. São Paulo: Thomson Reuters Brasil, 2021. MEDIDA PROVISÓRIA nº 954/2020. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_Ato2019-2022/2020/Mpv/mpv954.htm](http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Mpv/mpv954.htm)>. Acesso

em: 15 set. 2023. p. 68.

MARINHO, Fernando. **Os 10 Mandamentos da LGPD** - Como Implementar a Lei Geral de Proteção de Dados em 14 Passos. Grupo GEN, 2020. E-book. ISBN 9788597026009. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9788597026009/>>. Acesso em: 25 de out. de 2023. p. 82.

OLIVEIRA, Ricardo. **LGPD: Como evitar as sanções administrativas**. Editora Saraiva, 2021. E-book. ISBN 9786553623262. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9786553623262/>>. Acesso em: 25 de out. de 2023.

PEREIRA, L. S. **A Lei Geral de Proteção de Dados (LGPD): Seus Aspectos Fundamentais**. São Paulo: Novo Século Editora, 2019. p.45.

PESTANA, Márcio. **Os princípios no tratamento de dados na LGPD**. Consultor jurídico, 25 de maio de 2020. Disponível em: <<https://www.conjur.com.br/dl/artigo-mar-cio-pestanalgpd.pdf>>. Acesso em: 10 de out. de 2023. p. 02.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários à Lei n.º 13.709/2018 (LGPD)**. 2. ed. São Paulo: Saraiva Educação, 2020. p. 19.

SANTOS, Fernando de A. **Ética Empresarial: Políticas de Responsabilidade Social em 5 Dimensões**. Grupo GEN, 2023. E-book. ISBN 9786559775163. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9786559775163/>>. Acesso em: 23 de out. de 2023. p. 28.

SERPRO-SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS. **LGPD e saúde: os fins justificam os meios?** — LGPD - Lei Geral de Proteção de Dados Pessoais. Disponível em: <<https://www.serpro.gov.br/lgpd/noticias/2019/paciente-no-comando-lgpd-dados-sensiveis-saude>>.

TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei Geral de Proteção de dados pessoais: comentada artigo por artigo**. 2. Ed. rev. Atual. e ampl. Salvador: Editora JusPodivm, 2020 p. 56.

VIGLIAR, José Marcelo M. **LGPD e a Proteção de Dados Pessoais na Sociedade em Rede**. Grupo Almedina (Portugal), 2022. E-book. ISBN 9786556276373. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9786556276373/>>. Acesso em: 25 de out. de 2023. p. 240.