



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

**ISABELLE RAIANE SILVA CORREA**

**A PROTEÇÃO DE DADOS NA INDÚSTRIA DO AGRONEGÓCIO:  
DESAFIOS E PERSPECTIVAS NA APLICAÇÃO DA LGPD E NA ADOÇÃO DE  
TECNOLOGIAS AVANÇADAS**

**Assis/SP**

**2024**



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

**ISABELLE RAIANE SILVA CORREA**

**A PROTEÇÃO DE DADOS NA INDÚSTRIA DO AGRONEGÓCIO:  
DESAFIOS E PERSPECTIVAS NA APLICAÇÃO DA LGPD E NA ADOÇÃO DE  
TECNOLOGIAS AVANÇADAS**

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

**Orientanda: ISABELLE RAIANE SILVA  
CORREA**

**Orientadora: GISELE SPERA MÁXIMO**

**Assis/SP  
2024**

Correa, Isabelle Raiane Silva

C824p A proteção de dados na indústria do agronegócio: desafios e perspectivas na aplicação da LGPD e na adoção de tecnologias avançadas / Isabelle Raiane Silva Correa. -- Assis, 2024.

94p.

Trabalho de Conclusão de Curso (Graduação em Direito) -- Fundação Educacional do Município de Assis (FEMA), Instituto Municipal de Ensino Superior de Assis (IMESA), 2024.

Orientadora: Profa. Ma. Gisele Spera Máximo.

1. Proteção de dados pessoais. 2. Economia agrícola. 3. Aplicação da lei. I Máximo, Gisele Spera. II Título.

CDD 341.2738

**A PROTEÇÃO DE DADOS NA INDÚSTRIA DO AGRONEGÓCIO:  
DESAFIOS E PERSPECTIVAS NA APLICAÇÃO DA LGPD E NA ADOÇÃO DE  
TECNOLOGIAS AVANÇADAS**

**ISABELLE RAIANE SILVA CORREA**

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

**Orientadora:** GISELE SPERA MÁXIMO

**Examinador:** LUIZ ANTONIO RAMALHO ZANOTI

**Assis/SP  
2024**

# DEDICATÓRIA

Dedico este trabalho àquele que deu razão à minha existência. Autor da vida, definição de tudo, que se revela na realeza e na simplicidade, na tempestade e na calma. A Ele, que usou a coroa de espinhos, o Cordeiro de Deus e o rugido do Leão. Alfa e Ômega, princípio e fim de todas as coisas.

## **AGRADECIMENTOS**

Em primeiro lugar, expresso minha sincera gratidão a Deus pela oportunidade de realizar este trabalho, assim como pela saúde e sabedoria que me foram concedidas para enfrentar os desafios ao longo deste percurso.

Agradeço profundamente aos meus pais, Simone dos Santos Silva e Carlos Alberto Assunção Correa, que têm sido pilares fundamentais em minha vida. Seu amor incondicional, apoio constante e incentivo foram essenciais para a realização desta jornada acadêmica.

Sou igualmente grata aos meus irmãos Mayara e Lucas pela presença constante e apoio inestimável. Um agradecimento especial ao meu namorado, Allan Antonucci Duarte, cujo companheirismo, carinho, assistência e apoio foram cruciais para superar os desafios e alcançar este objetivo.

Minhas mais sinceras palavras de agradecimento vão à minha orientadora, Gisele Spera Máximo, por sua dedicação exemplar, profissionalismo e orientação ao longo deste trabalho.

Agradeço também aos amigos que estiveram ao meu lado, com um reconhecimento especial a Gabriela, pois sua parceria foi valiosa e essencial ao compartilhar desafios e conquistas vividos neste período. Sou grata ainda a Sandy, Beatriz e Mariana pela amizade, alegrias e companheirismo.

## RESUMO

A Lei Geral de Proteção de Dados (LGPD) introduziu um novo paradigma no cenário jurídico brasileiro, demandando das organizações uma profunda revisão de suas práticas de tratamento de dados pessoais. O agronegócio, setor estratégico para a economia nacional, não está imune a essa transformação. Este estudo analisa os desafios e oportunidades da aplicação da LGPD nesse contexto, considerando a complexidade da cadeia produtiva e a crescente digitalização do setor.

O presente estudo evidencia que a LGPD, inspirada no Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, estabelece um conjunto de princípios e garantias aos titulares de dados, exigindo das empresas a adoção de medidas técnicas e administrativas para proteger as informações coletadas. No entanto, a implementação da LGPD no agronegócio enfrenta desafios específicos, como a resistência à mudança de atores mais tradicionais, a necessidade de conciliar a proteção de dados com as dinâmicas do ambiente rural e a complexidade das operações agrícolas.

A digitalização do agronegócio, impulsionada por tecnologias como a agricultura de precisão e a inteligência artificial, gera grandes volumes de dados, intensificando a necessidade de conformidade com a LGPD. A coleta, o armazenamento e a utilização desses dados devem ser realizados de forma transparente e segura, respeitando os direitos dos titulares.

A implementação da LGPD no setor agropecuário é cada vez mais necessária, mas enfrenta desafios significativos. Estes desafios incluem a resistência à mudança de gerações habituadas a práticas menos regulamentadas, a adaptação às novas tecnologias e a complexidade inerente ao setor. Portanto, para garantir a conformidade com a LGPD e promover a proteção adequada dos dados pessoais, é essencial que o setor agropecuário adote práticas robustas de gestão e proteção de dados, além de investir em capacitação e conscientização contínuas.

**Palavras-chave:** Lei Geral de Proteção de Dados, LGPD, setor agropecuário, digitalização, proteção de dados, desafios regulatórios, conformidade e tecnologia.

## ABSTRACT

The General Data Protection Law (LGPD) has introduced a new paradigm in Brazil, demanding that organizations overhaul their data handling practices. The agribusiness sector, crucial to Brazil's economy, is no exception. This study examines the challenges and opportunities of implementing the LGPD within this context, given the sector's complex supply chain and increasing digitalization.

Inspired by the EU's GDPR, the LGPD establishes principles and guarantees for individuals whose data is processed. It requires businesses to implement technical and administrative safeguards. However, applying the LGPD to agribusiness is fraught with unique challenges: resistance to change among traditional players, balancing data protection with rural realities, and the complexity of agricultural operations.

The digitalization of agribusiness, propelled by technologies like precision agriculture and AI, generates vast amounts of data, heightening the need for LGPD compliance. Data collection, storage, and use must be transparent and secure, respecting individuals' rights.

Implementing the LGPD in agriculture is essential but faces hurdles. These include generational resistance to regulation, adapting to new technologies, and the sector's inherent complexity. To ensure compliance and robust data protection, agribusiness must adopt strong data management practices and invest in ongoing training and awareness.

**Keywords:** General Data Protection Law, LGPD, agricultural sector, agribusiness, digitalization, data protection, regulatory challenges, compliance, technology.

## LISTA DE ILUSTRAÇÕES

<b>Figura 1:</b> Ranking mundial em 2020 de produção e exportações brasileiras ..	17
<b>Figura 2:</b> Fases da Agricultura .....	27
<b>Figura 3:</b> Linha do tempo da LGPD .....	34

## LISTA DE TABELAS

**Tabela 1:**Bases Legais Para O Tratamento De Dados Pessoais Na LGPD .... 63

**Tabela 2:** Direitos dos Titulares de Dados Pessoais ..... 67

## LISTA DE ABREVIATURAS

§ - Parágrafo

ANPD - Autoridade Nacional de Proteção de Dados

Art. – Artigo

CNA - Confederação da Agricultura e Pecuária do Brasil

CEPEA: Centro de Estudos Avançados em Economia Aplicada

FTC - Faculdade de Tecnologia e Ciências

GDPR - General Data Protection Regulation

IA - Inteligência Artificial

IoT - Internet das Coisas

LGPD - Lei Geral de Proteção de Dados

MAPA - Ministério da Agricultura, Pecuária e Abastecimento

ML - Machine Learning (Aprendizado de Máquina)

PNAD - Pesquisa Nacional por Amostra de Domicílios

# SUMÁRIO

INTRODUÇÃO.....	14
<b>1. TRANSFORMAÇÕES E SUSTENTABILIDADE NA AGRICULTURA BRASILEIRA .....</b>	<b>16</b>
1.1. A CONTRIBUIÇÃO DA AGROPECUÁRIA AO PIB E À ECONOMIA NACIONAL .....	16
1.2. A RELEVÂNCIA SOCIAL DA AGROPECUÁRIA .....	17
1.3. A ORIGEM E EXPANSÃO DO CONCEITO DE AGRIBUSINESS.....	18
1.4. A CONSOLIDAÇÃO DO CONCEITO AGRONEGÓCIO NO BRASIL..	20
1.5. A MODERNIZAÇÃO DA AGRICULTURA E SUAS FASES.....	21
1.5.1. <b>A Agricultura Pré-Histórica e as Primeiras Transformações ..</b>	<b>21</b>
1.5.2. <b>A Revolução da Agricultura 1.0 a 2.0.....</b>	<b>22</b>
1.5.3. <b>A Fase 3.0 da Agricultura - Agricultura de Precisão .....</b>	<b>24</b>
1.5.4. <b>A Transição para a Fase 4.0 - Agricultura Digital .....</b>	<b>25</b>
1.5.5. <b>Rumo a Agricultura 5.0 .....</b>	<b>26</b>
<b>2. LGPD: UMA ANÁLISE NORMATIVA ABRANGENTE DE PRINCÍPIOS, ESTRUTURA E CONCEITOS .....</b>	<b>30</b>
2.1. SURGIMENTO DA LGPD .....	32
2.2. PRINCÍPIOS DA LGPD.....	37
2.2.1. <b>Princípio da Boa-fé.....</b>	<b>39</b>
2.2.2. <b>Princípio da Finalidade .....</b>	<b>40</b>
2.2.3. <b>Princípio da Adequação .....</b>	<b>41</b>
2.2.4. <b>Princípio da Necessidade .....</b>	<b>43</b>
2.2.5. <b>Princípio do Livre Acesso.....</b>	<b>43</b>
2.2.6. <b>Princípio da Qualidade de Dados .....</b>	<b>44</b>
2.2.7. <b>Princípio da Transparência .....</b>	<b>45</b>
2.2.8. <b>Princípios da Segurança e da Prevenção.....</b>	<b>47</b>
2.2.9. <b>Princípio da Não Discriminação .....</b>	<b>49</b>
2.2.10. <b>Princípio da Responsabilização e Prestação de Contas .....</b>	<b>51</b>
2.3. ESTRUTURA E APLICABILIDADE NORMATIVA.....	52
2.4. CONCEITOS DA LGPD .....	54

2.4.1. Agentes de Tratamento .....	56
2.4.2. Tratamento de Dados Pessoais e Bases Legais .....	58
2.4.3. Direitos dos Titulares .....	63
<b>3. PROTEÇÃO DE DADOS NO SETOR AGROPECUÁRIO: DESAFIOS E PERSPECTIVAS FUTURAS .....</b>	<b>68</b>
3.1. O BIG DATA .....	69
3.2. PERCEPÇÕES DO SETOR AGROPECUÁRIO EM RELAÇÃO À LGPD: DESAFIOS E PERSPECTIVAS GERACIONAIS.....	71
3.3. PROTEÇÃO DE DADOS AGRÍCOLAS .....	74
3.4. INCIDENTES E MEDIDAS DE SEGURANÇA .....	76
3.5. ANPD FISCALIZAÇÃO E APLICAÇÃO DE SANÇÕES.....	77
3.6. DESAFIOS E APLICAÇÃO DA LGPD NO SETOR AGROPECUÁRIO	80
<b>CONCLUSÃO .....</b>	<b>86</b>
<b>BIBLIOGRAFIA .....</b>	<b>88</b>

## INTRODUÇÃO

A proteção de dados pessoais tornou-se um tema central em diversas indústrias ao redor do mundo, impulsionada pelo advento de tecnologias avançadas e pela crescente digitalização dos processos produtivos. No Brasil, a Lei Geral de Proteção de Dados (LGPD) estabelece um marco regulatório para o tratamento de dados pessoais, impondo diretrizes que impactam significativamente todos os setores econômicos, incluindo o agronegócio. Este setor, de grande relevância para a economia nacional devido à sua contribuição substancial para o Produto Interno Bruto (PIB) e sua capacidade de geração de empregos, enfrenta desafios únicos na implementação das normas de proteção de dados.

A modernização da agricultura brasileira, marcada por sucessivas revoluções tecnológicas desde a era pré-histórica até a atualidade, resultou em um aumento exponencial na geração e no tratamento de dados. A evolução das práticas agrícolas, desde a agricultura tradicional até as fases contemporâneas de agricultura de precisão e digital, trouxe consigo a necessidade de um manejo eficiente e seguro das informações coletadas. Este cenário exige que os agentes envolvidos no setor agropecuário compreendam e adotem medidas rigorosas para garantir a conformidade com a LGPD, ao mesmo tempo em que exploram o potencial das tecnologias emergentes.

Neste contexto, o presente estudo busca analisar os desafios e as perspectivas da aplicação da LGPD na indústria do agronegócio, com um enfoque particular na adoção de tecnologias avançadas. Será investigado como a coleta, o armazenamento e o uso de dados podem ser otimizados para garantir a proteção dos dados pessoais, respeitando os princípios fundamentais da legislação. A análise inclui uma revisão das transformações históricas na agricultura brasileira, a relevância socioeconômica do agronegócio e a adaptação das práticas de proteção de dados às novas realidades tecnológicas.

Além disso, o estudo abordará a importância da conscientização e da educação dos agentes do setor sobre as normas de proteção de dados, considerando as peculiaridades culturais e geracionais que influenciam a aceitação e a implementação das novas práticas. Serão discutidas também as responsabilidades e os desafios enfrentados pelos pequenos e médios produtores, que muitas vezes carecem de recursos e conhecimento técnico para

atender às exigências da LGPD. Por fim, a pesquisa pretende oferecer recomendações práticas para fortalecer a cadeia produtiva do agronegócio por meio da adequada gestão de dados, promovendo uma cultura de privacidade e segurança que beneficie todas as partes envolvidas

# 1. TRANSFORMAÇÕES E SUSTENTABILIDADE NA AGRICULTURA BRASILEIRA

## 1.1. A CONTRIBUIÇÃO DA AGROPECUÁRIA AO PIB E À ECONOMIA NACIONAL

O Brasil atualmente ocupa uma posição proeminente no cenário global em relação à produção agropecuária, destaque este, que se deve a investimentos substanciais em pesquisas e tecnologias nesse setor, além de sua vantajosa localização geográfica propícia para atividades agrícolas. No ano de 2023, o referido setor registrou seu desempenho mais expressivo em 28 anos, evidenciando um crescimento de 18,1% no Produto Interno Bruto (PIB) ao longo do ano, em comparação com o mesmo período do ano anterior, conforme dados fornecidos pela Confederação da Agricultura e Pecuária do Brasil (CNA). Esse notável avanço impulsionou o PIB brasileiro, resultando em um crescimento de 3,2%, considerando a mesma base de comparação.

Em uma hipótese em que a agropecuária não tivesse experimentado esse marcante crescimento em 2023, o crescimento econômico do Brasil teria se limitado a 1,7%. Dessa maneira, o setor foi responsável por aproximadamente 47,5% da taxa de crescimento do PIB no referido ano no país. Atualmente, a participação desse setor representa 8,11% do PIB total.

Ao longo das últimas quatro décadas, a produção agropecuária brasileira tem se desenvolvido de maneira notável, posicionando o país como um dos principais fornecedores de alimentos para o futuro. Em 2020, o faturamento proveniente de bens e serviços gerados no agronegócio alcançou a expressiva cifra de R\$ 1,98 trilhão. Desse montante, a agricultura contribuiu com R\$ 1,38 trilhão, enquanto a pecuária gerou R\$ 602,3 bilhões. Este desempenho robusto reforça a relevância crescente do setor na economia nacional e global.

Na contemporaneidade, o Brasil detém a posição de quarto maior exportador global de produtos agropecuários, alcançando aproximadamente USD 100,7 bilhões, ficando atrás somente da União Europeia, Estados Unidos e China. Destaca-se que o país lidera não apenas em volume de produção, mas também em exportação de commodities agrícolas essenciais, como por exemplo: soja, café, suco de laranja e açúcar.

Ademais, a proeminência do Brasil no cenário global é ainda mais evidente ao observarmos sua posição, como o segundo maior produtor e exportador de carne bovina e figura como o terceiro maior produtor e exportador de carne de frango. No cenário da carne suína, o país assume a posição de quarto maior exportador global. Tais indicadores evidenciam a importância do país no comércio internacional de produtos agropecuários, consolidando sua posição como um ator significativo nos mercados globais de alimentos e commodities.



**Figura 1:** Ranking mundial em 2020 de produção e exportações brasileiras (ASBRAAP, BRASSCOM, MAPA, 2020)

## 1.2. A RELEVÂNCIA SOCIAL DA AGROPECUÁRIA

Demonstrou-se de forma incontestável que o setor agrícola detém uma influência crucial na economia. Além de ser um dos principais motores na geração de riquezas, destaca-se também como uma fonte significativa de geração de empregos, absorvendo aproximadamente 1 de cada 3 trabalhadores brasileiros.

Segundo os dados obtidos na Pesquisa Nacional por Amostra de Domicílios (PNAD) de 2015, o setor agrícola empregava 32,3% dos trabalhadores brasileiros naquele ano. Isso representa um total de 30,5 milhões de pessoas, considerando um contingente total de 94,4 milhões de trabalhadores. Dentro desse contexto, foi observado que 42,7% estavam envolvidos em atividades agropecuárias, 21,1% no comércio agropecuário, 21% nos agrosserviços e 15,2% na agroindústria. Esses números revelam a diversificação de áreas de atuação dentro do setor agrícola.

O crescimento do Produto Interno Bruto (PIB) do setor agrícola não apenas reflete a expansão econômica, mas também se traduz na ampliação das demandas por serviços correlatos. O aumento na produção, impulsiona a necessidade de serviços como armazenagem, transporte, comércio, incluindo serviços financeiros, contábeis, jurídicos e diversos outros.

Dessa forma nota-se, o papel social relevante que o setor desempenha ao fornecer oportunidades de emprego para milhões de trabalhadores em diversas áreas, consolidando-se como um sustentáculo vital para a estabilidade e o crescimento social e econômico do país.

### 1.3. A ORIGEM E EXPANSÃO DO CONCEITO DE AGRIBUSINESS

Durante a década de 1950, nos Estados Unidos, os pesquisadores John Herbert Davis e Ray Allan Goldberg foram alocados na renomada instituição *Harvard Business School* pelas indústrias de alimentação, que tinham como propósito o aprofundamento de seus estudos sobre a otimização das crescentes interações do setor agropecuário. Neste contexto, conceberam o termo “*Agribusiness*”, segundo as palavras de Ray Goldberg em uma entrevista concedida em 16 de março de 2017, o objetivo era englobar em sua totalidade, “*the whole food system*”, em tradução literal, todo o sistema alimentar.

Agribusiness significa a soma de todas as operações da fazenda, mais a manufatura e a distribuição de todos os insumos de produção agrícola providos pelos negócios, mais o total das operações realizadas em conexão com a manipulação, estocagem, processamento e distribuição de commodities agrícolas. Em suma, agribusiness refere-se à soma total de todas as operações envolvidas na produção e distribuição de alimentos e fibras (DAVIS; 1955, p.5)

Ainda para compreensão, o conceito foi descrito também por Massilon (1999, apud RUFINO), como:

O conjunto de todas as operações e transações envolvidas desde a fabricação dos insumos agropecuários, das operações de produção nas unidades agropecuárias, até o processamento e distribuição e consumo dos produtos agropecuários 'in natura' ou industrializados.

Em suma, o conceito de agronegócio, conforme descrito por Davis e Goldberg (1957), refere-se ao desenvolvimento abrangente da agropecuária integralmente, que desencadeia uma reação setorial em cada cadeia produtiva. Isso envolve uma variedade de atores, incluindo fornecedores de insumos, prestadores de serviços, indústrias transformadoras de alimentos, fibras e energia, sistemas de armazenagem e transporte, marketing, distribuição e escoamento produtivo.

Segundo Batalha (2014), mesmo que a teoria dos sistemas <sup>1</sup> não seja explicitamente mencionada nos primeiros trabalhos de Davis e Goldberg (1957), ela pode ser claramente inferida a partir da própria definição abrangente de agronegócio, como um conjunto de atividades que funcionam de maneira integrada. Essa visão holística do agronegócio promove uma compreensão mais profundada das complexas relações entre os diferentes segmentos da cadeia produtiva de alimentos, fomentando uma abordagem interdisciplinar na pesquisa e administração do setor agropecuário.

O termo rapidamente se espalhou e muitos países começaram a utilizar. No Brasil um pouco mais tardar, esse novo olhar para “agricultura” começou a se difundir em meados de 1980, atravessando toda essa década ainda em inglês de forma generalizada. Somente na segunda metade da década de 1990, o termo agronegócios começa de fato ser aceito e adotado pela mídia, resultando inclusive na elaboração de cursos superiores de agronegócios, até em um nível de graduação universitária.

Na Bahia, a primeira proposta concreta de inserção do agronegócio no meio acadêmico surgiu na UNYAHNA, em 1997, seguida pela Faculdade de Tecnologia e Ciências (FTC) em 1999. A FTC fez avanços significativos, estabelecendo cursos de administração com habilitação em agronegócios em seis cidades diferentes. Em 2000, a instituição desenvolveu o Núcleo de Estudos Avançados em Agronegócios, cujo objetivo era aprimorar a integração entre o meio acadêmico e o setor empresarial.

---

<sup>1</sup> Os sistemas de produção consistem na aplicação conjunta de um grupo de conhecimentos interrelacionados, para obtenção de um determinado produto. Extraído de Gastal, Edmundo, "O Enfoque de Sistemas na Programação da Pesquisa Agropecuária". Dissertação ao Concurso de Livre Docência em Administração Rural da Faculdade de Agronomia "Eliseu Maciel " da Universidade Federal de Pelotas.

#### 1.4. A CONSOLIDAÇÃO DO CONCEITO AGRONEGÓCIO NO BRASIL

O conceito de agronegócios teve seus primeiros grandes focos em São Paulo e no Rio Grande do Sul, onde foram criados projetos fundamentados na obra de Davis e Goldberg (1957). Esses projetos centralizavam a ideia de integrar a agropecuária com outros setores da economia, afastando-se da visão compartimentada e isolada tradicionalmente adotada. Esse tema foi aprofundado na obra "Complexo Agroindustrial: o Agribusiness Brasileiro", publicada em 1990 pelo engenheiro agrônomo Ney Bittencourt de Araújo e outros autores, a primeira publicação que abordava essa integração de forma abrangente no Brasil.

Ainda neste cenário, surge a criação da Associação Brasileira de Agribusiness (Abag) em 1993, na qual sempre se utilizara da característica totalizadora do termo Agribusiness para fundamentar seus projetos de fato. Em 2000, a associação contratou pesquisadores de órgãos públicos para calcular o Produto Interno Bruto (PIB) do agronegócio, baseando-se na metodologia da pesquisa nos estudos de Davis e Goldberg em 1957.

Atualmente, o Centro de Estudos Avançados em Economia Aplicada (CEPEA), vinculado à Escola Superior de Agricultura "Luiz de Queiroz" da Universidade de São Paulo, destaca-se como o principal órgão de pesquisa quantitativa sobre o agronegócio no Brasil. O conceito abrangente de agronegócio introduzido por Davis e Goldberg em seus estudos serve como base para o cálculo do Produto Interno Bruto (PIB) do agronegócio, realizado pelo CEPEA. Esse cálculo abrange a soma de cada segmento do agronegócio, incluindo insumos, agropecuária, agroindústria e agro serviços, com o objetivo de avaliar o impacto do setor no bem-estar da sociedade.

<sup>2</sup> O coordenador do CEPEA, Geraldo Sant'Ana de Camargo Barros, enfatizou a utilização desses estudos na metodologia de quantificação do agronegócio, que considera não apenas o volume de produção, mas também o uso de tecnologia e a renda gerada em todas as etapas da cadeia produtiva:

---

<sup>2</sup> Informação verbal de Geraldo Sant'Ana de Camargo Barros, coordenador do Centro de Estudos Avançados em Economia Aplicada (entrevista em 13/06/2017).

Renda gerada de forma sistêmica na produção de insumos para a agropecuária, acrescida da renda gerada na produção primária e se estendendo por todas as demais atividades que processam e distribuem o produto ao destino final.

## 1.5. A MODERNIZAÇÃO DA AGRICULTURA E SUAS FASES

A modernização da agricultura representa um dos marcos mais significativos na evolução das práticas agrícolas ao longo da história. Este processo, que pode ser compreendido em diversas fases distintas, abrange desde a mecanização inicial e a introdução de tecnologias avançadas, até a atual era da agricultura digital e sustentável. Cada fase trouxe consigo mudanças profundas não apenas na maneira como os alimentos são produzidos, mas também na estrutura socioeconômica das áreas rurais e no próprio papel do agricultor.

Essas transformações não ocorreram de maneira uniforme, variando de acordo com as particularidades regionais e os diferentes níveis de acesso à tecnologia. Contudo, o resultado geral tem sido um setor agrícola cada vez mais eficiente, sustentável e capaz de atender à crescente demanda global por alimentos. Este contexto de modernização contínua e suas diversas fases será explorado, destacando, os principais avanços e seus impactos na agricultura contemporânea.

### 1.5.1. A Agricultura Pré-Histórica e as Primeiras Transformações

Durante o período Paleolítico, aproximadamente entre 250 mil anos atrás e 40.000 a.C., os Neandertais dependiam fortemente da coleta de frutas e raízes, bem como do consumo de carne de caça e peixes para sua subsistência. Devido à necessidade de buscar novas fontes de alimento, os Neandertais adotavam um estilo de vida nômade, deslocando-se constantemente conforme a disponibilidade de recursos naturais em diferentes regiões. Esse comportamento migratório era essencial para sua sobrevivência, uma vez que permaneciam em um local apenas enquanto este oferecesse suprimentos adequados para sua alimentação. Quando os recursos começavam a escassear, eles se moviam para novas áreas que pudessem fornecer as necessidades nutricionais necessárias.

Com o advento do período Neolítico, a última fase da pré-história, aproximadamente 10 mil anos atrás, ocorreu uma transformação significativa na história humana, marcada pelo surgimento da agricultura. Este desenvolvimento teve um impacto profundo na alimentação, cultura e organização das sociedades humanas, com efeitos que perduram até os dias atuais. Cansados da constante necessidade de deslocamento e da dependência das fontes alimentares disponíveis, os seres humanos começaram a estabelecer-se em locais fixos, inaugurando o período de sedentarização.

A fixação em residências permanentes, especialmente próximas a rios e lagos, permitiu aos seres humanos sobreviverem cultivando seus próprios alimentos. Eles começaram a plantar trigo, cevada, milho, arroz e outros cereais, que se tornaram a base da alimentação tradicional de diversas culturas até hoje. Além disso, o Neolítico viu o início da domesticação de animais, como bovinos, ovinos, caprinos e suínos, complementando a dieta e fornecendo recursos adicionais como leite, lã e carne, e a utilização dos mesmos, para transportes na agricultura.

Essas mudanças possibilitaram o surgimento de grandes agrupamentos humanos com o objetivo principal de produzir alimentos para a sobrevivência. A transição para a agricultura e a domesticação de animais não apenas melhorou a segurança alimentar, mas também promoveu o desenvolvimento de estruturas sociais mais complexas e a especialização do trabalho.

### **1.5.2. A Revolução da Agricultura 1.0 a 2.0**

A partir disso, inicia-se a evolução da agricultura ao longo do tempo, que é marcada e classificada por distintas fases, cada uma caracterizada pelo surgimento e adoção de novas tecnologias e práticas. Agricultura 1.0, consiste na agricultura tradicional de fato. No início do século XX, essa modalidade experimentou uma redução significativa em sua relevância, embora ainda seja praticada em diversas propriedades rurais. Ela se fundamenta no sistema de subsistência, comumente associado ao trabalho manual e à utilização de tecnologias rudimentares, como por exemplo a tração animal.

Ao considerarmos que, no passado, o tamanho da população permaneceu baixo, com menos de um milhão de pessoas até o início da revolução agrícola, observa-

se que a população demorou aproximadamente 1.500 anos para duplicar de tamanho. Devido a esse crescimento relativamente lento, era possível manter estabilidade e qualidade de vida utilizando métodos rudimentares de subsistência.

No entanto, as projeções da Divisão de População da ONU<sup>3</sup>, indicam que a população mundial poderá ultrapassar 11 bilhões de habitantes até 2100. Com o planeta já tendo superado sua capacidade de carga, torna-se evidente que os métodos rudimentares da fase inicial da agricultura não são mais suficientes para atender às necessidades globais. Atualmente, frente ao aumento acelerado da população global e às mudanças climáticas, a agricultura enfrenta o desafio crítico de assegurar a segurança alimentar de maneira sustentável.

De acordo com o Ministério da Agricultura, Pecuária e Abastecimento (MAPA, 2021), a resposta para o futuro reside na inovação, particularmente na inovação agrícola que combina tecnologias biológicas e digitais, é imperativo otimizar o uso do tempo e dos recursos através de um planejamento adequado e novas tecnologias, considerando que já enfrentamos desafios significativos para garantir a segurança alimentar e a preservação da biodiversidade.

Em 1950, inicia-se a fase conhecida como Agricultura 2.0, também conhecida pela Revolução Verde, teve como principal marco a introdução de máquinas movidas a motores de combustão interna. Este período foi caracterizado pela substituição dos animais de tração por equipamentos mecanizados, surge neste período os primeiros tratores, o que permitiu um aumento significativo na escala de produção agrícola, dessa forma a agricultura é direcionada para um comportamento mais industrializado, como uma cadeia produtiva, mais organizada.

A Agricultura 2.0 facilitou o cultivo de áreas maiores com menos mão de obra, promovendo a expansão das fronteiras agrícolas e a produção em larga escala. Isso também impulsionou a comercialização de insumos e produtos agrícolas em nível global. Avanços em diversas áreas, como genética, biotecnologia e química, resultaram no desenvolvimento de sementes de alta produtividade e resistência a pragas. A introdução de novas variedades de plantas, fertilizantes

---

<sup>3</sup> UN/ESA, Population Division. World Population Prospects: The 2015 Revision

sintéticos, pesticidas e práticas de irrigação eficientes revolucionou a produção agrícola, permitindo colheitas mais abundantes e de maior qualidade.

No entanto, essa fase trouxe consigo desafios ambientais significativos. O uso intensivo de fertilizantes e pesticidas químicos levou à contaminação de solos e corpos d'água, além de causar resistência em pragas. A dependência de monoculturas reduziu a resiliência das lavouras a pragas e doenças, destacando novamente, a necessidade contínua de evolução tecnológica para mitigar esses problemas.

### **1.5.3. A Fase 3.0 da Agricultura - Agricultura de Precisão**

Entre meados da década de 1990 e 2010, desenvolveu-se a fase 3.0 da agricultura, caracterizada pelo surgimento da agricultura de precisão. Este período foi marcado pela introdução de sistemas de orientação baseados nos sinais do sistema de posicionamento global — GPS (Global Positioning System), que foram disponibilizados ao público. Tecnologias avançadas de georreferenciamento via satélite começaram a desempenhar um papel crucial, permitindo análises mais precisas das necessidades específicas de cada área de cultivo em termos de adubação e irrigação.

A fase 3.0 viu um aumento significativo na aplicação da agricultura de precisão em diversas áreas de produção. Paralelamente, houve um incremento nos estudos complementares voltados para aprimorar a precisão e a eficiência dos tratamentos culturais. Com o avanço contínuo das tecnologias digitais, a agricultura de precisão incorporou novas ferramentas e abordagens, como sistemas baseados em nuvem, aplicativos móveis, grandes conjuntos de dados, dispositivos conectados à internet e drones.

Essas tecnologias têm sido amplamente aplicadas em várias áreas da produção agrícola, desde o monitoramento detalhado de variáveis climáticas até a otimização das operações com máquinas agrícolas. Além disso, influenciam aspectos logísticos e comerciais das safras, promovendo uma gestão mais eficiente e integrada das atividades agrícolas.

#### **1.5.4. A Transição para a Fase 4.0 - Agricultura Digital**

A era da Agricultura Digital desponta como um novo paradigma em todas as fases da cadeia produtiva, impulsionada pela integração de tecnologias inovadoras que redefinem a forma como cultivamos e gerenciamos os recursos naturais. A partir de 2010, emergiu a fase 4.0 caracterizada pela convergência de ferramentas digitais avançadas, como Internet das Coisas (IoT), Big Data, inteligência artificial (IA), aprendizado de máquina (ML), impressão 3D, robótica, sensores, e diversas outras inovações (Klerkx et al., 2019).

Nesta etapa, destacam-se inovações amplamente adotadas no setor, como maquinários agrícolas autônomos, veículos automatizados, animais equipados com sensores e drones. Esses dispositivos estão conectados a uma central de processamento de dados, permitindo a coleta e análise em tempo real de uma vasta quantidade de informações relacionadas às atividades agrícolas.

No contexto da agricultura digital, a fase de coleta e gerenciamento de dados utiliza tecnologias como agricultura de precisão, internet das coisas e telemática, seguida pelo armazenamento em nuvem. Essa centralização dos dados exige uma capacidade analítica avançada, empregando inteligência artificial para processar grandes volumes de informações. Essa abordagem facilita a tomada de decisões na administração das propriedades agrícolas e na gestão da produção, além de impulsionar a operação de máquinas autônomas no campo (Saiz-Rubio; Rovira-Más, 2020).

A agricultura 4.0 possibilita que os agricultores tomem decisões de maneira mais eficiente e precisa, promovendo o surgimento da Agricultura Inteligente, também conhecida como "Smart Agriculture". Essa abordagem oferece insights aprimorados aos produtores, com recomendações específicas sobre manejo da lavoura, desempenho de máquinas, controle de pragas e doenças, entre outras áreas (ALCANTARA et al., 2021).

Os resultados dessa transformação digital são evidentes: aumento da produtividade, redução de custos e mão de obra, mitigação do impacto ambiental e, acima de tudo, a construção de um futuro mais sustentável para o agronegócio (Wolfert et al., 2014). A Agricultura 4.0 não se resume apenas à adoção de novas tecnologias, mas sim à transformação da cultura organizacional e da visão de negócio, impulsionando a transformação e a competitividade do setor.

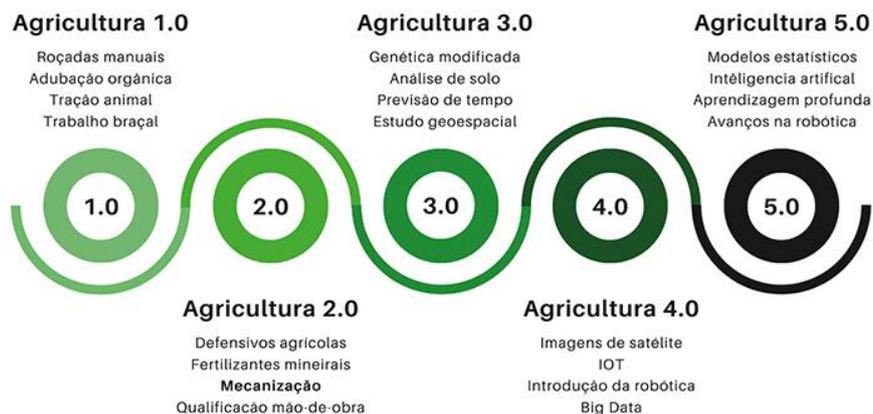
### **1.5.5. Rumo a Agricultura 5.0**

No horizonte da inovação agrícola, desponta a Agricultura 5.0, uma etapa crucial na jornada rumo à sustentabilidade e à inteligência. Essa fase crucial da jornada se caracteriza pela convergência de tecnologias digitais avançadas, como uso extensivo de inteligência artificial e robôs autônomos, que redefinem a forma como cultivamos e gerenciamos os recursos naturais.

No cerne da Agricultura 5.0 reside a fusão da gestão ciberfísica de fazendas com tecnologias de informação e comunicação (Wolfert, 2017). Essa convergência abre caminho para uma Agricultura Inteligente, onde a coleta e análise de dados em tempo real, via IoT, alimentam sistemas de IA que otimizam a tomada de decisões, automatizam tarefas e elevam a produtividade a novos patamares.

A proximidade entre sensores e alvos, reduzida para menos de dois metros, garante a captura de dados precisos sobre a intensidade da luz, a umidade do solo, das plantas e da atmosfera, e a severidade de doenças, permitindo uma atuação precisa e direcionada em cada planta ou animal (Saiz-Rubio; Rovira-Más, 2020). Além de otimizar a aplicação de insumos e melhorar a saúde das culturas, a agricultura 5.0 visa promover a produção de mais alimentos em menor área e com menos recursos, abordando também os aspectos sociais e políticos dos sistemas agrícolas.

A incorporação dessas tecnologias avançadas facilita a tomada de decisões complexas e precisas, possibilitando a transição da agricultura de precisão para a agricultura de decisão (Saiz-Rubio; Rovira-Más, 2020). No Brasil, a incorporação de processos de automação e a utilização de máquinas inteligentes guiadas por GPS já demonstram o alinhamento do país com essa transformação, evidenciando ganhos em produtividade, sustentabilidade e competitividade no mercado global.



**Figura 2:** Fases da Agricultura<sup>4</sup>

À medida que exploramos as mudanças no contexto agrícola, desde a consolidação do conceito de agronegócio até a emergência da agricultura de precisão, torna-se evidente a progressão contínua em direção a métodos mais avançados e eficientes. A introdução da agricultura de precisão representa uma transição crucial no setor agrícola, constituindo-se como uma evolução do paradigma do agronegócio, e significando um avanço substancial na gestão dos processos agrícolas. Esta abordagem não apenas se alinha com a perspectiva mais ampla de integração e interdependência entre os diversos segmentos da cadeia produtiva, mas também promove uma gestão mais precisa e estratégica dos recursos agrícolas.

Portanto, o conceito delineado por Davis e Goldberg não apenas estabelece uma base teórica fundamental para a compreensão da consolidação do agronegócio como um campo de estudo e prática, mas também proporciona uma abordagem interdisciplinar indispensável para elucidar a evolução da agricultura de precisão. Essa perspectiva abrangente reconhece a influência significativa de variáveis como tecnologia, logística, dinâmicas de mercado e sustentabilidade na configuração da produção agrícola contemporânea.

É verdade que a tecnologia como já pontuado, desempenha um papel central no desenvolvimento e na sustentabilidade do setor, impulsionando avanços

<sup>4</sup> Fonte: REVISTA Cultivar. In: **Como avança o processo de modernização da agricultura** s&a. [S. l.], 2019. Disponível em: <https://revistacultivar.com.br/noticias/como-avanca-o-processo-de-modernizacao-da-agricultura>. Acesso em: 14 jun. 2024.

essenciais em diversas áreas. No entanto, quanto mais desenvolvida a tecnologia, maior é o tráfego de dados. Exemplos desse fluxo incluem dados georreferenciados de propriedades agrícolas, que podem identificar os proprietários, e informações detalhadas sobre o uso de sua terra, produtividade, condições climáticas e monitoramento de pragas.

Outros exemplos, consistem em sensores instalados em campos que podem coletar dados em tempo real sobre a umidade do solo, o que permite a irrigação precisa, economizando água e melhorando o crescimento das plantas. Drones equipados com câmeras de alta resolução que podem monitorar a saúde das lavouras, identificar áreas que necessitam de atenção e aplicar insumos de maneira mais eficiente. Sistemas de GPS que permitem o mapeamento detalhado das propriedades, facilitando a aplicação localizada de fertilizantes e pesticidas, minimizando o impacto ambiental. Estes dados são vitais para a tomada de decisões informadas, permitindo aos agricultores otimizar o uso de recursos, reduzir desperdícios, agir de forma preventiva e aumentar a produtividade.

No entanto, a coleta e o armazenamento de grandes volumes de dados agrícolas levantam preocupações significativas sobre a privacidade e a segurança da informação. A proteção desses dados é essencial para garantir a confiança dos agricultores e a integridade de suas operações agrícolas. Sem medidas adequadas de segurança, os dados podem estar vulneráveis a acessos não autorizados, roubo, sequestro e manipulação. Além disso, a exposição de informações sensíveis pode levar a disputas legais e impactos econômicos negativos.

Para mitigar esses riscos, é fundamental implementar políticas robustas de segurança de dados que incluam criptografia, controle de acessos rigoroso e monitoramento contínuo de sistemas e estrutura. Além disso, é necessário a capacitação dos agricultores e demais atores do ramo sobre as melhores práticas de gestão de dados para garantir que eles compreendam a importância da proteção das informações e saibam como aplicar medidas de segurança eficazes.

Logo, a agricultura de precisão não apenas reflete um avanço tecnológico, mas também uma necessidade de integração de múltiplas disciplinas para promover

a sustentabilidade e a eficiência no setor agrícola. A aplicação de tecnologias avançadas, aliada à gestão estratégica de dados e à consideração de fatores ambientais e sociais, é fundamental para a evolução contínua do agronegócio e para a consolidação de práticas agrícolas mais responsáveis e eficazes.

## 2. LGPD: UMA ANÁLISE NORMATIVA ABRANGENTE DE PRINCÍPIOS, ESTRUTURA E CONCEITOS

A tecnologia está progressivamente predominante nos equipamentos de cenário agrícola, impulsionada pela constante inovação das empresas do setor. Embora os agricultores enfrentem dificuldades iniciais na adoção dessas novas tecnologias, há uma tendência crescente de incorporação desses avanços na prática agrícola. Essa adoção tem como consequência um aumento exponencial no volume de dados gerados. Com esse crescimento, a gestão e o tratamento desses dados estão sendo, em grande medida, delegados a terceiros.

Conforme a publicação da *The Economist* (2017), "*The world's most valuable resource is no longer oil, but data*" (O recurso mais valioso do mundo não é mais o petróleo, mas sim os dados). Esta afirmação enfatiza a preeminência dos dados na era digital contemporânea, destacando-os como o recurso mais valioso do século XXI. A transformação digital tem revolucionado diversos setores, e a agricultura não é exceção. Afinal, como afirmou Moran (2011), "*You can have data without information, but you cannot have information without data*" (Você pode ter dados sem informações, mas não pode ter informações sem dados).

A necessidade de proteger os dados pessoais não é um conceito novo. No entanto, o discurso em torno dessa questão se transformou significativamente ao longo do último século. inicialmente se fundamentava no direito à privacidade, um princípio essencial que assegura aos indivíduos o controle sobre suas informações pessoais e a liberdade de viver sem interferências indevidas. Contudo, com o início da era digital e a crescente coleta e utilização de dados pessoais, tornou-se evidente que o direito à privacidade, não era suficiente para garantir uma proteção abrangente dos dados. Nesse contexto, surgiram três abordagens distintas que contribuíram para a consolidação da proteção de dados na forma de um direito autônomo.

No primeiro entendimento ao final do século XIX, a proteção de dados passou a ser reconhecida como uma extensão do direito à privacidade. A seminal publicação de Samuel Warren e Louis Brandeis, "*The Right to Privacy*" (1890)<sup>5</sup>,

---

<sup>5</sup> No mês de dezembro de 1890, Samuel Warren e Louis Brandeis, ambos advogados, apresentaram na Harvard Law Review um artigo intitulado "The Right to Privacy". Nesse texto, eles defenderam que a evolução do direito à vida agora compreende o direito à privacidade, garantindo que o direito à liberdade abranja a proteção dos privilégios civis.

introduziu o conceito de "direito de estar só" como um componente essencial da liberdade individual. Este entendimento foi aprofundado após a Segunda Guerra Mundial, quando o uso abusivo de dados pessoais pelo regime nazista para segregar e exterminar grupos específicos,<sup>6</sup> destacou a importância de proteger a privacidade contra o arbítrio estatal. Este período foi marcado por avanços significativos, como a Declaração Universal dos Direitos Humanos de 1948 e a Lei Fundamental Alemã de 1949, que começaram a delinear as bases legais para a proteção da vida privada dos cidadãos.

No período de 1980, a proteção de dados começou a ser vista como um componente da dignidade da pessoa humana, especialmente no tocante ao direito comunitário europeu. O Tribunal Constitucional Federal Alemão, em sua decisão sobre a Lei do Censo de 1983, estabeleceu o princípio da autodeterminação informativa, afirmando que os indivíduos têm o direito de saber e decidir sobre o uso de seus dados pessoais. Este julgamento foi um marco que transformou a proteção de dados em um direito de personalidade<sup>7</sup>, limitando o poder do Estado e garantindo que cada pessoa tivesse controle sobre suas informações pessoais. Esta mudança refletiu um entendimento mais profundo da interconexão entre a proteção de dados e a dignidade humana.

Com o surgimento da 4ª Revolução Industrial e o rápido avanço das tecnologias de informação e comunicação, a proteção de dados passou a ser considerada um direito autônomo. O aumento exponencial no volume e na complexidade do compartilhamento de dados, impulsionado pelas redes sociais, aplicativos e assistentes virtuais, trouxe novos desafios e riscos para a privacidade dos indivíduos. Em resposta e diante desta nova era digital e do valor inestimável dos dados, as sociedades ao redor do mundo, com destaque para a brasileira e europeia, reconheceram a necessidade de criar leis específicas para promover medidas adequadas para a proteção desses dados.

A União Europeia implementou o Regulamento Geral sobre a Proteção de Dados (GDPR), que estabelece padrões elevados para a proteção de dados pessoais e impõe penalidades severas para o não cumprimento. Similarmente, no Brasil,

---

<sup>6</sup> SHARMA, Sanjay. *Data Privacy and GDPR Handbook*. New Jersey: Wiley, 2020. p. 25-26.

<sup>7</sup> LYNSKEY, Orla. *The Foundations of EU Data Protection Law*. Oxford: Oxford University Press, 2015. p. 81 e 95.

a Lei Geral de Proteção de Dados (LGPD) foi instituída para regular o tratamento de dados pessoais, impondo diretrizes sobre coleta, armazenamento, uso e compartilhamento de informações. Essas regulamentações tratam a proteção de dados como um direito autônomo, fundamental para garantir a privacidade e a segurança dos indivíduos no cenário digital atual.

É de extrema importância que os respectivos atores entendam e assimilem seus direitos e deveres legais, bem como a interconexão de suas ações. A falta de adequação e a incorreta aplicação da LGPD comprometem e fragilizam o setor agrário. Dados pessoais, como nome, endereço, número de telefone, histórico de saúde e financeiro, são informações sensíveis que, se não protegidas adequadamente, podem ser utilizadas para fins ilícitos, causando danos materiais e morais aos indivíduos. Violações de dados, como vazamentos e acessos não autorizados, podem levar a roubo de identidade, fraudes financeiras, discriminação e outros crimes.

A proteção eficaz dos dados pessoais tornou-se um critério essencial na escolha de parceiros de negócios. Empresas agora consideram a capacidade de seus parceiros em proteger os dados pessoais sob sua responsabilidade como um fator determinante para estabelecer ou manter relações comerciais. Esta nova exigência surge em resposta à necessidade de garantir que todas as partes envolvidas no tratamento de dados estejam em conformidade com as normas legais e possam assegurar a integridade e a segurança das informações.

## 2.1. SURGIMENTO DA LGPD

Antes da promulgação da LGPD, o tema da proteção de dados era abordado em dispositivos de leis esparsas, resultando na ausência de um complexo normativo unitário (MENDES, 2014). A constituição Federal de 1988, até o ano de 2022, não possuía qualquer dispositivo expresso que se pauta a proteção de dados, como um direito fundamental. Após a Emenda Constitucional nº 115 de fevereiro de 2022, isso mudou, assegurando no artigo LXXXIX, o direito a proteção dos dados pessoais, inclusive abrangendo também os meios digitais.

Entretanto, algumas legislações anteriores já abordavam este aspecto de proteção. Como por exemplo, a Lei nº 9.507/97 reguladora do habeas data, que permite o acesso da pessoa física ou jurídica as suas informações pessoais,

inclusive para corrigi-las. Outra situação, é o Código de Defesa do Consumidor (Lei nº 8.078/90) em seu artigo 43, que estabelece direitos e garantias aos consumidores em relação as suas informações pessoais compartilhadas em bancos e cadastros, assegurando seu acesso.

Seguindo pela Lei do Cadastro Positivo (Lei nº 12.414/2011) que regulamentou a formação e consultas aos bancos de dados, com informações de adimplemento, visando a formação de histórico de crédito. Em seguida vem a Lei de Acesso à informação (Lei 12.527/2011) que entra para regulamentar o direito constitucional, permitindo a solicitação das informações públicas sem necessidade de justificativas para o pedido.

Adiante temos o surgimento do Marco Civil da Internet (Lei 12.965/2014) estabelecendo princípios, garantias, direitos e deveres para provedores de serviços de internet, o objetivo da lei era regulamentar o uso da internet no Brasil, esta lei teve um impacto significativo na proteção dos direitos dos usuários, incluindo a privacidade, dessa forma, impondo deveres aos provedores e ao Poder Público. Essas legislações foram precursores importantes para a consolidação de um marco regulatório mais abrangente, culminando na LGPD, que unificou e ampliou a proteção dos dados pessoais no Brasil, alinhando o país às melhores práticas de proteção.

Com isso, somente em 14 de agosto de 2018, após um extenso período de debates, foi sancionada a Lei Geral de Proteção de Dados (LGPD) no Brasil, sob a designação de Lei nº 13.709/2018. Com a promulgação desta lei, o país se juntou ao grupo dos 100 países que possuem legislações específicas voltadas à proteção da privacidade e ao uso responsável dos dados pessoais. Embora a LGPD tenha sido sancionada em 2018, seus dispositivos somente passaram a vigorar e a produzir efeitos em 2020, após a publicação no Diário Oficial da União da Lei nº 14.058/2020, que derivou do Projeto de Lei de Conversão (PLV) nº 34/2020.

Para garantir a efetiva aplicação dessa lei, foi criada a Autoridade Nacional de Proteção de Dados (ANPD), constituída de fato em 2020, sendo um órgão público autônomo responsável por zelar pelo cumprimento da legislação e promover a cultura da proteção de dados no país. A ANPD atua em diversas frentes para garantir a efetividade da LGPD, como na normatização, ou seja,

criação de normas e diretrizes para o tratamento de dados pessoais, na fiscalização com o monitoramento do cumprimento da lei por empresas e órgãos públicos, na orientação, em esclarecimentos de dúvidas e fornecimento de informações sobre proteção de dados, na solução de conflitos entre titulares de dados e empresas e na cooperação internacional.

As sanções administrativas da LGPD entraram em vigor em agosto de 2021. Antes dessa data, diversas obrigações já estavam em vigor, exigindo que pessoas físicas e jurídicas alinhassem suas práticas aos princípios estabelecidos pela lei e respeitassem os direitos dos titulares de dados pessoais. A conformidade com a LGPD tornou-se crucial, uma vez que as empresas não aderentes à legislação enfrentavam sérios riscos reputacionais no mercado, muitas vezes mais danosos do que as próprias sanções legais.



**Figura 3:** Linha do tempo da LGPD

**Fonte:** ASBRAAP, BRASSCOM, MAPA, 2020.

O avanço tecnológico trouxe consigo uma série de novos desafios para os quais o Direito, muitas vezes, não dispõe de soluções imediatas. É, portanto, fundamental compreender o contexto contemporâneo em que vivemos e que motivou a criação dessa legislação, a qual tem causado um impacto significativo no campo jurídico. O conceito de “Sociedade da Informação”<sup>8</sup> ilustra de forma

<sup>8</sup> A sociedade da informação é um modelo em que a tecnologia e a informação são centrais para o desenvolvimento econômico, social e cultural, promovendo a integração global. WERTHEIN,

clara o paradigma tecnológico atual, intensificado pelo surgimento da internet, onde prevalece uma presunção de consentimento e uma confiança implícita no uso dos dados.

É bem verdade que o ambiente digital enfrenta diversos desafios neste sentido, entretanto segundo Fernanda Galera Soler, o ambiente digital:

Tampouco, trata -se de um local sem leis ou a margem da justiça, mas sim um local em que toda a legislação é aplicável, porém, com a devida adaptação ao ecossistema do caso posto, permitindo “inovações jurídicas”, as quais são incorporadas ao seu tempo pelo Direito, em especial o positivado.

A criação da Lei Geral de Proteção de Dados (LGPD) no Brasil foi fortemente motivada pela implementação da General Data Protection Regulation (GDPR) na União Europeia. A GDPR, que entrou em vigor em 25 de maio de 2018, substituiu a diretiva 95/46/CE de 1995, estabelecendo novos padrões rigorosos para a proteção de dados pessoais na Europa. Essa legislação europeia serviu de inspiração e modelo para a elaboração da Lei nº 13.709/2018, conhecida como LGPD, no Brasil (MENDES; DONEDA, 2018).

A criação da LGPD, está inserida em um contexto mais amplo de regulamentação da privacidade e proteção de dados na América do Sul. Diversos países da região já haviam implementado suas próprias legislações sobre o tema, estabelecendo precedentes importantes para a proteção dos dados pessoais.

A Argentina, por exemplo, foi pioneira com a *Ley de Protección de los Datos Personales* em 2000, estabelecendo um marco abrangente para a proteção de dados pessoais. O Chile, com a *Ley de Protección de Datos de Carácter Personal* de 1999, também garantiu direitos fundamentais como acesso, correção, suspensão temporária e exclusão de dados. A Colômbia promulgou a *Ley de Protección de Datos Personales* em 2012, introduzindo princípios como legalidade e transparência, e criando a Superintendência de Indústria e Comércio como órgão de fiscalização. O Uruguai seguiu com a *Ley de*

*Protección de Datos Personales y Acción de Habeas Data* em 2008, estabelecendo a Unidade Reguladora e de Controle de Dados Pessoais.

Além disso, o Peru promulgou a *Ley de Protección de Datos Personales* em 2011, que também introduziu uma estrutura robusta para a proteção dos dados pessoais dos cidadãos peruanos, tendo como exemplo o direito previsto a ser informado da coleta de dados, com quem serão compartilhados e suas funcionalidades.

Esses exemplos evidenciam a relevância e a necessidade urgente da regulamentação da proteção de dados em um mundo cada vez mais digital e interconectado, servindo como inspiração para a criação de normas como a LGPD no Brasil. A LGPD, portanto, emerge como um marco regulatório essencial, buscando equilibrar a proteção dos direitos individuais com as demandas do mercado e a inovação tecnológica. Ao se alinhar com as melhores práticas internacionais, o Brasil reforça sua posição no cenário global, promovendo um uso ético e responsável dos dados pessoais. Essa legislação não apenas resguarda os direitos dos cidadãos, mas também fomenta a competitividade e a responsabilidade corporativa, incentivando a adoção de políticas e práticas que assegurem a segurança e a privacidade das informações.

A criação dessas regulamentações demonstra a responsabilidade social necessária em relação à privacidade dos cidadãos, obrigando pessoas físicas e jurídicas a seguir políticas adequadas ao tratamento de dados pessoais. Entretanto, a criação da LGPD no Brasil não se baseia exclusivamente em um viés protecionista, mas também se justifica por motivações estratégicas. A entrada do Brasil na Organização para a Cooperação e Desenvolvimento Econômico (OCDE)<sup>9</sup> é um dos objetivos subjacentes que impulsionaram a formulação dessa normativa. Visto que o ingresso na organização era um dos objetivos do país

A OCDE composta por países que buscam promover políticas que melhorem o bem-estar econômico e social, exige que seus membros cumpram certos

---

<sup>9</sup> LEME, Carolina da Silva. Proteção e Tratamento de Dados sob o Prisma da Legislação Vigente. *Revista Fronteiras Interdisciplinares do Direito*, São Paulo, V.1, n. 1, 2019, p. 178-197. Disponível em: <https://revistas.pucsp.br/index.php/fid/article/view/41960>. Acesso em: 09 de julho de 2024

requisitos, incluindo a adoção de instrumentos normativos<sup>10</sup> como as Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais de 1980. Diante desse contexto, tornou-se imperativo para o legislador brasileiro elaborar uma normativa específica de proteção de dados pessoais que estivesse em conformidade com os requisitos estabelecidos pela OCDE. O objetivo não era apenas assegurar a proteção dos dados dos cidadãos, mas também pavimentar o caminho para a integração do Brasil na organização, o que seria um catalisador para atração de investimentos, dessa forma posicionando o Brasil de forma mais competitiva no cenário global, consolidando-o no grupo das nações mais desenvolvidas. Nesse sentido, foi promulgada em agosto de 2018 a Lei nº 13.709, conhecida como Lei Geral de Proteção de Dados (LGPD).

É crucial destacar que o marco regulatório de proteção de dados no Brasil não se encerrou com a LGPD. O cenário tecnológico em constante mutação exige um esforço contínuo de atualização e adaptação da legislação. Novas normas e interpretações devem ser elaboradas pelos órgãos competentes, a fim de garantir a efetiva proteção dos dados pessoais em um ambiente digital em constante transformação. A LGPD não apenas regula, mas também educa e conscientiza. As empresas que a implementam de forma eficaz conquistam a confiança dos clientes, fidelizam parceiros e se preparam para um futuro promissor na era digital.

## 2.2. PRINCÍPIOS DA LGPD

Nenhuma legislação, por mais ampla que seja, consegue antecipar todas as nuances e cenários que podem surgir durante sua aplicação. É nesse contexto que os princípios jurídicos desempenham um papel crucial, atuando como guias fundamentais para orientar a interpretação judicial e a implementação da lei em situações omissas ou controversas. Os princípios jurídicos não apenas preenchem lacunas legislativas, mas também estabelecem diretrizes éticas e normativas que moldam a conduta dos agentes envolvidos no sistema jurídico.

---

<sup>10</sup> SHREIBER, Anderson. Right to Privacy and Personal Data Protection in Brazilian Law. In: VICENTE, Dário Moura; CASIMIRO, Sofia de Vasconcelos (ed.). Data Protection in the Internet. V. 38. Cham: Springer, 2020. p.45-54, p. 46.

Ao proporcionar uma estrutura conceitual e axiológica, esses princípios garantem consistência e coerência na aplicação das normas, promovendo a justiça e a equidade no tratamento de questões jurídicas complexas e em evolução.

De Plácido e Silva (1989, p. 447) conceituam princípios jurídicos como:

As normas elementares ou os requisitos primordiais instituídos como base, como alicerce de alguma coisa. E, assim, princípios revelam o conjunto de regras e preceitos, que se fixaram para servir de norma a toda espécie de ação jurídica, traçando, assim, a conduta a ser tida em qualquer operação jurídica. Desse modo, exprimem sentido. Mostram a própria razão fundamental de ser das coisas jurídicas, convertendo-se em perfeitos axiomas. Princípios Jurídicos, sem dúvida, significam pontos básicos, que servem de ponto de partida ou de elementos vitais do próprio Direito. E, nesta acepção, não se compreendem somente os fundamentos jurídicos, legalmente instituídos, mas todo axioma jurídico derivado da cultura jurídica universal. Compreendem, pois, os fundamentos da Ciência Jurídica, onde se firmam as normas originárias ou as leis científicas do Direito, que traçam as noções em que se estrutura o próprio Direito. Assim, nem sempre os princípios inscrevem-se nas leis. Mas, porque servem de base ao Direito, são tidos como preceitos fundamentais para a prática do Direito e proteção aos Direitos.

Ainda sobre o conceito de princípios, Reale (1986, p. 60), afirma:

Princípios são, pois verdades ou juízos fundamentais, que servem de alicerce ou de garantia de certeza a um conjunto de juízos, ordenados em um sistema de conceitos relativos à dada porção da realidade. Às vezes também se denominam princípios certas proposições, que apesar de não serem evidentes ou resultantes de evidências, são assumidas como fundantes da validade de um sistema particular de conhecimentos, como seus pressupostos necessários.

Pois bem, a partir de tais considerações introdutórias, passemos a examinar os princípios jurídicos assim considerados pela LGPD em relação ao tratamento, que são: finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; e, responsabilização e prestação de contas, dispostos nos incisos I a X do artigo 6º da lei 13.709/2018.

### **2.2.1. Princípio da Boa-fé**

No âmbito das relações sociais e jurídicas, o Princípio da Boa-Fé ergue-se como um pilar fundamental, ancorado na presunção de que os indivíduos atuam com boas intenções. Essa premissa, embora possa parecer idealista, é crucial para a manutenção da confiança mútua, essencial tanto para a harmonia social quanto para a efetividade do direito. No artigo 6º da Lei LGPD, são elencados diversos critérios — denominados de princípios — que se constituem, em essência, como desdobramentos dos deveres da boa-fé.

A importância deste princípio no direito decorre do fato de que as interações humanas geram expectativas de comportamento futuro. Contudo, impossibilidade de conhecer plenamente as intenções internas de cada indivíduo gera uma inevitável sensação de insegurança diante do potencial de ser enganado. Nesse sentido, a boa-fé funciona como um mecanismo que mitiga essa insegurança, promovendo a confiança e previsibilidade nas relações jurídicas.

No contexto da LGPD, o tratamento de dados pessoais deve observar o princípio da boa-fé, que exige que os agentes responsáveis por esse tratamento protejam os direitos dos titulares dos dados e ajam de forma diligente e cuidadosa. Este princípio transcende a mera obediência à lei, representando um compromisso ético que fundamenta a construção de relações de confiança entre os agentes de tratamento e os titulares dos dados. A boa-fé na LGPD implica comportamentos leais, honestos e transparentes por parte dos agentes de tratamento, respeitando a confiança e as expectativas legítimas dos titulares. Portanto, a atuação deve ser diligente e ética, evitando abusos, fraudes ou manipulações que possam prejudicar os direitos e liberdades individuais.

Um exemplo evidente de descumprimento do princípio da boa-fé pode ser encontrado em uma cooperativa agrícola, que coleta dados de umidade e saúde das plantas usando drones e sensores de solo, mas não informa adequadamente os agricultores sobre a coleta, utilização e armazenamento desses dados. Sem o consentimento dos agricultores, a cooperativa vende essas informações a empresas de marketing agrícola, que utilizam os dados para enviar ofertas comerciais indesejadas. Além disso, a cooperativa negligencia a segurança dos dados, resultando em vazamentos frequentes. Essa prática viola os princípios

de transparência, finalidade e segurança estabelecidos pela LGPD, comprometendo a confiança e a privacidade dos agricultores.

Portanto, o princípio da boa-fé na LGPD não apenas orienta a conduta dos agentes de tratamento, mas também reforça a proteção dos direitos dos titulares de dados, promovendo um ambiente de confiança e segurança nas relações que envolvem o tratamento de informações pessoais. A adoção de práticas pautadas na boa-fé contribui para a construção de um sistema de proteção de dados mais justo e eficaz, alinhado com os valores democráticos e com a dignidade da pessoa humana. Por meio da observância de comportamentos leais e honestos, é possível garantir que o tratamento de dados pessoais respeite a confiança dos titulares e as expectativas legítimas em relação ao uso de suas informações, evitando abusos e fraudes que possam prejudicar os direitos e liberdades dos indivíduos.

### **2.2.2. Princípio da Finalidade**

O princípio da finalidade constitui um elemento central na LGPD, determinando que o tratamento de dados pessoais deve ser limitado a finalidades específicas, definidas de maneira precisa e relevantes para a relação em questão. Devem ser também explícitas, garantindo clareza, logo, não admitindo a equivocidade ou ambiguidade, não se restando dúvidas acerca do conteúdo. Além disso, devem ser legítimas, fundamentadas em razões de legalidade e bom senso, excluindo iniciativas emocionais ou de má-fé.

As finalidades do tratamento de dados são estabelecidas no momento da coleta dos mesmos, conforme o artigo 6º, I da LGPD, que requer que os dados pessoais sejam processados de acordo com os objetivos previamente comunicados aos titulares. Em outras palavras, os dados só podem ser utilizados para propósitos determinados, informados ao titular no momento da coleta, e não podem ser posteriormente processados de maneira incompatível com o acordo original. A importância deste princípio é evidenciada pela sua referência em diversos artigos da legislação, como os artigos 7º, 8º, 9º, 10º, 11º, 12º, 15º e 19º da LGPD.

O princípio da finalidade, como examinado por VAINZOF (2019, p. 138), tem um significado prático notável. Este princípio permite que os titulares garantam a

legalidade no tratamento de seus dados, com base nas informações previamente obtidas, restringindo a utilização dos dados a propósitos lícitos e regulando o acesso por terceiros. O objetivo principal é minimizar o risco de uso secundário dos dados sem o consentimento expresso do titular.

Louzada (2019, p. 95) destaca a necessidade de vincular o processamento de dados à finalidade específica previamente autorizada, não apenas para restringir a atividade de tratamento ao objetivo inicial, mas também para prevenir qualquer apropriação indevida dos dados. A autora enfatiza a importância de comunicar aos titulares a finalidade do processamento, assegurando que eles entendam como suas informações serão utilizadas e podendo consentir ou recusar o tratamento de maneira consciente. Este princípio visa, portanto, evitar práticas abusivas na coleta de dados e proteger a privacidade dos titulares, reduzindo os riscos de uso indevido ou não autorizado das informações.

Na prática, a implementação do princípio da finalidade requer que os controladores de dados estabeleçam políticas claras e procedimentos rigorosos para assegurar que os dados pessoais sejam utilizados exclusivamente para os fins previamente especificados. Isso implica a necessidade de garantir que todos os colaboradores e parceiros com acesso aos dados compreendam e respeitem as finalidades estabelecidas. Além disso, é essencial proceder no momento adequado com o descarte seguro dos dados, assim que a finalidade para a qual foram coletados for alcançada, utilizando métodos apropriados para assegurar a proteção e a privacidade dos titulares.

### **2.2.3. Princípio da Adequação**

Previsto no artigo 6º, inciso II da LGPD, o princípio da adequação estabelece que o tratamento de dados pessoais deve ser compatível com as finalidades informadas ao titular, considerando o contexto em que o tratamento ocorre. Este princípio enfatiza a necessidade de uma coerência lógica e uma pertinência clara entre o tratamento dos dados e as finalidades comunicadas, conforme informado ao titular no momento da coleta.

De acordo com Vainzof (2019, p. 142):

O princípio da adequação está vinculado ao da finalidade, pois prevê que o tratamento de dados pessoais somente pode ser realizado quando houver compatibilidade com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

O princípio da adequação exige mais do que uma mera compatibilidade entre os propósitos e o tratamento dos dados. Ele impõe que as organizações adotem medidas rigorosas para assegurar que os dados coletados sejam necessários, relevantes e precisos. Portanto, não basta que o tratamento esteja alinhado com as finalidades; é crucial que os dados sejam pertinentes e adequados ao contexto do tratamento.

Para garantir a adequação, deve-se estabelecer uma relação lógica entre vários elementos: o tratamento de dados e a finalidade pretendida, o tratamento de dados e a comunicação feita ao titular, a finalidade pretendida e a comunicação feita ao titular, e a interação entre esses elementos de forma integrada.

O contexto do tratamento, estabelece um sistema de referência que assegura a pertinência e a coerência do tratamento dos dados em relação às finalidades declaradas, conforme a circunstância. Este princípio exige uma avaliação constante das práticas de tratamento de dados para garantir que permaneçam dentro dos limites do que foi originalmente informado ao titular, prevenindo abusos e usos indevidos das informações pessoais.

Um exemplo prático pode ser observado em um e-commerce de produtos eletrônicos, onde não seria justificável solicitar dados de saúde dos usuários, pois essa solicitação não seria compatível com a objetivo do negócio. Assim, se os dados solicitados não são compatíveis com a finalidade, o tratamento se torna inadequado.

Adicionalmente, essencial que as organizações implementem políticas claras e procedimentos específicos para assegurar a conformidade com o princípio da adequação. Isso inclui a realização de avaliações regulares do contexto e das finalidades do tratamento de dados, garantindo que todos os colaboradores e parceiros compreendam e respeitem esses critérios.

#### **2.2.4. Princípio da Necessidade**

O princípio da necessidade, fundamentado no artigo 6º, III da LGPD, estabelece que o tratamento de dados pessoais deve ser limitado ao mínimo necessário para a realização de suas finalidades, utilizando apenas os dados pertinentes, proporcionais e não excessivos em relação aos objetivos do tratamento. Este princípio está intrinsecamente ligado aos princípios anteriores da LGPD, formando um núcleo da lei, juntamente ao princípio da transparência. (VAINZOF, 2019, p. 138).

A norma geral da LGPD determina que a coleta de dados deve ser restrita ao necessário para alcançar as finalidades estabelecidas, seguindo o critério de proporcionalidade: dados irrelevantes ou excessivos não devem ser coletados ou processados, uma vez que o excesso vai além dos limites da proporcionalidade. Dentro do escopo da LGPD, a proporcionalidade permite o tratamento de dados apenas na medida do estritamente necessário para alcançar os objetivos previamente definidos e consentidos pelo titular dos dados.

No GDPR, o princípio da necessidade é conhecido como "limitação das finalidades", onde os dados pessoais devem ser adequados, pertinentes e limitados ao mínimo necessário para os propósitos do tratamento. Isso implica que o período de retenção dos dados deve ser limitado ao mínimo necessário, conforme determinado pelo controlador.

Dessa forma, ao pautar-se no princípio e ao realizar a análise e a revisão dos dados pessoais armazenados e suas respectivas categorias, as organizações têm a oportunidade única de reavaliar suas estruturas de armazenamento e segurança da informação, adequando-as ao porte e à operação da empresa. Isso também oferece uma chance de reduzir custos com armazenamento, garantindo que apenas os dados essenciais e relevantes sejam mantidos.

#### **2.2.5. Princípio do Livre Acesso**

O artigo 6º, inciso IV, da Lei Geral de Proteção de Dados (LGPD) consagra o princípio do livre acesso, cujo objetivo é assegurar aos titulares de dados a possibilidade de consulta facilitada e gratuita sobre o tratamento de seus dados pessoais. Este princípio garante legalmente que os titulares possam consultar

seus próprios dados sem dificuldades, assegurando que as informações sejam disponibilizadas de maneira clara, compreensível e completa.

O referido princípio é reforçado pelo artigo 9º da LGPD, que demonstra a necessidade de garantir a integridade dos dados dos titulares. As informações devem ser apresentadas de forma adequada e evidente, abordando aspectos como a finalidade específica do tratamento, a identificação e os dados de contato do controlador, o compartilhamento de dados e suas finalidades, bem como as responsabilidades dos agentes de tratamento (VAINZOF, 2019, p. 147-148).

Ademais, a entrega das informações pode ocorrer em formato físico ou eletrônico, conforme a requisição do titular, e deve favorecer o exercício do direito de acesso. A entrega deve ser simplificada e imediata, podendo ser realizada por meio de uma declaração clara e completa que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, respeitando segredos comerciais e industriais. O prazo para disponibilização dessas informações é de até 15 dias a partir da solicitação do titular (Artigo 19, LGPD), devendo o formato escolhido permitir a utilização subsequente das informações, inclusive em outras operações de tratamento.

Antes do início do tratamento de dados, o titular deve ser informado sobre como poderá acessar os dados tratados, e sobre a duração do tratamento, incluindo o tempo necessário para sua realização e o período durante o qual os dados serão utilizados para atingir a finalidade proposta. Esta exigência pode ser desafiadora, pois é difícil prever antecipadamente o prazo de utilização dos dados tratados.

Para que a garantia de livre acesso e outras condições previstas na LGPD seja efetivamente materializada, é necessário que essas condições sejam satisfeitas e explicitamente consentidas pelos titulares, de forma adequada e em tempo oportuno. Tal concordância deve ser explícita, assegurando que os titulares estejam plenamente informados e de acordo com o tratamento de seus dados pessoais.

#### **2.2.6. Princípio da Qualidade de Dados**

O princípio da qualidade de dados, presente no artigo 6º, V da LGPD, desempenha um papel importante na garantia da exatidão, clareza, relevância e

atualização dos dados pessoais dos titulares. A exatidão refere-se à precisão dos dados, exigindo uma correspondência estrita entre os dados coletados, o tratamento realizado e a finalidade estabelecida. Dados imprecisos podem levar a conclusões errôneas, comprometendo a eficácia e a finalidade do tratamento. Por sua vez, a clareza implica que os dados e os procedimentos de tratamento sejam apresentados de forma compreensível e transparente, garantindo que as informações sejam comunicadas em termos que possam ser facilmente entendidos pelos titulares.

A relevância indica que apenas os dados necessários para alcançar a finalidade específica do tratamento devem ser coletados e utilizados, evitando o tratamento de dados irrelevantes ou excessivos, que pode resultar em invasões desnecessárias à privacidade dos titulares. Já a atualização dos dados enfatiza a necessidade de manter os mesmos, precisos e atualizados ao longo do tempo, refletindo as mudanças dinâmicas da vida dos titulares. Dados desatualizados podem levar a decisões inadequadas, comprometendo os direitos e a eficácia do tratamento.

A qualidade dos dados é um aspecto essencial para o tratamento ético dos dados pessoais. O seu uso desatualizado, obscuro ou irrelevante pode gerar consequências negativas significativas para os titulares. Por exemplo, a falta de precisão na localização das plantações pode comprometer a eficiência dos sistemas de irrigação e a aplicação de defensivos, resultando em desperdícios e danos ao meio ambiente. Além disso, dados desatualizados podem levar a decisões inadequadas.

Os titulares devem ser informados sobre as entidades públicas e privadas com as quais o controlador compartilhou seus dados, e sobre a possibilidade de não fornecer consentimento, bem como as consequências dessa negativa. Portanto, assegurar a qualidade dos dados é fundamental para proteger os direitos fundamentais dos indivíduos. Somente por meio de informações atualizadas e confiáveis, os agentes de tratamento podem tomar decisões informadas e justas.

### **2.2.7. Princípio da Transparência**

O princípio da transparência se configura como um dos pilares basilares da LGPD. Sua relevância reside na garantia do acesso claro e preciso dos titulares

a informações sobre o tratamento de seus dados pessoais. Essa prerrogativa fundamental encontra amparo no artigo 6º, inciso VI, da LGPD, que estabelece a *"garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial"* (BRASIL, 2018).

A transparência no tratamento de dados pessoais não é uma novidade introduzida pela LGPD. No contexto legislativo brasileiro, este princípio já estava presente em normativas anteriores. A Lei de Acesso à Informação (Lei 12.527/2011), por exemplo, destaca em seu artigo 6º, inciso I, a gestão transparente da informação, proporcionando amplo acesso e divulgação das informações. Ademais, o Marco Civil da Internet (Lei 12.965/2014) também estabelece a proteção à privacidade e aos dados pessoais como um de seus princípios fundamentais, assegurando que o uso da internet no Brasil observe esses direitos (BRASIL, 2014).

O princípio da transparência na LGPD visa a permitir que os titulares de dados possuam ampla informação sobre o percurso de seus dados pessoais dentro de uma organização. A transparência é fundamental para promover a confiança entre os titulares e os agentes de tratamento, constituindo uma premissa de lealdade e respeito. Para que este princípio seja efetivamente aplicado, é necessário que as informações referentes ao tratamento dos dados pessoais sejam apresentadas de forma concisa e acessível, utilizando uma linguagem simples e clara. Isso inclui a identificação do responsável pelo tratamento dos dados pessoais na organização e a explicação dos direitos dos titulares, como o direito de obter a comunicação de seus dados pessoais (VAINZOF, 2019b).

É importante destacar que a falta de transparência nas práticas de proteção de dados pessoais já resultou em sanções significativas para diversas organizações, inclusive para Multinacionais. Um exemplo notável é o caso da empresa Facebook, que, antes da implementação do Regulamento Geral sobre a Proteção de Dados (GDPR), foi penalizada com uma multa de €500.000,00 (quinhentos mil euros) pelo órgão regulador do Reino Unido devido à ausência de transparência na proteção das informações dos usuários da plataforma (MARTIN; MARKS, 2020). Se o GDPR já estivesse em vigor na época, a

penalidade teria sido consideravelmente mais alta, alcançando até US\$1 bilhão (MARTIN; MARKS, 2020)

Outro caso exemplificativo, agora já sob a vigência do GDPR, envolveu a Google, que foi sancionada com uma multa de €50.000.000,00 (cinquenta milhões de euros) pela Autoridade Francesa de Proteção de Dados (CNIL), também devido a deficiências na transparência dos processos de tratamento de dados (VAINZOF, 2019a). No contexto brasileiro, embora a Lei Geral de Proteção de Dados (LGPD) ainda não estivesse plenamente em vigor, foi aplicada uma multa administrativa a uma drogaria com base na falta de transparência nas práticas de proteção de dados (VAINZOF, 2019a). Esses exemplos ressaltam a importância crítica do princípio da transparência tanto na legislação brasileira quanto na europeia, evidenciando a necessidade de conformidade rigorosa para evitar penalidades substanciais.

A transparência exige que não se utilize linguagem excessivamente técnica ou hermética, para que todas as pessoas, independentemente de seu nível cultural, possam compreender facilmente como seus dados estão sendo tratados. O objetivo é garantir que, num relance, o titular possa entender o que ocorrerá com seus dados após serem coletados e durante todo o processo de tratamento.

Conforme ensina Viana (2011, p.7), "As questões de transparência estão novamente em vigor nas regulamentações processuais, incluindo a promoção de uma cultura de transparência e disponibilização de dados em línguas acessíveis sem barreiras técnicas". Portanto, o princípio da transparência na LGPD é indispensável para a proteção dos direitos dos titulares de dados

#### **2.2.8. Princípios da Segurança e da Prevenção**

O princípio da segurança, disposto no artigo 6º, VII, da LGPD, impõe aos agentes de tratamento de dados pessoais a obrigação de implementar medidas técnicas e administrativas capazes de proteger esses dados contra acessos não autorizados. Além disso, tais medidas devem evitar ocorrências acidentais ou ilegais de destruição, perda, modificação, transmissão ou divulgação dos dados. O objetivo central deste princípio é assegurar a integridade e a confidencialidade

dos dados pessoais, mitigando riscos de violações que possam resultar em danos aos titulares.

A relevância do princípio da segurança é evidente diante da urgência em prevenir violações de dados pessoais, que representam uma ameaça constante aos direitos dos titulares. Essas violações não apenas comprometem a privacidade dos indivíduos, mas também impõem aos agentes de tratamento responsabilidades significativas, incluindo possíveis sanções administrativas e responsabilidade civil (Vainzof, 2019).

Para implementar o princípio da segurança de maneira eficaz, é imperativo que as organizações adotem tecnologias de segurança contemporâneas e práticas administrativas robustas, prática está diretamente interligada ao princípio da prevenção. O que inclui a criação de uma cultura organizacional que valorize a proteção de dados, através de treinamentos contínuos para colaboradores e a definição de responsabilidades claras em todos os níveis da organização. Além disso, a prática de realizar avaliações periódicas de vulnerabilidades e testes de penetração é essencial para identificar e corrigir falhas de segurança de maneira proativa.

Destaca-se que, no contexto do princípio da segurança, é irrelevante se a perda, acesso, alteração ou difusão de dados resulta de uma conduta voluntária e ilícita ou de um mero acidente, independentemente de ser causado por negligência, imprudência ou imperícia. Os agentes de tratamento são obrigados a prever e se precaver contra todos os cenários possíveis que possam ocorrer, garantindo a proteção integral dos dados pessoais sob sua responsabilidade. Essa obrigação não se estende aos titulares dos dados, que devem ter acesso autorizado às suas informações, porém com as devidas cautelas procedimentais e técnicas constantemente apuradas e atualizadas.

O artigo 46, da LGPD, em seus parágrafos 1º e 2º, estipula que além da responsabilidade pela adoção de medidas de proteção, a Autoridade Nacional de Proteção de Dados (ANPD) poderá dispor sobre os padrões técnicos mínimos aceitáveis. A conformidade com esses padrões pode representar um custo significativo para as organizações, mas é indispensável para a proteção adequada dos dados pessoais. O escopo de responsabilidade dos agentes de

tratamento é, portanto, extenso e complexo, abrangendo tanto medidas preventivas quanto reativas para assegurar a segurança dos dados pessoais.

O princípio da prevenção, embora esteja intrinsecamente relacionado ao princípio da segurança, é explicitamente destacado no artigo 6º, VIII da LGPD. No qual é determinado que durante o tratamento de dados pessoais, devem ser adotadas medidas necessárias para prevenir a ocorrência de danos. Essa reiteração enfatiza a responsabilidade contínua dos agentes de tratamento em proteger os dados antes, durante e após o seu processamento, sendo abrangidos pelo princípio da segurança. Visto que, a palavra prevenção que advém do latim PRAEVENIRE, com o significado de antecipar, literalmente chegar antes.

Logo, a prevenção vai além de medidas reativas, ou seja, não é suficiente agir somente após a ocorrência de um incidente. Medidas preventivas devem ser implementadas para evitar possíveis danos, garantindo que todos os riscos associados ao tratamento de dados sejam adequadamente gerenciados e mitigados.

A LGPD, em seus artigos 46 e 50, estabelece diretrizes para a implementação de ações de governança e treinamentos, essenciais para uma abordagem preventiva. Essas diretrizes incluem a criação de programas de conformidade, monitoramento constante das práticas de tratamento de dados e a realização de auditorias periódicas para garantir que as medidas preventivas sejam eficazes e atualizadas.

Em síntese, o princípio da prevenção reforça a necessidade de uma postura ativa e contínua na proteção dos dados pessoais. As organizações devem adotar uma abordagem panorâmica que integre políticas de segurança, práticas de governança e capacitação de pessoal para garantir que todos os aspectos da proteção de dados sejam contemplados.

### **2.2.9. Princípio da Não Discriminação**

A LGPD assentou, expressamente, a impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos, no artigo 6º, IX da LGPD. Não se pode ter exclusão de titulares de dados pessoais no momento de

seu tratamento de dados por determinadas características, sejam elas de origem racial ou étnica, opinião política, religião ou convicções, geolocalização, filiação sindical, estado genético ou de saúde ou orientação sexual.

VAINZOF, 2019, p. 165, já previu isso:

Ademais, há uma preocupação evidente quanto ao tratamento de dados pessoais para a adoção de decisões automatizadas, principalmente quanto à possibilidade, por meio de tecnologias como Inteligência Artificial, consumarem medidas discriminatórias.

O princípio da não discriminação, conforme consagrado no artigo 6º, IX da LGPD, estabelece a proibição expressa de tratar dados pessoais para fins discriminatórios, ilícitos ou abusivos. Este princípio visa garantir que, no processo de tratamento de dados, não haja exclusão ou segregação dos titulares com base em características pessoais, tais como origem racial ou étnica, opiniões políticas, religião ou crenças, geolocalização, filiação sindical, condições genéticas ou de saúde, ou orientação sexual.

A LGPD, ao incorporar esse princípio, assegura que a coleta e o processamento de dados pessoais sejam conduzidos de maneira justa e equitativa, sem perpetuar preconceitos ou injustiças sociais. A legislação procura impedir que as práticas de tratamento de dados reforcem desigualdades existentes ou criem novas formas de discriminação.

Além disso, há uma preocupação crescente com o uso de tecnologias avançadas, como a Inteligência Artificial (IA), na tomada de decisões automatizadas. Conforme destaca Vainzof (2019), essas tecnologias possuem um potencial significativo para consolidar medidas discriminatórias se não forem cuidadosamente reguladas e supervisionadas. Decisões automatizadas baseadas em algoritmos podem, inadvertidamente, replicar vieses existentes nos dados de treinamento, resultando em discriminação sistemática contra determinados grupos.

Para mitigar esses riscos, a LGPD exige que os agentes de tratamento implementem salvaguardas robustas que garantam a transparência e a justiça nos processos automatizados de tomada de decisão. Isso inclui a necessidade de revisões periódicas e auditorias dos algoritmos utilizados, bem como a

obrigação de fornecer aos titulares dos dados informações claras sobre os critérios e os processos envolvidos na tomada de decisões automatizadas.

A conformidade com o princípio da não discriminação também implica a adoção de políticas de diversidade e inclusão dentro das organizações, promovendo um ambiente onde todas as decisões relacionadas ao tratamento de dados sejam livres de preconceitos e baseadas em critérios objetivos e transparentes. As organizações devem, portanto, integrar esse princípio em suas práticas de tratamento de dados, garantindo que todas as operações sejam realizadas com respeito à dignidade e aos direitos dos titulares.

#### **2.2.10. Princípio da Responsabilização e Prestação de Contas**

O princípio da responsabilização e prestação de contas, conforme delineado no artigo 6º, X da Lei Geral de Proteção de Dados Pessoais (LGPD), estabelece que os controladores e operadores de dados pessoais são responsáveis por todas as medidas adotadas para cumprir as exigências legais e os princípios estabelecidos pela legislação. Este princípio enfatiza que as ações tomadas pelos agentes de tratamento de dados devem ser não apenas implementadas, mas também eficazes na proteção dos direitos dos titulares.

A boa-fé objetiva, como mencionado por Louzada (2019), está intrinsecamente ligada ao princípio da responsabilização e prestação de contas. Ao analisar que a boa-fé objetiva se refere à conduta ética e transparente que se espera dos agentes de tratamento, baseada na lealdade, honestidade e respeito aos direitos dos titulares. Este conceito jurídico assegura que os agentes de tratamento atuem de forma justa e razoável.

De acordo com Vainzof (2019), a LGPD tem como objetivo assegurar que os agentes de tratamento estejam cientes de suas responsabilidades e sejam capazes de demonstrar, a qualquer momento, a conformidade com a lei. Isso implica em uma gestão rigorosa e transparente dos dados pessoais, onde cada ação e procedimento deve ser documentado e justificado. A capacidade de prestação de contas é fundamental para garantir que os controladores e operadores possam responder adequadamente a quaisquer questionamentos ou

auditorias realizadas pela Autoridade Nacional de Proteção de Dados (ANPD) ou por outros órgãos competentes

A rastreabilidade, como palavra de ordem nos tempos atuais, exige comprovação dos procedimentos e atos praticados, e no âmbito da proteção de dados pessoais, ganha a importância adicional da fácil acessibilidade. Rastreabilidade com responsabilidade implica a adoção de posturas sérias, técnicas e respeitadas em relação aos dados do tratamento, refletindo diretamente nos respectivos titulares.

Interessante também, observar que o agente de tratamento não só deverá comprovar que adotou os procedimentos e praticou os atos permitidos pela normativa, mas também que todos eles foram eficazes. Caso contrário, ainda que o agente tenha agido com boa-fé, o descumprimento das normas de proteção de dados equivalerá a um confronto direto com o princípio da responsabilização e prestação de contas.

Portanto, o princípio da responsabilização e prestação de contas exige uma postura ativa e contínua dos agentes de tratamento na busca pela conformidade com a LGPD. As organizações devem adotar medidas que não apenas cumpram as exigências legais, mas que também promovam uma cultura de proteção de dados fundamentada na ética e na transparência. A eficácia dessas medidas será avaliada pela capacidade das organizações de demonstrar, de forma clara e documentada, o cumprimento de suas responsabilidades perante a lei e perante os titulares de dados.

### 2.3. ESTRUTURA E APLICABILIDADE NORMATIVA

A Lei Geral de Proteção de Dados (LGPD) estabelece normas rigorosas e abrangentes sobre o tratamento de dados pessoais, aplicáveis tanto ao ambiente físico quanto ao digital, e abrangendo tanto pessoas físicas quanto jurídicas. No entanto, destaca-se a proteção aos dados pessoais de indivíduos, considerando que o tratamento pode indiretamente envolver informações de caráter íntimo. Devido à sua abrangência e relevância, a LGPD se aplica a todos os entes federativos brasileiros.

O propósito primordial da LGPD, conforme expresso no Art. 1º, é assegurar a proteção dos dados pessoais, visando a garantir os direitos fundamentais de liberdade, privacidade e desenvolvimento da personalidade dos indivíduos. O Art. 2º complementa esse objetivo ao vincular a lei aos princípios fundamentais da República Federativa do Brasil.

Estruturalmente, a LGPD inicia sua regulamentação definindo os conceitos e princípios fundamentais para o tratamento de dados pessoais (Capítulo I - Disposições Preliminares). Em sequência, especifica as hipóteses e modalidades autorizadas para o tratamento desses dados (Capítulos II e IV). Adicionalmente, a lei consagra um conjunto de direitos aos titulares dos dados (Capítulo V) e determina as obrigações dos agentes de tratamento (Capítulo VI).

Para garantir a observância dessas disposições e a efetiva proteção dos dados pessoais, a LGPD incorpora no Capítulo VII recomendações de boas práticas e padrões de conduta. Ademais, a lei estabelece um robusto sistema processual destinado a assegurar a eficácia dos direitos dos titulares e das próprias disposições legais, delineando mecanismos de fiscalização no Capítulo VIII e atribuindo competências à Autoridade Nacional de Proteção de Dados (ANPD) no Capítulo XII.

Para a aplicação da Lei Geral de Proteção de Dados (LGPD), é imperativo analisar as hipóteses de não aplicabilidade da norma, especialmente no que diz respeito, às transferências de dados. Essa análise está delineada nos artigos 3º e 4º, da LGPD, entretanto aplicação também requer a verificação da existência de outros tratados e convenções internacionais que possam convergir com a legislação brasileira.

Conforme o artigo 3º, da LGPD, a aplicabilidade da lei é determinada nas circunstâncias: quando a coleta de dados ocorre em território brasileiro, quando a operação de tratamento é realizada no Brasil, ou quando há oferta de produtos e serviços a titulares localizados no Brasil.

Por outro lado, o artigo 4º da LGPD estabelece um rol taxativo de situações nas quais a lei não é aplicável. Especificamente, a LGPD não abrange o tratamento de dados realizado com fins exclusivamente pessoais e sem finalidade econômica, incluindo atividades artísticas, jornalísticas e acadêmicas. Além

disso, a lei exclui de sua abrangência as operações de tratamento de dados que tenham como finalidade exclusiva a segurança pública, a defesa nacional, a segurança do Estado e a repressão criminal. Adicionalmente, a LGPD também não é aplicável aos dados originados fora do território nacional que não sejam compartilhados com agentes de tratamento do país ou de transferência internacional.

De forma exemplificativa e para fins de ilustração, imagine a seguinte hipótese: no setor agrário, uma empresa brasileira que coleta dados pessoais de agricultores locais para fornecer serviços de agricultura de precisão deve estar em conformidade com a LGPD ao compartilhar esses dados com uma empresa parceira situada na União Europeia. O que implica, na garantia de que a empresa estrangeira ofereça um nível de proteção de dados compatível com a legislação brasileira e assegurar que os titulares dos dados sejam devidamente informados sobre a transferência e seus direitos associados.

#### 2.4. CONCEITOS DA LGPD

Em conformidade com a estrutura da Lei Geral de Proteção de Dados (LGPD), o artigo 5º apresenta uma série de definições cruciais que fundamentam as disposições subsequentes. Conforme discutido no capítulo anterior deste trabalho acadêmico, a intensificação da digitalização no contexto rural resulta no aumento de atividades que requerem o tratamento de dados pessoais. Assim, para a adequada observância das normas estabelecidas pela lei, é imperativo compreender estes conceitos e critérios.

Os dois primeiros incisos do referido artigo tratam da definição de dado pessoal. Mas, afinal, o que constitui um dado?<sup>11</sup> Segundo BIONI, Proteção de Dados Pessoais (...), (2019):

O dado é o estado primitivo da informação, pois não é algo que per se acresce conhecimento. Dados são simplesmente fatos brutos que,

---

<sup>11</sup> A leitura do conceito de dado pessoal apresentado pela GDPR é relevante, pois proporciona uma definição detalhada e exemplificativa. Conforme o Artigo 4º, a GDPR define "dados pessoais" como "informação relativa a uma pessoa singular identificada ou identificável ('titular dos dados'); considera-se identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como, por exemplo, um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular".

quando processados e organizados, se convertem em algo inteligível, podendo ser deles extraída uma informação.

Dessa forma, conclui-se que os dados pessoais, termo este presente no inciso I do artigo 5º da lei, se referem aos fragmentos de informações associáveis a uma pessoa natural identificada ou identificável. A diferença entre uma pessoa natural identificada e uma pessoa natural identificável reside na maneira pela qual a identificação pode ser realizada. Uma pessoa natural identificada pode ser reconhecida de forma direta e isolada, através de informações como nome completo ou número de documento. Em contrapartida, uma pessoa natural identificável requer a associação de múltiplos dados para que a identificação seja efetivamente realizada. Por exemplo, o número de telefone por si só não identifica uma pessoa, mas em combinação com outros dados, pode levar à identificação do indivíduo.

O termo "dados pessoais" possui uma amplitude significativa, abrangendo uma vasta gama de atividades no setor agropecuário. A coleta e o processamento de dados pessoais tornaram-se elementos essenciais para diversas operações e serviços do ramo. Um exemplo disso é a rastreabilidade de processos produtivos, que envolve o monitoramento detalhado de todas as etapas da produção, desde o plantio até a colheita, exigindo o registro e a análise de informações pessoais dos trabalhadores e operadores.

No contexto do acesso a créditos, instituições financeiras coletam dados pessoais dos agricultores, como informações de renda, histórico de crédito e garantias, para avaliar a capacidade de pagamento e os riscos associados. Além disso, outro exemplo constitui, na utilização de dados georreferenciados que permite a coleta de informações espaciais precisas sobre as propriedades rurais, como coordenadas geográficas, características do solo e padrões climáticos, entre outros.

A Lei Geral de Proteção de Dados Pessoais (LGPD) também aborda os dados pessoais sensíveis, que requerem uma atenção especial devido ao seu potencial de gerar discriminação ou causar prejuízos e dados<sup>12</sup>. Esses dados, por sua natureza, revelam aspectos íntimos e privados da vida das pessoas, justificando

---

<sup>12</sup> Em alusão ao parágrafo primeiro do art. 11 da LGPD

a abordagem mais rigorosa da lei em relação ao seu uso. Dados sensíveis incluem informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, bem como informações sobre a vida sexual, saúde, dados genéticos e biometria, sempre que vinculados a uma pessoa natural<sup>13</sup>.

#### **2.4.1. Agentes de Tratamento**

A Lei Geral de Proteção de Dados Pessoais (LGPD), em seu artigo 5º, define os principais envolvidos no tratamento de dados pessoais, sendo eles o titular<sup>14</sup>, os agentes de tratamento<sup>15</sup>, e o encarregado<sup>16</sup>.

Embora a LGPD forneça uma definição precisa do titular, que é a pessoa natural a quem os dados se referem, é fundamental esclarecer que o responsável pelo tratamento dos dados não é o titular, mas sim o agente de tratamento que atua em nome deste. Os agentes de tratamento podem ser tanto pessoas naturais quanto jurídicas, de direito público ou privado, e são designados conforme a estrutura institucional relevante. Importante destacar que, na prática, o agente de tratamento refere-se à entidade como um todo e não a uma área ou indivíduo específico.

De acordo com as orientações da Autoridade Nacional de Proteção de Dados (ANPD), o controlador<sup>17</sup> é responsável por tomar decisões estratégicas relacionadas ao tratamento de dados pessoais. Isso inclui definir as finalidades do tratamento e as diretrizes para a atuação dos agentes operadores. Em contraste, o operador<sup>18</sup> executa o tratamento dos dados pessoais em nome do controlador, operando conforme as instruções fornecidas e realizando as operações práticas de tratamento. A principal distinção entre esses agentes reside na capacidade de decisão: enquanto o controlador tem a prerrogativa de definir o escopo e os objetivos do tratamento, o operador limita-se à execução das tarefas conforme determinado.

---

<sup>13</sup> Art. 5º, II, da LGPD

<sup>14</sup> Vide Art. 5º, V, da LGPD

<sup>15</sup> Art. 5º, IX da LGPD

<sup>16</sup> Art. 5º, VIII, da LGPD

<sup>17</sup> Art. 5º, VI, da LGPD

<sup>18</sup> Art., 5º, VII da LGPD

A definição do papel de cada agente deve ser realizada de acordo com a natureza específica de cada atividade de tratamento. Portanto, um agente pode assumir a função de controlador em uma determinada operação e atuar como operador em outra, dependendo das circunstâncias.

A compreensão do papel do controlador é crucial, pois este agente assume a maior parte das responsabilidades previstas pela LGPD. Entre suas obrigações estão a elaboração do Relatório de Impacto à Proteção de Dados (RIPD), a garantia dos direitos dos titulares de dados, a nomeação do encarregado pelo tratamento, a notificação de incidentes de segurança à ANPD e aos titulares, e a responsabilidade pelo ônus da prova do consentimento.

Segundo a ANPD:

O segundo ponto relevante é a desnecessidade de que todas as decisões sejam tomadas pelo controlador, bastando apenas que este mantenha sob sua influência e controle as principais decisões, isto é, aquelas relativas aos elementos essenciais para o cumprimento da finalidade do tratamento.<sup>19</sup>

No que tange ao operador, sua função é estritamente seguir as instruções fornecidas pelo controlador, desempenhando atividades relacionadas ao tratamento de dados pessoais conforme estabelecido. Além disso, o operador pode definir aspectos não essenciais do tratamento, como a implementação de medidas técnicas de segurança. Sua principal responsabilidade é assegurar a segurança dos dados enquanto realiza o tratamento efetivo, funcionando essencialmente como o executor das operações de tratamento de dados.

O encarregado, figura introduzida pela LGPD, mas ainda não abordado, atua como o canal de comunicação sobre questões de proteção de dados, servindo como o interlocutor entre a empresa, a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares dos dados. Conforme disposto na legislação, o encarregado pode ser uma pessoa física ou uma pessoa jurídica, e sua função é essencial para garantir a conformidade com as normas de proteção de dados.

---

<sup>19</sup> ANPD. Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado. Disponível em: [https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento\\_Final.pdf](https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf). Acesso em 22/07/2024.

A ANPD pode, futuramente, estabelecer regulamentações adicionais para definir com mais precisão as atribuições e qualificações deste profissional.

Por fim, é imperativo não esquecer e reconhecer o papel regulador da ANPD, que inclui a criação de normas e diretrizes para a implementação e o cumprimento da LGPD. A ANPD tem a responsabilidade de esclarecer aspectos relevantes para todos os agentes de tratamento, promovendo a padronização de documentos e melhores práticas. Seu objetivo é garantir uma adequada conformidade com a LGPD, assegurando que as obrigações legais dos agentes de tratamento sejam efetivamente atendidas e que as práticas de proteção de dados sejam aprimoradas continuamente.

#### **2.4.2. Tratamento de Dados Pessoais e Bases Legais**

Segundo a LGPD, mais especificamente no inciso X, do artigo 5º, toda atividade realizada com o uso dos dados pessoais, pode ser definida como tratamento, incluindo no que desrespeito a coleta, armazenamento, classificação, distribuição, utilização ou próprio descarte.

Dessa forma, as empresas públicas ou privadas que realizam a coleta de dados dos clientes, mantêm os dados de seus colaboradores e fazem a gestão da folha de pagamento de salário, realizam ações promocionais e envio de informações, devem estar adequadas a LGPD, visto que são exemplos de situações que constituem tratamento de dados pessoais, que poderá ser por meio físico, documentos em papel, ou digital, por meio de arquivos digitalizados.

Conforme a lei toda atividade de tratamento de dados pessoais, deve estar amparada em uma base legal, que referência as hipóteses de tratamento listadas na LGPD. São estabelecidas 10 hipóteses para os dados pessoais dispostas no artigo 7º, da lei e 8º para os dados sensíveis, é importante destacar que não existe hierarquia entre elas, todas tem igual relevância e podem ser utilizadas de forma ampla.

O amplo conhecimento e entendimento das bases legais é crucial para o cumprimento da LGPD, isso porque, são elas que embasarão qualquer tratamento de dados e devem nortear o uso dos dados pessoais pelos players do mercado.

Abaixo temos uma tabela com a descrição das bases legais dispostas no artigo 7º em seus incisos da LGPD Tal qual foi realizado com os princípios, para trazeremos mais didática no desenvolvimento das 10 bases legais, somando-se a exemplos e resumos.

<b>Bases legais para o tratamento de dados pessoais na LGPD</b>		
<b>Base legal</b>	<b>Descrição</b>	<b>Exemplo</b>
Consentimento (art. 7º, I)	O art. define o consentimento como uma manifestação livre, informada e inequívoca do titular, concordando com o tratamento de seus dados para uma finalidade específica <sup>20</sup> . Este consentimento deve ser claro e explícito, não podendo ser presumido ou genérico <sup>21</sup> . Embora considerado seguro por garantir a autodeterminação informativa do titular, pode ser revogado a qualquer momento, o que pode interromper o tratamento de dados em andamento. A responsabilidade de obter e demonstrar o consentimento recai sobre o controlador, que deve garantir que o titular esteja plenamente informado e que sua decisão seja voluntária e claramente expressada.	Ofertas personalizadas: coletar dados para oferecer produtos e serviços adequados aos produtores;  Tratamento de dados de geolocalização para fins de navegação em aplicativos de entrega de comida.
Obrigação Legal ou Regulatória (art. 7º, II)	Permite o tratamento de dados pessoais necessário para atender exigências legais ou regulamentares, como no setor financeiro ou	Instituições financeiras podem tratar dados para prevenir fraudes, mas usá-los para publicidade seria ilegal.

<sup>20</sup> É relevante notar que o conceito de consentimento na LGPD difere daquele presente no Marco Civil da Internet. Enquanto o Marco Civil exige que o consentimento seja expresso e destacado, conforme o art. 7º, IX, a LGPD adota o consentimento inequívoco. Marcel Leonardi destaca que essa diferença foi intencional para evitar a "fadiga do consentimento," onde o excesso de solicitações de consentimento expresso pode levar os usuários a aceitar tudo sem ler. Isso enfraquece a proteção legal, pois os titulares dos dados não prestariam a devida atenção, ficando menos protegidos. (LEONARDI, Marcel. Principais bases legais para o tratamento de dados pessoais no setor privado. In SOUZA; Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscilla (coord.). Caderno especial: Lei Geral de Proteção de Dados (LGPD). 1ª edição, São Paulo: Thomson Reuters Brasil, 2019.)

<sup>21</sup> Em linha com a redação do art. 8º, §1º da LGPD.

	de saúde. No entanto, o uso desses dados é restrito à finalidade específica. Utilizar os dados para outros fins, como marketing, sem nova base legal, viola a LGPD.	
Execução de política pública pela administração pública (art. 7º, III)	Permite à Administração Pública tratar dados pessoais para cumprir atos de governo e deveres do Estado, abrangendo órgãos da administração direta e indireta, bem como contratos e convênios. O tratamento de dados para políticas públicas não requer consentimento, mas deve ser transparente sobre quais dados são compartilhados e com quem, justificando o uso baseado na política pública específica.	Um exemplo é o controle de vacinação infantil, onde o governo utiliza dados para planejar a compra de vacinas e direcionar campanhas de conscientização.
Realização de estudos por órgãos de pesquisa (art. 7º, IV)	Permite o tratamento de dados pessoais por entidades públicas ou privadas sem fins lucrativos dedicadas à pesquisa histórica, científica, tecnológica ou estatística. A LGPD não se aplica a fins exclusivamente acadêmicos (art. 4º, II), mas os tratamentos devem seguir os princípios de finalidade, boa-fé e interesse público. A anonimização dos dados é recomendada para afastar a aplicabilidade da LGPD. Órgãos de pesquisa devem garantir que a anonimização seja irreversível; caso contrário, devem cumprir as disposições da LGPD, especialmente os arts. 7º e 11º.	Uma universidade pode tratar dados de pacientes para realizar pesquisas sobre novos tratamentos médicos.
Execução de Contratos (Art. 7º, V)	Autoriza o tratamento de dados pessoais para a execução de contratos. Abrange desde os procedimentos preliminares até o cumprimento de	Uma empresa de telefonia coleta dados pessoais do cliente, como nome, endereço e número de telefone, para instalar a linha telefônica e fornecer o

	<p>obrigações contratuais a pedido do titular. Essa autorização se baseia no interesse do titular na concretização do contrato, seja para fornecimento de produtos, serviços ou relações de trabalho.</p>	<p>serviço de telecomunicações.</p>
<p>Exercício regular de direitos (art. 7º, VI)</p>	<p>Permite o tratamento de dados pessoais para assegurar o exercício da justiça, incluindo o contraditório, a ampla defesa e o livre acesso à justiça. Essencial para a condução de processos judiciais, administrativos e arbitrais, esta base legal permite a coleta e manutenção de dados necessários à produção de provas e comunicação entre partes. Ela é utilizada para a preservação de dados que podem originar processos judiciais, como registros de empregados, para defesa em ações trabalhistas ou de consumo. A utilização dessa base deve ser específica para o exercício regular de direitos, evitando-se qualquer desvio de finalidade.</p>	<p>Um advogado coleta dados pessoais de clientes para defender seus direitos em processos judiciais.</p>
<p>Proteção a vida ou Integridade física (art. 7º, VII)</p>	<p>permite o tratamento de dados pessoais em situações emergenciais para salvaguardar a vida e a integridade física dos indivíduos. Este inciso, que abrange diversos cenários, justifica o acesso e uso de dados pessoais rapidamente em emergências, como em acidentes para identificar vítimas inconscientes ou em hospitais para determinar tratamentos médicos compatíveis com as crenças religiosas dos pacientes. A sua aplicação pode ser</p>	<p>A um paciente em um hospital, e a necessidade de determinar a religião do paciente para apurar se poderá realizar uma transfusão de sangue e certo tratamento, ou não.</p>

	<p>ampla, mas exige cuidados especiais, especialmente ao tratar dados de crianças e adolescentes.</p>	
<p>Tutela a saúde (art. 7º, VI)</p>	<p>permite o tratamento de dados pessoais por profissionais de saúde, serviços de saúde e autoridades sanitárias. Esta previsão abrange uma ampla gama de atividades essenciais para a proteção da saúde, como tratamentos médicos e intervenções sanitárias, embora a definição de "serviços de saúde" possa ser interpretada de forma abrangente. Exemplos incluem a necessidade de uma empresa de alimentação hospitalar tratar dados de pacientes para fornecer refeições adequadas. No entanto, o uso de dados deve estar alinhado com a finalidade específica de tutela da saúde e respeitar as diretrizes da LGPD para evitar potenciais abusos.</p>	<p>Um plano de saúde coleta dados pessoais de beneficiários para autorizar procedimentos médicos e reembolsar despesas com saúde.</p>
<p>Legítimo Interesse (Art. 7º, IX)</p>	<p>Permite o tratamento de dados pessoais quando necessário para atender a interesses legítimos do controlador ou de terceiros, desde que não prevaleçam sobre os direitos e liberdades fundamentais dos titulares. Para aplicá-la, o controlador deve garantir que o interesse seja específico, legítimo e não se sobreponha desproporcionalmente aos direitos dos titulares. A base legal não se aplica a dados sensíveis e exige minimização dos dados,</p>	<p>Um exemplo prático é o uso de dados para personalizar ofertas, desde que os dados utilizados sejam estritamente necessários e não infrinjam direitos dos titulares.</p>

	transparência nas operações e análise documentada de riscos. A LGPD também requer que o controlador e o operador mantenham registros das operações de tratamento, e a ANPD pode exigir um relatório de impacto à proteção de dados. <sup>22</sup>	
Proteção ao crédito (art. 7º, X)	permite que profissionais de saúde, serviços de saúde e autoridades sanitárias tratem dados pessoais para atividades essenciais à proteção da saúde, incluindo tratamentos médicos e intervenções sanitárias. Embora a definição de "serviços de saúde" seja ampla, o tratamento de dados deve sempre estar alinhado com a finalidade específica de tutela da saúde e em conformidade com a LGPD para evitar abusos.	Uma instituição financeira pode tratar dados pessoais de clientes para avaliar o risco de crédito e conceder empréstimos.

**Tabela 1:** Bases Legais Para O Tratamento De Dados Pessoais Na LGPD

### 2.4.3. Direitos dos Titulares

Os direitos dos titulares de dados, conforme estabelecido pela Lei Geral de Proteção de Dados (LGPD), são elementos essenciais para a eficácia da proteção de dados pessoais no Brasil. Sem a garantia desses direitos, a implementação da proteção proposta pela Lei seria consideravelmente enfraquecida. A LGPD não apenas define normas que devem ser seguidas por empresas e organizações no tratamento de dados pessoais, mas também assegura uma série de direitos aos titulares desses dados.

<sup>22</sup> Cumpre ressaltar que o tratamento de dados baseado no legítimo interesse não pode ser revogado a pedido do titular de dados, dessa forma, alguns profissionais de proteção de dados, seguindo a doutrina europeia, sugerem o desenvolvimento do *Legitimate Interests Assessment* (LIA), também conhecido como um teste de ponderação acerca da melhor aplicabilidade da base legal. Dessa forma, será necessária a realização de três (3) análises sobre o tratamento de dados pretendido, sendo elas: 1. Teste de Finalidade – identificação de quem é o legítimo interesse; 2. Teste de Necessidade – validação se de fato é necessário esse tratamento de dados para que seja atingido o interesse pretendido; 3. Teste de Balanceamento – equalização do tratamento com os direitos do titular

O propósito é harmonizar os direitos dos titulares com as operações de processamento de dados.

Os direitos estão elencados no Capítulo III, da Lei Geral de Proteção de Dados (LGPD), abrangem os artigos 17 a 22. Este capítulo da lei pode ser resumido da seguinte forma: o Art. 17 estabelece garantias constitucionais fundamentais relacionadas à proteção de dados pessoais. Já o Art. 18 detalha os direitos dos titulares, especificando a forma de exercer esses direitos e as responsabilidades dos controladores para assegurar seu cumprimento.

O Art. 19 descreve as obrigações dos controladores quanto à informação sobre a existência e o acesso aos dados, garantindo transparência e acesso para os titulares. O Art. 20, por sua vez, aborda o direito de revisão dos dados e as obrigações associadas ao cumprimento desse direito. Finalmente, os Arts. 21 e 22 fornecem previsões sobre a forma de execução dos direitos, funcionando quase como um “direito processual” que orienta a aplicação prática desses direitos.

Para uma análise mais aprofundada, o presente trabalho se concentrará especificamente no Art. 18, que delinea os principais direitos dos titulares. A seguir, será apresentada uma tabela para ilustrar esses direitos de maneira mais clara e detalhada.

<b>Direitos dos Titulares de Dados Pessoais</b>		
<b>Direito do Titular</b>	<b>Descrição do Direito</b>	<b>Base Legal (Art. e Inciso)</b>
Direito à Informação	Este direito permite que o titular seja informado sobre a existência de tratamento de seus dados pessoais, incluindo a confirmação da existência desse tratamento, as entidades com as quais os dados foram compartilhados e a	Art. 18, I, VII, VIII

	possibilidade de não fornecer consentimento para o tratamento.	
Direito de Acesso	O titular tem o direito de acessar os dados pessoais que estão sendo tratados pelo controlador, podendo solicitar informações detalhadas sobre seus dados, tanto em formato simplificado quanto completo	Art. 18, II
Direito de Retificação	O titular pode solicitar a correção de dados pessoais que estejam incompletos, inexatos ou desatualizados. O controlador deve atender a essa solicitação, realizando a devida correção.	Art. 18, III
Direito de Anonimização	Este direito permite que o titular solicite a anonimização de dados pessoais que sejam considerados desnecessários ou excessivos. O controlador deve proceder com a anonimização dos dados conforme o pedido do titular	Art. 18, IV
Direito de Bloqueio	O titular pode solicitar o bloqueio de dados pessoais que sejam desnecessários ou excessivos. O controlador deve atender a essa solicitação e restringir o uso dos dados	Art. 18, IV
Direito de Eliminação	Este direito possibilita ao titular solicitar a eliminação de dados pessoais que sejam desnecessários, excessivos ou que estejam sendo tratados em desacordo com a legislação. A eliminação pode ocorrer, especialmente, quando o	Art. 18, IV, VI

	tratamento é baseado no consentimento do titular	
Direito de Portabilidade	O titular tem o direito de solicitar a transferência de seus dados pessoais para outro fornecedor de serviços. Este direito está sujeito às regulamentações estabelecidas pela Autoridade Nacional de Proteção de Dados (ANPD) e visa proteger segredos comerciais e dados anonimizados	Art. 18, V
Direito de Revogar Consentimento	O titular pode revogar o consentimento dado para o tratamento de seus dados pessoais, o que obriga o controlador a cessar o tratamento dos dados.	Art. 18, IX
Direito de Oposição	O titular pode se opor ao tratamento de seus dados pessoais quando este não se basear em consentimento. Este direito é aplicável nos casos em que o tratamento não é fundamentado no consentimento do titular	Art. 18, §2º
Direito de Petição	Este direito permite que o titular apresente petições contra o controlador junto à ANPD ou aos órgãos de defesa do consumidor, visando a proteção de seus direitos.	Art. 18, §1º, §8º, 22
Direito à Revisão de Decisões Automatizadas	O titular pode solicitar a revisão de decisões que sejam baseadas exclusivamente em tratamento automatizado de dados pessoais, podendo	Art. 20

	exigir uma revisão humana dessas decisões que impactem seus interesses	
--	--	--

**Tabela 2:** Direitos dos Titulares de Dados Pessoais

Os direitos previstos na Lei Geral de Proteção de Dados (LGPD) podem ser exercidos a qualquer momento pelo próprio titular ou por um representante legalmente autorizado. Neste contexto, é responsabilidade do controlador de dados implementar e disponibilizar mecanismos adequados para o recebimento e processamento dessas solicitações, garantindo a validação da autenticidade das mesmas. Em relação aos prazos para resposta, a LGPD estabelece que respostas simplificadas devem ser fornecidas imediatamente, enquanto respostas completas devem ser entregues no prazo máximo de 15 dias. No entanto, é importante observar que a Autoridade Nacional de Proteção de Dados (ANPD) possui a competência para regulamentar prazos específicos que possam variar conforme as particularidades de diferentes setores.

### **3. PROTEÇÃO DE DADOS NO SETOR AGROPECUÁRIO: DESAFIOS E PERSPECTIVAS FUTURAS**

No capítulo anterior, abordamos a definição de dados pessoais e dados sensíveis. Agora, exploraremos o conceito de dados agrícolas, essenciais para este estudo. Dados agrícolas são informações geradas a partir de operações agropecuárias, incluindo aspectos relacionados à terra, aos animais, às finanças da fazenda, entre outros. Esses dados são normalmente obtidos através de tecnologias integradas aos processos produtivos, como máquinas, sensores e sistemas automatizados.

O continente europeu é reconhecido pela vanguarda em legislação de proteção de dados. O Regulamento Geral sobre a Proteção de Dados (GDPR) estabelece diretrizes rigorosas sobre como os dados pessoais dos residentes da União Europeia (UE) devem ser processados. O GDPR visa eliminar a fragmentação regulatória e promover uma abordagem uniforme na proteção de dados, impondo restrições severas à coleta e ao uso subsequente de dados pessoais (GDPR, 2016). Embora os dados agrícolas sejam classificados como dados não pessoais, a GDPR motivou a criação de um documento autorregulador sobre o Fluxo Livre de Dados Não Pessoais, que aborda explicitamente os dados agrícolas. O artigo 4º desse documento trata do armazenamento de dados da agricultura inteligente, proibindo seu armazenamento exclusivo em uma única localização geográfica, prática conhecida como 'localização'. A proibição da localização busca evitar inovações limitadas e restrições ao fluxo de informações nas economias de dados globais (REGULAMENTO UE, 2018).

A redação do Código Autorregulador, apoiado pelos países membros da União Europeia, foi impulsionada pelos principais stakeholders do setor agropecuário. Este código visa garantir que os agricultores se adaptem perfeitamente à era digital e adotem rapidamente soluções tecnológicas para a agricultura (COPA-COGECA, 2018). O regulamento coloca o agricultor no centro da coleta, processamento e gestão de dados agrícolas, promovendo a conscientização sobre as questões do compartilhamento de dados e incentivando o diálogo entre agricultores e provedores de tecnologias agrícolas para ajustar os termos do compartilhamento de dados (COPA-COGECA et al., 2018).

A incorporação de tecnologia na agricultura resultou em um aumento significativo no desenvolvimento e produtividade do setor agropecuário, gerando um fluxo imenso de dados. Atividades agrícolas são agora potencializadas por grandes volumes de dados coletados e compartilhados em tempo real. Empresas que fornecem tecnologia agropecuária têm acesso e armazenam esses dados, e com a implementação da Lei Geral de Proteção de Dados (LGPD) no Brasil, essas empresas devem garantir transparência máxima na utilização e tratamento desses dados, evitando práticas oportunistas.

Segundo Van Der Burg (2020), o potencial da tecnologia agrícola digital só será plenamente realizado quando os agricultores estiverem dispostos a compartilhar seus dados com outras partes interessadas, como agroindústrias desenvolvendo essas tecnologias. Contudo, há uma relutância por parte dos agricultores em compartilhar dados, devido ao receio de que esses parceiros utilizem os dados para outros fins, excluindo os agricultores dos benefícios. Esse receio é evidenciado na possibilidade de utilização de dados para influenciar mercados financeiros, traçar perfis de agricultores e vender esses perfis a terceiros, como fornecedores de insumos, ou até mesmo comercializar dados com pesquisadores, governos, ONGs, bancos, seguradoras, entre outros (VAN DER BURG, 2020). Tal cenário cria um ambiente de incertezas.

Em síntese, a proteção dos dados agrícolas no Brasil deve ser amparada pela LGPD, seus princípios e pelos códigos de práticas de compartilhamento de dados agrícolas, visando estabelecer confiança entre agricultores e provedores de tecnologia agrícola. A revolução digital na agricultura apresenta desafios que devem ser superados com base na confiança e responsabilidade, considerando os aspectos éticos, legais e sociais inerentes à agricultura digital.

### 3.1. O BIG DATA

Desde os anos 2000, o termo "big data" ganhou popularidade, porém sua definição ainda apresenta várias interpretações. Para o presente trabalho, o big data será definido como a capacidade crescente de produzir, gerenciar, analisar e sintetizar dados, criando e destruindo diferentes formas de valor (IDS, 2015). Esse processo utiliza ferramentas não tradicionais, tanto de hardware quanto de software, para lidar com grandes volumes de dados estruturados e

não estruturados. Nos negócios, o investimento em big data é significativo, mas seu desenvolvimento e implementação oferecem vantagens competitivas substanciais às organizações (TRAN; SREENATH; JAIMIN, 2013).

A aplicação do big data no agronegócio representa uma transformação muito relevante na maneira como os dados são coletados, analisados e utilizados. Big data refere-se ao processamento de grandes volumes de dados gerados em alta velocidade e variedade, fornecendo insights valiosos que podem ser utilizados para otimizar processos, melhorar a tomada de decisões e aumentar a eficiência operacional. Na sua versão rural, o objetivo é armazenar e processar informações sobre o solo, o clima e as características das variedades agrícolas disponíveis para aumentar a produtividade e a eficiência no uso da água, sementes e fertilizantes (MAIA, 2014).

Desde os anos 2000, o termo "big data" ganhou popularidade, porém sua definição ainda apresenta várias interpretações. Para o presente trabalho, o big data será definido como a capacidade crescente de produzir, gerenciar, analisar e sintetizar dados, criando e destruindo diferentes formas de valor (IDS, 2015). Esse processo utiliza ferramentas não tradicionais, tanto de hardware quanto de software, para lidar com grandes volumes de dados estruturados e não estruturados. Nos negócios, o investimento em big data é significativo, mas seu desenvolvimento e implementação oferecem vantagens competitivas substanciais às organizações (TRAN; SREENATH; JAIMIN, 2013).

, não estruturados e semiestruturados; velocidade, que indica a rapidez com que os dados são processados; veracidade, que classifica as fontes de dados considerando a qualidade, precisão e atualidade dos dados; e valor, que corresponde ao valor que a informação dos dados terá no processo de tomada de decisão.

Sonka (2016) ao abordar o setor agrário, sugere três caminhos para a criação de valor: a aplicação de ferramentas para medir e monitorar as atividades agrícolas com baixo custo; a análise de dados (analytics), que integra dados de diversas fontes para gerar novas ideias; e pressões externas para melhor monitoramento das atividades agrícolas, que, se realizado, tende a criar fontes de dados que podem levar a mudanças estratégicas. Dessa forma, no longo prazo, big data poderá auxiliar no fornecimento de respostas à algumas

questões, como sobre como atender a demanda de alimentos no futuro sem colocar pressões irreparáveis sobre os recursos naturais. O uso de informações de clima, solo e outras variáveis, portanto, é decisivo para alcançar modos de produção sustentáveis.

Segundo Wolfert (2017), a agricultura inteligente (smart farming) é um desenvolvimento que enfatiza o uso de tecnologias de informação e comunicação no ciclo de gestão ciberfísica das fazendas. O fenômeno do big data gera volumes massivos de dados com uma grande variedade, que são capturados, analisados e empregados para a tomada de decisões. Nesse contexto, big data vem sendo empregado para fornecer insights preditivos em operações agrícolas, orientando decisões operacionais em tempo real.

Diante do exposto, pode-se afirmar que o agronegócio foi um dos setores que mais absorveu o impacto da tecnologia de big data. A busca pela eficiência na produção colocou a inovação tecnológica em primeiro plano no setor rural, desenvolvendo sistemas de gerenciamento agrícola fundamentados no controle tecnológico das variáveis de espaço e tempo.

### 3.2. PERCEPÇÕES DO SETOR AGROPECUÁRIO EM RELAÇÃO À LGPD: DESAFIOS E PERSPECTIVAS GERACIONAIS

A implementação da Lei Geral de Proteção de Dados Pessoais (LGPD) no setor agropecuário enfrentará desafios significativos, com a disseminação limitada da lei emergindo como um dos principais obstáculos. De maneira mais específica, no setor agrário, esse desafio foi exacerbado pela coexistência de duas gerações principais de agricultores, cada uma apresentando características e abordagens distintas em relação à adoção de novas tecnologias e práticas de proteção de dados. Sendo elas, os agricultores tradicionais, podendo pertencer a gerações mais velhas e os agricultores modernos, muitas vezes pertencentes a gerações mais novas.

Os agricultores tradicionais adotam uma abordagem conservadora em relação à tecnologia. Eles confiam predominantemente em práticas tradicionais e no conhecimento empírico acumulado ao longo dos anos. Esta geração tende a ser mais relutante em adotar big data e outras inovações tecnológicas, devido à percepção de risco e à falta de familiaridade com essas ferramentas. A resistência à mudança é uma barreira significativa para a implementação eficaz

da LGPD entre esses agricultores, que podem não reconhecer imediatamente a relevância da proteção de dados pessoais em suas operações

Por outro lado, os agricultores modernos, são mais abertos à adoção de novas tecnologias e práticas inovadoras. Eles estão mais propensos a integrar big data, inteligência artificial e outras ferramentas avançadas em suas operações agrícolas. Esta geração é caracterizada por uma abordagem dinâmica e disposta a experimentar novas metodologias para melhorar a eficiência e a produtividade. Além disso, eles valorizam a formação contínua e a atualização constante sobre as últimas tendências e tecnologias no setor agrícola, o que facilita a implementação e o cumprimento da LGPD.

Em reconhecimento à necessidade de maior disseminação da LGPD no setor agropecuário, foi criada, no Brasil, uma cartilha específica para o agronegócio. Esta cartilha destaca a importância da LGPD, define conceitos-chave e fornece recomendações práticas para os agricultores. Segundo um estudo conduzido pela Associação Brasileira de Agricultura de Precisão e Digital (ASBRAAP) em parceria com o Ministério da Agricultura, Pecuária e Abastecimento (MAPA) e a Associação Brasileira das Empresas de Tecnologia de Informação e Comunicação (BRASSCOM, 2022), apenas um terço dos respondentes possuía conhecimento básico sobre privacidade e proteção de dados pessoais. Este conhecimento e acultramento precisam ser um exercício diário dos agentes do setor, visto que são fatores chave para assegurar o cumprimento da LGPD (BRASSCOM, 2022).

A conformidade com a LGPD e a maturidade em termos de proteção de dados são componentes cada vez mais comuns na avaliação de empresas, considerando o alto grau de integração entre os atores do setor, o que pode fortalecer toda a cadeia. O estudo revela que 30% dos respondentes estão em um nível avançado de adequação para a implementação da LGPD. Esta porcentagem corresponde as empresas de grande porte, com faturamento igual ou superior a R\$ 300 milhões, que se adequaram mais rapidamente. Em contraste, empresas menores encontram mais dificuldades para compreensão do tema e consequente adequação de suas atividades (BRASSCOM, 2022).

Dois terços dos respondentes indicaram que a dificuldade de implantação foi de grande ou média intensidade. A implementação de políticas e regras de

governança é essencial para a mudança necessária na cultura organizacional. Empresas maiores, em geral, têm mais condições de formar amplas parcerias envolvendo produtores, fornecedores, clientes e institutos de pesquisa, criando condições estruturais adequadas (BRASSCOM, 2022).

O estudo também mostra que 88% dos respondentes terceirizam, ao menos parcialmente, os sistemas de TI. Devido ao elevado índice de contratação de ferramentas de tecnologia operadas por terceiros e às responsabilidades dos agentes de tratamento previstas na LGPD, é importante formalizar os direitos e deveres de parceiros comerciais e prestadores de serviço através de contratos, identificando as funções de controlador e operador dos dados pessoais (BRASSCOM, 2022).

A capacitação foi o tipo de investimento mais citado, com 55% dos entrevistados indicando que investiram recursos para se adequarem à legislação. A implementação de políticas e a definição de estruturas de governança corporativa ajudam no processo de aculturação, porém a capacitação contínua é um elemento chave no desenvolvimento de programas de privacidade que auxiliam na adequação e implementação da Lei. As instituições representativas das categorias podem desempenhar um papel crucial nesse processo de capacitação (BRASSCOM, 2022).

Os dados coletados internamente são os de maior incidência (34%), seguidos dos de origem externa (30%). A heterogeneidade dos dados coletados pela agropecuária extrapola essa simples conceituação, incluindo dados de telemetria, agronômicos, de imageamento aéreo e estatísticos. O limite conceitual da abrangência do dado pessoal é um fator de preocupação e crítico para a operação segura e o contínuo processo de inovação (BRASSCOM, 2022).

A adequação à LGPD é vista por 56% dos respondentes como uma obrigação legal/regulatória, enquanto 44% enxergam oportunidades de inovação e agregação de valor ao negócio. Esta divisão reflete uma visão legalista, que pode ser justificada pela vigência recente da legislação e pelo fato de que um terço dos respondentes ainda possui pouco conhecimento sobre a LGPD. A capacitação, governança corporativa e implementação de políticas auxiliam na mudança dessa visão, contribuindo para a transformação da cultura organizacional (BRASSCOM, 2022).

Finalmente, 60% dos respondentes adotaram a nomeação de pessoas responsáveis pelo tratamento de dados pessoais, demonstrando uma atitude positiva em relação à conformidade com a lei e preocupação em se adequar às novas exigências (BRASSCOM, 2022).

Portanto, para uma implementação eficaz da LGPD no setor agropecuário, é crucial considerar as diferentes características e necessidades das gerações de agricultores. Iniciativas educacionais e de capacitação devem ser adaptadas para abordar as preocupações específicas dos agricultores tradicionais, ao mesmo tempo em que se aproveita a abertura dos agricultores modernos para integrar práticas de proteção de dados em suas operações. Somente assim será possível garantir a conformidade com a LGPD e proteger adequadamente os dados pessoais no contexto do agronegócio brasileiro.

### 3.3. PROTEÇÃO DE DADOS AGRÍCOLAS

A moderna agricultura tem se beneficiado significativamente da coleta e análise de dados, sendo que a produtividade das safras depende cada vez mais dessas informações. A análise de grandes volumes de dados, conhecida como big data agrícola, permite a otimização de práticas de cultivo e gestão de recursos. Segundo Maia (2014), a utilização de dados sobre o solo, o clima e as características das variedades agrícolas contribuem para melhorar a produtividade e a eficiência no uso de água, sementes e fertilizantes.

Ejnisman (2019) observa que a integração de tecnologias conectadas no campo resulta em um fluxo contínuo e massivo de dados, abrangendo desde métricas do agronegócio até informações sobre indivíduos que trabalham no setor. Esse fenômeno levanta questões significativas sobre a privacidade e o uso de dados pessoais, uma vez que a acessibilidade à internet e às tecnologias de big data, internet das coisas (IoT) e inteligência artificial aproxima o ambiente rural dessas tecnologias avançadas.

A Agricultura de Precisão (AP) tem transformado o setor agropecuário ao possibilitar a coleta e análise detalhada de dados relacionados a diversos aspectos da produção agrícola. No entanto, a vastidão e a complexidade das informações geradas pela AP suscitam preocupações acerca da proteção de

dados agrícolas. Para garantir a segurança, a privacidade e o uso responsável dessas informações, é essencial implementar medidas robustas de proteção de dados.

A AP depende de uma ampla gama de dados, que podem ser classificados em várias categorias, como segue:

I. **Dados Geoespaciais:** Incluem informações sobre a localização da propriedade, mapas topográficos e imagens de satélite, que ajudam a monitorar e gerenciar a distribuição e o uso do espaço agrícola.

II. **Dados Ambientais:** Envolvem condições climáticas, umidade do solo, temperatura e radiação solar, fornecendo insights sobre o ambiente que influencia o crescimento das culturas.

III. **Dados Operacionais:** Relacionam-se ao desempenho das máquinas agrícolas, consumo de combustíveis e horas trabalhadas, essenciais para a eficiência operacional.

IV. **Dados Biológicos:** Referem-se à saúde das plantas, desenvolvimento das culturas e à presença de pragas e doenças, permitindo intervenções mais precisas e oportunas.

V. **Dados Econômicos:** Abrangem custos de produção, preços de mercado e lucratividade das culturas, fundamentais para a análise econômica e a tomada de decisões estratégicas.

Portanto, a gestão eficaz da proteção de dados agrícolas é crucial para a maximização dos benefícios da Agricultura de Precisão, equilibrando a inovação tecnológica com a necessidade de assegurar a privacidade e a integridade das informações.

A conformidade com a LGPD representa um desafio significativo para a AP, especialmente considerando a natureza dinâmica e massiva dos dados gerados. As empresas devem investir em infraestrutura e processos para garantir a proteção de dados e lidar com a complexidade dos requisitos legais. Além disso, a necessidade de obter consentimento e garantir a transparência pode implicar ajustes nas práticas operacionais e na comunicação com os titulares dos dados.

### 3.4. INCIDENTES E MEDIDAS DE SEGURANÇA

A premissa fundamental da LGPD é a gestão de risco, que requer que os agentes de tratamento adotem medidas técnicas e administrativas de segurança para proteger dados pessoais contra acessos não autorizados e incidentes de segurança.

Os incidentes de segurança podem variar desde acessos não autorizados até a destruição acidental de dados. A natureza dos incidentes de segurança é intrinsecamente ligada à complexidade e à dinâmica dos ambientes tecnológicos. Embora as medidas de segurança robustas sejam fundamentais, é inevitável que alguns incidentes possam ocorrer devido a falhas, vulnerabilidades ou ações maliciosas. Portanto, a LGPD exige que as organizações não apenas previnam incidentes, mas também estejam preparadas para mitigar seus impactos.

Existem diversas medidas que podem ser adotadas para a prevenção de acidentes envolvendo a proteção de dados. A criptografia, por exemplo, constitui uma técnica fundamental para a salvaguarda de dados tanto em repouso quanto em trânsito. Ao criptografar os dados, mesmo que ocorra uma interceptação, a informação permanece inacessível sem a chave de descryptografia apropriada. Essa prática é essencial para assegurar a confidencialidade dos dados pessoais e reduzir o risco de exposição indevida, disponibilizando informações apenas para os usuários autorizados. Ademais, a criptografia, por meio de sua capacidade de garantir a integridade dos dados, assegura que as informações não foram manipuladas e confirma a autenticidade em relação à identidade dos usuários.

O controle de Acesso, que consiste em implementar controles rigorosos para acessar, assegura que apenas indivíduos autorizados possam acessar dados sensíveis, por exemplo desbloquear um smartphone com a biometria facial. Isso envolve autenticação multifatorial, que aumenta a segurança ao exigir múltiplos métodos de verificação antes de conceder acesso.

O Backup Regular também é essencial pois permite a recuperação de dados em caso de perda ou corrupção. Essa prática é uma salvaguarda crítica para assegurar a integridade e disponibilidade dos dados.

Utilizar ferramentas de monitoramento e detecção para identificar e responder a atividades suspeitas permite a detecção precoce de possíveis incidentes. A capacidade de resposta rápida é crucial para minimizar danos e proteger a integridade dos dados.

Uma boa Política de Segurança de Dado clara de segurança de dados orienta as práticas de proteção e manejo de informações. Políticas bem definidas são essenciais para assegurar a conformidade e promover uma cultura de segurança dentro da organização. Avaliação de Risco também é de extrema importância, regularmente ajuda a identificar vulnerabilidades e implementar medidas corretivas. A avaliação contínua do risco permite uma abordagem proativa para a gestão da segurança da informação.

A proteção física dos servidores e dispositivos de armazenamento é fundamental para evitar acessos não autorizados e proteger contra roubo ou danos. Medidas como o controle de acesso físico e a proteção contra desastres são componentes críticos dessa estratégia.

Manter sistemas e softwares atualizados é uma prática essencial para proteger contra vulnerabilidades conhecidas. As atualizações regulares garantem que as proteções de segurança estejam sempre em vigor.

Por fim, Auditorias e avaliações periódicas de segurança ajudam a verificar a conformidade com as políticas de proteção de dados e identificar áreas que necessitam de melhorias. Essas revisões proporcionam uma visão crítica sobre a eficácia das medidas de segurança adotadas.

### 3.5. ANPD FISCALIZAÇÃO E APLICAÇÃO DE SANÇÕES

Conforme abordado anteriormente, a Autoridade Nacional de Proteção de Dados (ANPD) é o “órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional”<sup>146</sup>. Sua criação, constituição e competência estão previstos nos arts. 55-A a 58-B da LGPD, sendo aqui incluídas as previsões relativas ao Conselho Nacional de

Proteção de Dados Pessoais e da Privacidade, órgão que também compõe a ANPD.

A ANPD tem como um de seus principais objetivos promover a orientação e a conscientização dos agentes de tratamento de dados, titulares e demais partes interessadas sobre a proteção de dados pessoais. Para além dessas atividades, a ANPD é responsável pela fiscalização e pela aplicação de sanções, conforme estabelecido no artigo 52 da LGPD e regulamentado pela Resolução CD/ANPD nº 1/2021. Esta resolução detalha o processo de fiscalização e as sanções administrativas, que entraram em vigor em 1º de agosto de 2021.

As sanções que a ANPD incluem:

- a) Advertência, com a estipulação de um prazo para a adoção de medidas corretivas;
- b) Multa simples, de até 2% (dois por cento) do faturamento, limitada a R\$ 50.000.000,00 (cinquenta milhões de reais);
- c) multa diária, limitada ao total de R\$ 50.000.000,00 (cinquenta milhões de reais);
- d) Publicização da infração;
- e) Bloqueio dos dados pessoais até a sua regularização;
- f) Eliminação dos dados pessoais;
- g) Suspensão parcial do funcionamento do banco de dados por até seis meses, prorrogável por mais seis meses;
- h) Suspensão do exercício da atividade de tratamento dos dados pessoais relacionada à infração, por até seis meses, prorrogável por igual período;
- i) Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados;

Embora tais sanções possam causar apreensão entre os agentes de tratamento, é importante ressaltar que, antes da aplicação de qualquer penalidade, a ANPD instaurará um processo administrativo. Este processo permite que os agentes de tratamento exerçam seu direito ao contraditório e à ampla defesa. Se a

penalidade for aplicada, a ANPD seguirá as diretrizes estabelecidas nos parágrafos 1º, 4º, 6º e 7º dos artigos 52, 53 e 54 da LGPD

Além da atuação direta da ANPD, outras entidades podem aplicar sanções relacionadas ao não cumprimento das normas de proteção de dados, como o Código de Defesa do Consumidor (CDC) e possíveis infrações penais apuradas durante a análise do tratamento de dados. A ANPD tem o papel de informar essas autoridades, se necessário.<sup>23</sup>

Para garantir o pagamento da indenização ao titular, a LGPD também estabelece que o controlador e o operador dos dados pessoais são solidariamente responsáveis por qualquer dano causado ao titular em caso de descumprimento da lei<sup>24</sup>. O operador pode ser responsabilizado se descumprir as instruções lícitas do controlador. Contudo, se for comprovado que os agentes de tratamento não realizaram o tratamento ilícito, ou se o dano for causado exclusivamente pelo titular ou por terceiros, os agentes de tratamento não serão considerados responsáveis.

A fiscalização da ANPD inclui promover o conhecimento das normas e políticas públicas sobre proteção de dados, além de assegurar a adoção de boas práticas e medidas de segurança. Os agentes regulados devem fornecer cópias de documentos, permitir o acesso a instalações e sistemas, e disponibilizar representantes para suporte durante a fiscalização.

Quanto ao processo administrativo sancionador pode ser iniciado de três formas: por iniciativa própria da ANPD, em decorrência de monitoramento, ou mediante requerimento. O legislador definiu critérios para a apuração de irregularidades, como o modo de tratamento, o balanceamento entre resultados e riscos, e as técnicas disponíveis no momento do tratamento. O processo poderá ser instaurado, a qualquer tempo, por ato da ANPD: (i) de ofício (por iniciativa da própria Autoridade); (ii) em decorrência de processo de monitoramento; e (iii) diante de requerimento em que a ANPD, através da Coordenação-Geral de Fiscalização, deliberar por sua abertura\*

---

<sup>23</sup> Por força do art. 55-J, XXI da LGPD

<sup>24</sup>Vide art. 42, § 1º da LGPD.

Ademais, é relevante considerar o impacto na imagem e na reputação das empresas como um risco significativo. A conformidade com a LGPD é não apenas uma obrigação legal, mas também uma questão estratégica para manter a competitividade no mercado. As empresas tendem a estabelecer relações comerciais com parceiros que também cumpram as normas da LGPD, a fim de evitar riscos associados a violações de dados que possam afetar sua posição no mercado.

### 3.6. DESAFIOS E APLICAÇÃO DA LGPD NO SETOR AGROPECUÁRIO

Conforme discutido ao longo deste estudo, torna-se evidente a relevância da devida conformidade com a Lei Geral de Proteção de Dados (LGPD) e a necessidade de conscientização dos usuários, especialmente no que se refere aos direitos dos titulares de dados. Esta transformação e processo de adaptação serão imprescindíveis em todos os setores econômicos, incluindo o agronegócio. Contudo, a implementação da LGPD no contexto das organizações rurais exigirá uma transformação cultural profunda nas instituições, abrangendo todos os níveis hierárquicos, desde a esfera estratégica até as operações práticas.

Para alcançar esse objetivo, é essencial uma ampla disseminação da lei, mas além disso, torna-se crucial refletir sobre a privacidade dos dados pessoais em todas as fases de seu tratamento. Será necessário desenvolver, cada vez mais, ações de conscientização que incorporem de forma intrínseca o respeito à privacidade de dados nas atividades cotidianas baseadas em dados. No contexto específico deste trabalho, que aborda o agronegócio, o produtor rural deve desempenhar um papel central, uma vez que está diretamente envolvido nas etapas de coleta, transferência, processamento e análise dos dados. Assim, o conhecimento e a cultura da privacidade de dados devem ser praticados diariamente pelos agentes do setor para fortalecer a cadeia produtiva.

A deficiência de conhecimento e/ou entendimento sobre a Lei Geral de Proteção de Dados (LGPD) constitui um dos desafios mais significativos no setor agropecuário, especialmente entre pequenas e médias empresas. Para abordar esta questão, a Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação - BRASSCOM (2022), sugere o estabelecimento de

parcerias com a Autoridade Nacional de Proteção de Dados (ANPD) e outras entidades setoriais, visando à disseminação de informações. Além disso, propõe a promoção de treinamentos específicos sobre o tema.

Uma solução pertinente para estas empresas de menor porte é apresentada pela Resolução CD/ANPD nº 2/2022, a qual regulamenta um regime jurídico diferenciado para agentes de tratamento de pequeno porte, incluindo startups. Esta resolução considera as dificuldades inerentes à implementação da LGPD por parte desses agentes, buscando equilibrar a viabilidade operacional com a garantia dos direitos dos titulares de dados. Pequenas empresas frequentemente expressam preocupação em relação à obrigatoriedade de designar um Encarregado de Proteção de Dados (DPO). A Resolução da ANPD, ao flexibilizar essa exigência para agentes de pequeno porte, deve ser amplamente divulgada com o intuito de mitigar essas preocupações. (BRASSCOM 2022).

Nesse contexto, um desafio adicional que se destaca é o desconhecimento sobre a aplicação da LGPD em sua interface com legislações específicas, como a Consolidação das Leis do Trabalho (CLT) e a Lei de Acesso à Informação (LAI). Para mitigar essa lacuna, é essencial realizar capacitações que esclareçam que essas leis são complementares e não se sobrepõem, garantindo uma compreensão mais holística da legislação. (BRASSCOM 2022).

Outro desafio identificado é a falta de conhecimento sobre as responsabilidades inerentes à coleta de dados físicos e virtuais. Para enfrentar essa questão, recomenda-se a implementação de alertas de coleta de dados em ambientes físicos e virtuais, bem como a adoção de um FAQ com informações claras aos titulares sobre as aplicações dos dados tratados. (BRASSCOM 2022).

Além disso, a falta de experiência dos contratantes com as complexidades da contratação de armazenamento de dados de terceiros é uma preocupação significativa. Para lidar com isso, é importante revisar os contratos e cláusulas de responsabilidades e obrigações entre as partes, especialmente no que tange à segurança da informação, vazamento e tratamento de dados. Também é recomendado realizar capacitações internas voltadas à educação sobre essas contratações, possivelmente com a participação de empresas prestadoras de serviços em nuvem. (BRASSCOM 2022).

Outro desafio destacado pela pesquisa da BRASSCOM (2022) refere-se à carência de conhecimento sobre o conceito de dados pessoais sensíveis e sua aplicação no setor. Além disso, observa-se uma dificuldade em compreender a extensão do conceito de dado pessoal e o desconhecimento das bases legais disponíveis para o tratamento de dados. A cartilha recomenda ampliar o conhecimento sobre as possibilidades que a LGPD oferece, além do consentimento, promovendo o desenvolvimento de processos de resolução coletiva para melhor entendimento dessas definições e a utilização de exemplos práticos do setor.

A adequação à Lei Geral de Proteção de Dados (LGPD) exige um investimento contínuo em capacitação e atualização de processos. Assim, com uma visão a longo prazo, é fundamental estabelecer prazos claros e designar responsáveis que implementem um programa robusto de *Compliance*. Além disso, é imperativo desenvolver programas de treinamento contínuo e utilizar ferramentas tecnológicas que facilitem o cumprimento das normas de proteção de dados.

O Programa de Proteção de Dados não segue um caminho único e predefinido, mas sim diversas possibilidades adaptáveis às rotinas, expectativas e culturas organizacionais das empresas. Essas variáveis compreendem as formas de aprendizado e o cumprimento das normas de conformidade, além do grau de complexidade envolvido no tratamento de dados pelas organizações.

Alexandre Pacheco delinea seis pilares essenciais que devem orientar tanto a conformidade quanto o estudo acadêmico em proteção de dados pessoais:

- I. Base Legal, que exige justificativas jurídicas claras para o tratamento de dados;
- II. Processos, que demanda a definição de procedimentos para a gestão de dados, a identificação dos agentes envolvidos e a justificação do tratamento;
- III. Segurança, que requer a identificação, comunicação e aprendizado contínuo a partir de incidentes de segurança;

IV. Design, que deve considerar a estruturação das atividades de forma a otimizar a receptividade dos titulares e atender às expectativas do mercado;

V. Transparência, que implica a disponibilização clara, completa e acessível de informações aos titulares; e

VI. Prevenção, que abrange a realização do tratamento e a gestão do programa de forma a antecipar e mitigar riscos ao longo de sua implementação.

Para um programa de adequação à Lei Geral de Proteção de Dados (LGPD), Soler (2022) propõe um conjunto estruturado de etapas que são cruciais para garantir a conformidade com os requisitos legais e promover uma gestão eficaz dos dados pessoais, sendo elas: o mapeamento, as bases legais, Gap Analysis, Análise de Riscos, Governança, Criação e Adaptação de Documentos e Conscientização. A autora afirma que não necessariamente precisam estar nesta ordem, pois o programa deverá ser personalizado conforme a demanda da empresa.

O mapeamento é a primeira etapa crucial abordada por Soler (2022) para a implementação da LGPD. Consiste em entender quais dados pessoais são tratados pela empresa, neste estudo uma empresa agropecuária, como são coletados, armazenados e utilizados. Isso inclui uma análise detalhada dos fluxos de dados, tanto físicos quanto digitais. É essencial que o profissional responsável pela proteção de dados tenha um conhecimento profundo da organização e interaja com todos os setores envolvidos para identificar e documentar as operações de tratamento de dados ainda que seja um profissional externo.

Após o mapeamento, Soler (2022) aborda a identificação das bases legais que justificam o tratamento de dados. A LGPD estabelece diversas bases legais, como consentimento, execução de contratos, cumprimento de obrigações legais e proteção ao crédito. No contexto agropecuário, é fundamental analisar cada atividade e determinar a base legal mais adequada, documentando os riscos e benefícios de cada escolha.

A Gap Analysis envolve a identificação das lacunas existentes entre as práticas atuais da empresa e as exigências da LGPD, ou seja, de forma simplificada é a técnica pela qual empresas conseguem visualizar o caminho mais curto para sair de um ponto A a um B. Constitui uma análise de riscos, por sua vez, visa avaliar os potenciais riscos associados ao tratamento de dados e desenvolver estratégias para mitigá-los. Isso inclui a criação de políticas de segurança da informação, procedimentos de resposta a incidentes e treinamento contínuo dos funcionários.

A governança em proteção de dados envolve a designação de um encarregado e a formação de um grupo de trabalho dedicado à implementação e monitoramento da LGPD. A criação de um plano de ação detalhado, que inclua políticas, procedimentos e responsabilidades claras, é essencial para garantir a conformidade contínua.

A LGPD exige a criação e adaptação de diversos documentos, como políticas de privacidade, termos de consentimento e cláusulas contratuais específicas. No setor agropecuário, é importante revisar e atualizar todos os contratos com fornecedores, parceiros e clientes para garantir que estão em conformidade com a LGPD.

Por fim a conscientização é uma etapa contínua e crucial para o sucesso do programa de adequação. Envolve a realização de treinamentos regulares, campanhas de sensibilização e a criação de uma cultura organizacional que valorize a proteção de dados. A participação ativa da alta gestão é fundamental para garantir o compromisso de toda a organização com a conformidade à LGPD.

Dessa forma, a construção de um programa de conformidade com a LGPD no setor agropecuário deve seguir os princípios e práticas delineados, refletindo as diretrizes essenciais para a adequação às normas de proteção de dados. A jornada para a conformidade é, portanto, um processo dinâmico e contínuo, que exige um esforço colaborativo e coordenado por parte de todos os níveis da organização. A análise dos desafios e das estratégias discutidas ao longo deste estudo enfatiza a necessidade de uma abordagem integrada e proativa. A implementação eficaz da LGPD não só reduz os riscos legais e operacionais,

mas também contribui para a criação de um ambiente mais transparente e seguro para o tratamento de dados pessoais.

## CONCLUSÃO

Este estudo demonstrou a importância da implementação da Lei Geral de Proteção de Dados (LGPD) para o setor agropecuário brasileiro. A análise realizada evidenciou que, embora o agronegócio seja um dos pilares da economia nacional, sua adaptação às exigências da LGPD enfrenta desafios significativos devido à diversidade de agentes envolvidos e à complexidade do setor e de suas tecnologias empregadas.

Primeiramente, destacamos que a necessidade de uma abordagem educacional robusta emerge como uma prioridade indiscutível. É imperativo que a conscientização acerca da proteção de dados seja promovida de forma abrangente em todos os níveis da cadeia produtiva agrícola. A formação contínua e a capacitação técnica são essenciais para garantir que tanto grandes corporações agrícolas quanto pequenos e médios produtores compreendam suas responsabilidades e estejam aptos a implementar práticas de conformidade com a legislação. Este esforço educativo deve ser sustentado por estratégias que abordem a diversidade do setor e suas particularidades, garantindo que a proteção de dados seja uma prioridade compartilhada por todos os agentes envolvidos.

Ademais, a modernização da agricultura brasileira, caracterizada pela adoção crescente de tecnologias emergentes, demanda uma infraestrutura robusta de segurança da informação. A agricultura de precisão e outras inovações tecnológicas, que são dependentes de dados precisos e seguros, requerem sistemas avançados para a coleta, armazenamento e processamento de informações. A integração destas tecnologias deve ser acompanhada por políticas rigorosas de proteção de dados, que assegurem a privacidade e a segurança das informações pessoais e sensíveis. O desenvolvimento de tais políticas deve considerar a evolução contínua das tecnologias e os riscos associados à sua aplicação.

No âmbito regulatório, é fundamental que o governo e as instituições competentes estabeleçam diretrizes claras e acessíveis, oferecendo suporte técnico e jurídico para auxiliar os agentes do agronegócio na implementação da LGPD. Políticas públicas e incentivos que facilitem a adaptação às novas exigências legais podem contribuir significativamente para a conformidade do

setor, promovendo uma cultura de privacidade e segurança que beneficie toda a cadeia produtiva.

Por fim, este estudo enfatiza a relevância de um esforço coletivo para superar os desafios impostos pela LGPD, visto que a proteção de dados é um componente essencial para a sustentabilidade e a competitividade do agronegócio brasileiro. As recomendações aqui apresentadas visam não apenas assegurar o cumprimento da legislação, mas também fomentar uma agricultura mais segura, eficiente e ética, alinhada com os princípios de transparência e responsabilidade.

Em suma, a aplicação da LGPD no setor agropecuário exige uma abordagem multidimensional, envolvendo educação, inovação tecnológica, apoio regulatório e cooperação entre todos os agentes. Somente através de um compromisso conjunto será possível transformar os desafios da proteção de dados em oportunidades de crescimento e desenvolvimento sustentável para o agronegócio brasileiro.

## BIBLIOGRAFIA

ALCÂNTARA, G. D. et al. Smart agriculture: Trends and opportunities for precision farming. **Sensors**, v. 21, n. 10, p. 11743, 2021.

ALVES, Fabrício da Mota. Estruturação do Cargo de DPO em entes públicos. In VAINZOF, R.; BLUM, R. M. S. O. (Org.); FABRETTI, H. (Org.). *Data Protection Officer: Teoria e Prática de Acordo com a LGPD e o GDPR*. 1. ed. São Paulo: Revista dos Tribunais, 2020. v. 1., p. 523-544.

ALVES, José Eustáquio Diniz. *A continuidade do crescimento demoeconômico e da pegada antrópica, no contexto do metabolismo entrópico, pode levar ao colapso da economia moderna*. **EcoDebate**, Rio de Janeiro, 05 abr. 2017. Disponível em: <https://www.ihu.unisinos.br/categorias/186-noticias-2017/566517-o-impressionante-crescimento-da-populacao-humana-atraves-da-historia>. Acesso em: 28 jul. 2024

ASSOCIAÇÃO BRASILEIRA DE AGRICULTURA DE PRECISÃO E DIGITAL. *Cartilha Lei Geral de Proteção de Dados Pessoais para o Setor Agropecuário: Importância, Conceitos e Recomendações*. **BRASSCOM**, 2022.

ASBRAAP, BRASSCOM, MAPA. *Cartilha Lei geral de proteção de dados pessoais para o setor agropecuário: importância, conceitos e recomendações*. Associação Brasileira de Agricultura de Precisão e Digital, 2020.

BENARDI, C.; INAMASU, R. *Agricultura de Precisão*. In: *A AGRICULTURA BRASILEIRA: DESAFIOS E PERSPECTIVAS*. **Embrapa**, 2014.

BIONI, Bruno Ricardo. *Proteção de Dados Pessoais*. **Forense**, 2 ed., 2019.

BRASIL. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. **Lei nº 13.709**, de 14 de agosto de 2018. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709). Acesso em: 14 abr. 2020.

BRASIL. *Código de Defesa do Consumidor*. **Lei nº 8.078**, de 11 de setembro de 1990. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/Leis/L8078](http://www.planalto.gov.br/ccivil_03/Leis/L8078). Acesso em: jan. 2023.

BRASIL. *Habeas Data*. **Lei nº 9.507**, de 12 de novembro de 1997. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/l9507](http://www.planalto.gov.br/ccivil_03/leis/l9507). Acesso em: jan. 2021.

BRASIL. *Lei do Acesso à Informação. Lei nº 12.527*, de 18 de novembro de 2011. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2011/lei/l12527](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527). Acesso em: jan. 2021.

BRASIL. *Lei do Cadastro Positivo. Lei nº 12.414*, de 9 de junho de 2011. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2011/lei/l12414](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414). Acesso em: jan. 2021.

BRASIL. *Marco Civil da Internet. Lei nº 12.965*, de 23 de abril de 2014. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965). Acesso em: 05 maio 2021.

CNA. *Panorama do Agro*. Disponível em: <https://www.cnabrazil.org.br/cna/panorama-do-agro>. Acesso em: 23 jul. 2024.

CNA. *PIB da Agropecuária Cresce 18,1% no Acumulado do Ano*. Disponível em: <https://www.cnabrazil.org.br/publicacoes/pib-da-agropecuaria-cresce-18-1-no-acumulado-do-ano>. Acesso em: 12 jun. 2024.

COPA-COGECA. *Código de Conduta para o Compartilhamento de Dados Agrícolas na UE*. Bruxelas: COPA-COGECA, 2018.

COPA-COGECA, Farm Europe, and CE Delft: (2018). *Sharing Agricultural Data: A Guide for European Farmers*. Brussels: COPA-COGECA, Farm Europe, and CE Delft.

European Agricultural Machinery Association. *Agriculture 4.0: The Future of Food and Farming*. CEMA. (2017).

EMBRAPA. *Avanço Tecnológico na Produção de Cana*. Disponível em: <https://www.embrapa.br/agencia-de-informacao-tecnologica/cultivos/cana/producao/avanco-tecnologico>. Acesso em: 12 jun. 2024.

FRASER, E. D.; CAMPBELL, B. M. Redefining Agriculture: Sustainable Food Systems for the Future. *Sustainability*, v. 11, n. 1, p. 142, 2019.

GASTAL, Edmundo. *Os Sistemas de Produção na Pesquisa Agropecuária*. EMBRAPA, Brasília, 1975.

HADLEY, P. *Precision Agriculture for Sustainability: A Review of Recent Advances*. *Agronomy for Sustainable Development*, v. 35, n. 4, p. 411-421, 2015.

HU, A. et al. *How 'Big Data' Can Make Big Impact: Findings from a Systematic Review and a Longitudinal Case Study*. *International Journal of Production Economics*, v. 165, p. 234-246, 2015.

IDS – Institute of Development Studies. *Ensuring Developing Countries Benefit from Big Data*. **IDS Policy Briefing**, n. 107, dez. 2015.

KLERKX, L. et al. *A Review of Farm Management Information Systems Research: Towards a New Generation of Decision Support Systems for Heterogeneous Farmers*. *Agricultural Systems*, v. 167, p. 15-32, 2019.

LEME, Carolina da Silva. *Proteção e Tratamento de Dados sob o Prisma da Legislação Vigente*. *Revista Fronteiras Interdisciplinares do Direito*, São Paulo, V.1, n. 1, 2019, p. 178-197. Disponível em: <https://revistas.pucsp.br/index.php/fid/article/view/41960>. Acesso em: 09 de julho de 2024

LIOUTAS, E. *Big Data in Agriculture: Concepts, Applications, and Challenges*. In: *Big Data*. 2019.

LYNSKEY, Orla. *The Foundations of EU Data Protection Law*. Oxford: Oxford University Press, 2015. p. 81 e 95.

MACHADO, Luciana Cristina Pinto; MARCONI, Licia Pimentel. *Estudos preliminares sobre os princípios aplicados ao tratamento de dados pessoais na Lei nº 13.709/2018 - LGPD*. Universidade do Oeste Paulista – UNOESTE, Presidente Prudente, SP.

MAIA, H. J. *Da Terra Brotando dos Dados: Uso do Big Data no Campo Promete Aumentar a Produtividade*. *Exame*, v. 48, n. 18, p. 60, 2014.

MENDES, L. S. *Privacidade, Proteção de Dados e Defesa do Consumidor: Linhas Gerais de um Novo Direito Fundamental*. São Paulo: **Saraiva**, 2014.

Parlamento Europeu e Conselho da União Europeia. *Regulamento (UE) 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção*

de Dados). Diário Oficial da União Europeia, Bruxelas, 4 maio 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679>. Acesso em: 28 junho. 2024.

Parlamento Europeu e Conselho da União Europeia. Regulamento (UE) 2018/1713, de 16 de novembro de 2018. Estabelece regras relativas ao fluxo livre de dados não pessoais na União e revoga o Regulamento (UE) nº 2016/679 (Regulamento Geral sobre a Proteção de Dados). Diário Oficial da União Europeia, Bruxelas, 19 nov. 2018. Disponível em: [URL inválido removido]. Acesso em: 28 junho. 2024.

POMPEIA, C. “Agro é tudo”: simulações no aparato de legitimação do agronegócio. *Horizontes antropológicos*, 26(56), 195-224. 1, 2020. Disponível em: <https://www.scielo.br/j/ha/a/xjhwQdTB5jVzgPqjnSCfGvQ/#>. Acesso em: 15 de junho de 2024.

SAIZ-RUBIO, A.; ROVIRA-MÁS, D. (2020). *Big data and smart agriculture: A review of the state of the art*. *Sensors*, 2019, 5405

SAIZ-RUBIO, V.; ROVIRA-MÁS, F. *From Smart Farming Towards Agriculture 5.0: A Review on Crop Data Management*. *Agronomy*, v. 10, n. 2, p. 1-21, fev. 2020. DOI: 10.3390/agronomy10020207.

SHREIBER, Anderson. Right to Privacy and Personal Data Protection in Brazilian Law. In: VICENTE, Dário Moura; CASIMIRO, Sofia de Vasconcelos (ed.). *Data Protection in the Internet*. V. 38. Cham: Springer, 2020. p.45-54, p. 46.

SILVA, Alexandre Pacheco da. Slides e material da primeira aula desenvolvidos para a apresentação para o curso de curta-duração “Proteção de Dados Pessoais”, da Direito FGV/SP. Ministrado em 10/03/2020.

SILVA, Dandara Ramos Silvestre da; SILVA, Gustavo Henrique Luz; RIBEIRO, Natália Góis; PORTO JÚNIOR, Odélio; BRAOIOS, Rafaella Resck. *Guia América Latina: Legislações de Proteção de Dados. A Year in Privacy*, n. 11/12, [Ano]. Disponível em: [https://baptistaluz.com.br/wp-content/uploads/2022/12/bluz\\_221130\\_AYIP\\_America-Latina-Legislacao-de-protecao-de-dados\\_V2.pdf](https://baptistaluz.com.br/wp-content/uploads/2022/12/bluz_221130_AYIP_America-Latina-Legislacao-de-protecao-de-dados_V2.pdf) . Acesso em: 18 março de 2024

SILVA, De Plácido e. *Vocabulário Jurídico*. 11. ed. Rio de Janeiro: Forense, 1989. v. III.

SONKA, S. T. *Big Data: Fueling the Next Evolution of Agricultural Innovation*. *Journal of Innovation Management*, v. 4, n. 1, p. 114-136, 2016.

SOLOR, Fernanda G. *Proteção de Dados: Reflexões Práticas e Rápidas sobre a LGPD*. São Paulo: **SRV Editora LTDA**, 2022. E-book. ISBN 9786553622500. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786553622500/>. Acesso em: 23 jul.

TRAN, N.; SREENATH, B.; JAIMIN, D. Designing query optimizers for big data problems of the future. *Journal Proceedings of the VLDB Endowment*, v.6, n.11, p.1168-1169,2013.2024.

UE, General Data Protection Regulation (GDPR), Regulation 2016/679. *Official Journal of the European Union*. Disponível em: <<https://eur-lex.europa.eu/eli/reg/2016/679/oj>>. Acesso em: 21 JulHO. 2024.

WAMBA, S. F.; AKTER, S.; EDWARDS, A.; CHOPIN, G.; GNANZOU, D. *How 'Big Data' Can Make Big Impact: Findings from a Systematic Review and a Longitudinal Case Study*. *International Journal of Production Economics*, v. 165, p. 234-246, 2015.

WARREN, Samuel D.; BRANDEIS, Louis D. "The Right to Privacy". *Harvard Law Review*, 4(5), 193-220, dec. 1890.

WERTHEIN, Jorge. A sociedade da informação e seus desafios. **Ciência da Informação, Brasília**, v. 29, n. 2, p. 71-77, maio/ago. 2000

Wolfert, C. *Agriculture 4.0: The future of food and farming*. CEMA. (2017).

WOLFERT, S. et al. *Applications of ICT in Agriculture in Europe: Current Status and Future Perspectives*. *Agronomy for Sustainable Development*, v. 34, n. 1, p. 197-218, 2014

DAVIS, J.; GOLDBERG, R. *A Concept of Agribusiness*. Boston: Harvard University Press, 1957.

MENDES, L. S. *Privacidade, Proteção de Dados e Defesa do Consumidor: Linhas Gerais de um Novo Direito Fundamental*. São Paulo: Saraiva, 2014.

MORAN, Daniel Keys. *The Armageddon Blues*. Berkley Books, 2011.

REALE, Miguel. *Filosofia do Direito*. 11. ed. São Paulo: Saraiva, 1986.

SHARMA, Sanjay. *Data Privacy and GDPR Handbook*. New Jersey: Wiley, 2020. p. 25-26.

VAINZOF, R. *Dados Pessoais, Tratamento e Princípios*. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coords.). *Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia*. 2. ed. São Paulo: Revista dos Tribunais, 2019. p. 33-77.

VAINZOF, R. *Estruturação do Cargo de DPO em Entes Públicos*. In: VAINZOF, R.; BLUM, R. M. S. O.; FABRETTI, H. (Orgs.). *Data Protection Officer: Teoria e Prática de Acordo com a LGPD e o GDPR*. 1. ed. São Paulo: Revista dos Tribunais, 2020. v. 1., p. 523-544.

VAINZOF, R. In: *Lei de proteção de Dados comentada*. MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coords.). São Paulo: Thomson Reuters Brasil, 2019<sup>a</sup>

VAN DER BURG, S.; WISEMAN, L.; KRKELJAS, J. Trust in farm data sharing: reflexões sobre o código de conduta da UE para a partilha de dados agrícolas. *Ethics Inf Technol*, 2020.

Uma Análise Comparativa Entre os Algoritmos de Criptografia: RSA e DSA. AllanAntonucciDuarte. 24 jul. de 2024. Disponível em: <https://pt.slideshare.net/slideshow/criptografia-rsa-57184162/57184162>. Acesso em: 22 jul. 2024.

AMAZON. What is cryptography? Amazon Web Services. Disponível em: <https://aws.amazon.com/pt/what-is/cryptography/>. Acesso em: 22 jul. 2024.

ANPD. *Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado*. Disponível em: [https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento\\_Final.pdf](https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf). Acesso em: 22 jul. 2024.

BRASIL. Tribunal de Contas da União. Boas práticas em segurança da informação. 3. ed. Disponível em: [https://www.dnocs.gov.br/php/util/downloads\\_file.php?&dir=&file=/home/util/livres/dnocs/tecnologia/Seguranca\\_da\\_Informacao/Boas\\_praticas\\_em\\_seguranca\\_da\\_informacao\\_TCU\\_3a\\_edicao.pdf](https://www.dnocs.gov.br/php/util/downloads_file.php?&dir=&file=/home/util/livres/dnocs/tecnologia/Seguranca_da_Informacao/Boas_praticas_em_seguranca_da_informacao_TCU_3a_edicao.pdf). Acesso em: 25 jul. 2024.

CLOUDFLARE. O que é controle de acesso? Cloudflare. Disponível em: <https://www.cloudflare.com/pt-br/learning/access-management/what-is-access-control/>. Acesso em: 23 jul. 2024

ICO. *How Do We Apply Legitimate Interests in Practice?*. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/>. Acesso em: 21 jul. 2024.

INSTITUTO FEDERAL DO SUL DE MINAS GERAIS. CSI - Boas práticas em segurança da informação. Disponível em: <https://portal.ifsuldeminas.edu.br/index.php/institucional-geral/5938-csi-boas-praticas-em-seguranca-da-informacao#:~:text=Boas%20pr%C3%A1ticas%20de%20seguran%C3%A7a%20da,ser%20compartilhadas%20com%20outras%20pessoas>. Acesso em: 08 jul. 2024.

LIMA, L. (2020, janeiro 13). Os 10 Princípios para tratamento de dados da LGPD. Tripla. Disponível em: <https://tripla.com.br/os-10-principios-para-tratamento-de-dados-da-lgpd/> Acesso em: 24 março. 2024.

PESTANA, M. (2020, 25 de maio). Os princípios no tratamento de dados na Lei Geral da Proteção de Dados Pessoais. Consultor Jurídico. Disponível em: <https://www.conjur.com.br/2020-mai-25/marcio-pestana-principios-tratamento-dados-lgpd/> Acesso em: 25 março. 2024.

SILVA, Daniel Neves. Pré-História: características, períodos e curiosidades. História e Mundo, [S.l.], [S.d.]. Disponível em: <https://www.historiadomundo.com.br/pre-historia>. Acesso em: 15 jan. 2024.

VELOSO, Thássius. O que é segurança da informação? Disponível em: <https://tecnoblog.net/responde/o-que-e-seguranca-da-informacao/> Publicado em: 29 out. 2010. Atualizado em: 28 fev. 2023. Acesso em: 17 jul. 2024.