
PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO

NÚCLEO DE PRÁTICA JURÍDICA COORDENAÇÃO ADJUNTA

DE TRABALHO DE CONCLUSÃO DE CURSO

ARTIGO CIENTÍFICO

# COMPLIANCE E GOVERNANÇA CORPORATIVA À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS: ENTRE A ÉTICA E A EFICIÊNCIA

ORIENTANDA: LUA HELENA DALLOCHIO

ORIENTADOR: PROF. DR. NIVALDO DOS SANTOS

GOIÂNIA

2026

LUA HELENA DALLOCHIO

# COMPLIANCE E GOVERNANÇA CORPORATIVA À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS: ENTRE A ÉTICA E A EFICIÊNCIA

Artigo apresentada à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação, da Pontifícia Universidade Católica de Goiás (PUC GOIÁS).

Prof. Orientador – Dr. Nivaldo dos Santos

GOIÂNIA

2026

LUA HELENA DALLOCHIO

**COMPLIANCE E GOVERNANÇA CORPORATIVA À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS: ENTRE A ÉTICA E A EFICIÊNCIA**

Data da Defesa: 02 de junho de 2026

BANCA EXAMINADORA

Orientador: Prof. Dr. Nivaldo dos Santos Nota:

Examinadora Convidada: Prof. Ma. Kenia Cristina Ferreira de Deus Lucena Nota:

À minha mãe, Rafaela Cobra, fonte primeira de tudo que sou, a voz que, nos momentos mais difíceis, nunca deixou de acreditar em mim, antes que eu mesma conseguisse. Aos meus avós Vera Aguiar e Edson Palley, por me ensinarem, antes de qualquer livro, o valor da integridade e da perseverança. Às minhas irmãs Frida, Suri e Alice, por tornarem mais leve o peso de crescer. A vocês, que tornaram possível não apenas este trabalho, mas a pessoa que o escreve.

Agradeço à Pontifícia Universidade Católica de Goiás (PUC Goiás) pelo apoio necessário para a realização deste trabalho, assim como às professoras e aos professores pelo compartilhamento de conhecimentos e sabedoria, sempre com tanta inspiração e paixão pelo ensino.

*“Não posso ser todas as pessoas que quero e viver todas as vidas que quero. Não posso desenvolver e mim todas as aptidões que quero. E por que eu quero? Quero viver e sentir as nuances, os tons e as variações das experiências físicas e mentais possíveis de minha existência.”*

*(Sylvia Plath)*

# COMPLIANCE E GOVERNANÇA CORPORATIVA À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS: ENTRE A ÉTICA E A EFICIÊNCIA

Lua Helena Dallochio[1]

O presente trabalho analisa a intersecção entre a Lei Geral de Proteção de Dados (LGPD), a Governança Corporativa e o *Compliance* Digital. Com a rápida transformação digital, os dados tornaram-se ativos corporativos inestimáveis, exigindo das organizações não apenas adequação normativa, mas uma reestruturação ética e gerencial profunda. O objetivo geral da pesquisa é demonstrar como a interdependência entre os programas de *compliance* e as diretrizes de governança atua como ferramenta hábil para a sustentabilidade empresarial, convertendo uma árdua obrigação legal em diferencial competitivo focado na confiança do mercado. A metodologia adotada constitui-se de uma pesquisa básica e descritiva, com abordagem qualitativa e método dedutivo, alicerçada em revisão bibliográfica e documental. O estudo discute os pilares da governança, transparência, equidade, prestação de contas (*accountability*) e responsabilidade corporativa, evidenciando que o *compliance* atua como o mecanismo pragmático de execução desses princípios. Analisa-se a dialética dos custos de implementação, que impõem desafios financeiros reais às pequenas e médias empresas (PMEs), contrapostos ao gravíssimo risco do "custo reputacional" gerado por violações de privacidade e vazamento de dados. Ademais, a pesquisa aborda frentes contemporâneas de risco tecnológico, como a cibersegurança e a opacidade de decisões automatizadas por Inteligência Artificial, que exigem governança algorítmica. Conclui-se que o *Compliance* Digital transcende a mera submissão à lei, consolidando-se como um escudo preventivo e estratégico. A *accountability* materializa a síntese exata entre a ética, ao proteger os direitos e liberdades fundamentais dos titulares, e a eficiência, ao blindar a corporação contra sanções, ratificando a integridade como pilar inegociável da perenidade empresarial na era digital.

**Palavras-chave:** *Compliance* Digital; Governança Corporativa; Lei Geral de Proteção de Dados; *Accountability*; Custo Reputacional.

[1] Acadêmica de Direito da Pontifícia Universidade Católica de Goiás, Escola de Direito, Negócios e Comunicação, cursando 9º período.

# COMPLIANCE AND CORPORATE GOVERNANCE IN LIGHT OF THE GENERAL DATA PROTECTION LAW: BETWEEN ETHICS AND EFFICIENCY


## ABSTRACT

This study analyzes the intersection between the Brazilian General Data Protection Law (LGPD), Corporate Governance, and Digital Compliance. With rapid digital transformation, data has become an invaluable corporate asset, requiring organizations to undergo not only regulatory adaptation but also profound ethical and managerial restructuring. The general objective of the research is to demonstrate how the interdependence between compliance programs and governance guidelines acts as a skillful tool for business sustainability, converting an arduous legal obligation into a competitive advantage focused on market trust. The methodology adopted consists of basic and descriptive research, with a qualitative approach and deductive method, based on bibliographic and documentary review. The study discusses the pillars of Governance, transparency, equity, accountability, and corporate responsibility, highlighting that compliance acts as the pragmatic execution mechanism for these principles. It analyzes the dialectic of implementation costs, which impose real financial challenges on small and medium-sized enterprises (SMEs), contrasted with the extremely serious risk of "reputational cost" generated by privacy violations and data breaches. Furthermore, the research addresses contemporary technological risk fronts, such as cybersecurity and the opacity of automated decisions by Artificial Intelligence, which require algorithmic governance. It concludes that Digital Compliance transcends mere compliance with the law, consolidating itself as a preventive and strategic shield. Accountability materializes the exact synthesis between ethics, by protecting the fundamental rights and freedoms of data subjects, and efficiency, by shielding the corporation against sanctions, ratifying integrity as an non-negotiable pillar of corporate longevity in the digital age.



**Keywords**: Digital Compliance; Corporate Governance; General Data Protection Law; Accountability; Reputational Cost.

## LISTA DE ABREVIATURAS E SIGLAS

| | |
|---|---|
| **ABNT** | Associação Brasileira de Normas Técnicas |
| **CGU** | Controladoria-Geral da União |
| **CVM** | Comissão de Valores Mobiliários |
| **FCPA** | Foreign Corrupt Practices Act |
| **IBGC** | Instituto Brasileiro de Governança Corporativa |
| **LGPD** | Lei Geral de Proteção de Dados |

**SUMÁRIO**

**COMPLIANCE E GOVERNANÇA CORPORATIVA À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS: ENTRE A ÉTICA E A EFICIÊNCIA** .....
**ABSTRACT**.....
**LISTA DE ABREVIATURAS E SIGLAS**.....
**INTRODUÇÃO** .....1
**1.GOVERNANÇA CORPORATIVA E COMPLIANCE: PILARES DA INTEGRIDADE EMPRESARIAL** .....2
1.1 CONCEITO E EVOLUÇÃO DA GOVERNANÇA CORPORATIVA.....2
1.1.1 Princípios fundamentais da governança corporativa: transparência, equidade, prestação de contas e responsabilidade corporativa .....3
1.2 O COMPLIANCE COMO MECANISMO DE EXECUÇÃO DA GOVERNANÇA....4
1.2.1 Origem, definição e elementos de um programa de *compliance* .....4
1.3 A INTERDEPENDÊNCIA ENTRE GOVERNANÇA E COMPLIANCE .....6
1.3.1 A Governança de Dados como Extensão da Governança Corporativa e a Base para a LGPD.....6
**2.A LGPD E O NOVO PARADIGMA DO *COMPLIANCE* DIGITAL**.....7
2.1LGPD: O MARCO LEGAL DA PROTEÇÃO DE DADOS NO BRASIL .....7
2.1.1 Fundamentos e princípios da LGPD.....8
2.2 O CONCEITO DE *COMPLIANCE* DIGITAL E GOVERNANÇA DE DADOS .....9
2.2.1 Da conformidade reativa à gestão estratégica: a LGPD como vetor de valor.....10
2.3 A RELAÇÃO ENTRE LGPD, GOVERNANÇA DE DADOS E CULTURA ÉTICA 10
**3.*COMPLIANCE* DIGITAL, CIBERSEGURANÇA E *ACCOUNTABILITY*: DA CONFORMIDADE LEGAL À GERAÇÃO DE VALOR**.....11
3.1 *COMPLIANCE* DIGITAL E CIBERSEGURANÇA COMO PILARES DA PROTEÇÃO DE DADOS NA ERA DA INTELIGÊNCIA ARTIFICIAL .....11
3.2 GESTÃO DE RISCOS, DISRUPÇÃO DIGITAL E O PAPEL DO *COMPLIANCE* NAS ORGANIZAÇÕES .....12
3.3 *ACCOUNTABILITY* COMO SÍNTESE ENTRE ÉTICA E EFICIÊNCIA: A LGPD COMO VETOR DE VALOR CORPORATIVO .....14
**CONCLUSÃO** .....16
**REFERÊNCIAS** .....17

# INTRODUÇÃO

No cenário contemporâneo, a transformação digital e a consolidação da "economia de dados" reconfiguraram as dinâmicas de mercado, elevando a informação pessoal à categoria de um dos ativos mais valiosos e cobiçados pelas organizações (Dantas Filho e Silva, 2025). Nesse contexto, a promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD: Lei nº 13.709/2018) emerge como um marco regulatório fundamental no ordenamento jurídico brasileiro, estabelecendo um novo paradigma que exige das empresas uma profunda revisão de seus processos internos e de sua cultura organizacional.

Diante da complexidade desse cenário, a integração entre a Governança Corporativa e os programas de *Compliance* desponta não apenas como uma resposta às exigências legais, mas como o modelo de gestão indispensável para garantir a sustentabilidade das corporações. Assim, o presente trabalho levanta o seguinte problema de pesquisa: de que maneira a interdependência entre Governança Corporativa e *Compliance* pode ser estrategicamente utilizada pelas empresas para promover a conformidade com a LGPD, transformando uma árdua obrigação legal em um diferencial competitivo alicerçado na prestação de contas (*accountability*)?

Para responder a essa indagação, o objetivo geral deste estudo é analisar a interrelação entre as estruturas de *Compliance* e Governança Corporativa no ambiente empresarial e demonstrar sua relevância estratégica para a efetivação das exigências da LGPD. De forma específica, o trabalho propõe-se a: a) explorar o arcabouço teórico dos princípios da governança e do *compliance* corporativo; b) analisar o impacto normativo da LGPD e as contradições envolvendo os custos de adequação versus os ganhos institucionais; e c) avaliar a implementação do *Compliance* Digital como uma ferramenta proativa para mitigar riscos oriundos da cibersegurança e da Inteligência Artificial.

Justifica-se a relevância do tema pela premente necessidade de as organizações superarem a visão antiquada do *compliance* como um mero entrave financeiro ou custo burocrático. A inobservância das normas de proteção de dados acarreta danos que ultrapassam as pesadas sanções da Autoridade Nacional de Proteção de Dados (ANPD), culminando em um gravíssimo "custo reputacional" capaz de inviabilizar a própria existência institucional (Garcia, 2024).

Metodologicamente, adota-se o método de abordagem dedutivo, partindo de premissas gerais sobre governança para a análise particular da proteção de dados. A pesquisa, de natureza básica e descritiva, utiliza-se de uma abordagem qualitativa, estruturada por meio de revisão bibliográfica e documental, com base em doutrinas, legislação e artigos científicos pertinentes.

Para a consecução dos objetivos propostos, o trabalho está estruturado em três seções de desenvolvimento, além desta introdução e das considerações finais. A primeira seção aborda os pilares da Governança Corporativa e o *Compliance* como seu mecanismo de execução. A segunda seção analisa a LGPD como o novo paradigma do *Compliance* Digital, explorando o princípio do legítimo interesse e a *accountability*. Por fim, a terceira seção discute as frentes contemporâneas de risco, notadamente a cibersegurança e a Inteligência Artificial, demonstrando como a governança algorítmica mitiga falhas éticas na era digital.

# 1. GOVERNANÇA CORPORATIVA E COMPLIANCE: PILARES DA INTEGRIDADE EMPRESARIAL

Este primeiro capítulo tem como finalidade estabelecer o arcabouço teórico conceitual necessário para a análise da Lei Geral de Proteção de Dados (LGPD) no contexto corporativo. A exposição se concentra na Governança Corporativa e no Compliance, institutos que, quando integrados, operam como pilares inseparáveis da integridade empresarial.

A articulação desses conceitos, à luz dessa premissa, é crucial para fundamentar a tese central da monografia: a de que a conformidade com a LGPD não é apenas um custo regulatório, mas sim uma manifestação da intersecção entre Ética e Eficiência que define a Governança moderna. O estudo detalhado desta fundação é indispensável para demonstrar que a proteção de dados não é um elemento isolado, mas sim a mais recente e crucial exigência do Direito Empresarial moderno, refletindo a crescente preocupação do ordenamento jurídico com a função social da empresa na era digital.

Inicialmente, a seção explorará o conceito e a evolução da Governança Corporativa, detalhando seus princípios fundamentais. Em seguida, o foco se desloca para o Compliance, definido como o principal mecanismo de execução da Governança. Serão abordados sua origem, definição, e os elementos essenciais que configuram um programa de integridade eficaz, visando a redução de riscos e a aderência ética. Por fim, o capítulo consolidará a interdependência e a sinergia entre Governança e Compliance, posicionando-os como fundamentos coesos de uma cultura empresarial baseada na ética e na eficiência, indispensável para absorver as exigências da LGPD.

## 1.1 CONCEITO E EVOLUÇÃO DA GOVERNANÇA CORPORATIVA

A Governança Corporativa não é apenas um modismo gerencial, mas um sistema formalizado e em constante evolução, “essencial para a longevidade e a sustentabilidade de qualquer organização.” (Nogueira; Campos, 2025, p. 22).

Define-se como o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas.

Em sua essência, a Governança busca mitigar os conflitos inerentes à separação entre propriedade e gestão, alinhando os interesses dos administradores aos dos proprietários e, mais recentemente, a todos os stakeholders. Esta evolução reflete uma mudança paradigmática, onde a empresa é vista como uma entidade social complexa, e não apenas um instrumento de maximização do lucro acionário. A Governança, portanto, impõe um pacto de confiança entre a gestão e a sociedade, cujo descumprimento gera riscos sistêmicos, de reputação e legal.

Historicamente, as primeiras iniciativas surgiram nos Estados Unidos na década de 1980 como uma resposta dos investidores institucionais às gestões ilícitas, o que impulsionou o movimento globalmente, especialmente a partir da crescente globalização econômica no final do século XX e início do XXI. No Brasil, a Governança ganhou destaque a partir do final dos anos 90 e 2000, estimulada por escândalos de corrupção e a necessidade de estabelecer diretrizes de gerenciamento. A Comissão de Valores Mobiliários (CVM) e o Instituto Brasileiro

de Governança Corporativa (IBGC) têm sido protagonistas na definição e disseminação dessas práticas, “cujo cerne reside na capacidade da organização de planejar, decidir, implementar, avaliar e revisar práticas para garantir sua sustentabilidade multidimensional” (Figueiredo, 2021, p. 15).

Desse modo, a evolução da Governança marca a transição de um foco estritamente acionário (*shareholder centric*) para uma visão mais ampla, que reconhece o papel social da corporação e sua interdependência com o ambiente em que está inserida. Este reconhecimento se traduz na necessidade de incorporar valores éticos e sociais, como a proteção ambiental e, indiscutivelmente, a proteção de dados pessoais, ao escopo da administração. A Governança, em sua maturidade, passa a ser vista como a arte de balancear a busca por resultados com o imperativo ético.

### 1.1.1 Princípios fundamentais da governança corporativa: transparência, equidade, prestação de contas e responsabilidade corporativa

O modelo brasileiro de Governança Corporativa, amplamente difundido pelo IBGC, estrutura-se sobre quatro pilares básicos, “que garantem a integridade e a integridade empresarial” (Nogueira; Campos, 2025, p. 25). Estes princípios não são meras sugestões de boas práticas, eles se tornam o alicerce para a materialização da integridade e da sustentabilidade jurídica e econômica da organização.

O primeiro pilar é a Transparência (*Disclosure*), que consiste na disponibilização de informações relevantes, que transcendem as exigências legais e abrangem o desempenho econômico-financeiro e outros fatores, inclusive intangíveis, que guiam a ação gerencial. No contexto da LGPD, este princípio encontra um contraponto, “pois deve ser ponderado com a necessidade de sigilo e privacidade dos dados pessoais” (Figueiredo, 2021, p. 35). A Transparência, neste cenário, se metamorfoseia em um dever de clareza (LGPD, art. 6º, VI) sobre o tratamento de dados, e não em uma simples divulgação de informações. A empresa precisa ser clara sobre como usa os dados, sem, contudo, violar o sigilo inerente à própria natureza confidencial da informação pessoal ou dos seus segredos de negócio. Trata-se de um exercício de equilíbrio hermenêutico e prático.

Em seguida, a Equidade caracteriza-se pelo tratamento justo e isonômico de todos os stakeholders (sócios, funcionários, credores, comunidade etc.), “este pilar é essencial para coibir tratamentos desiguais e reduzir a influência de fatores escusos, fortalecendo a ética na empresa” (Nogueira; Campos, 2025, p. 26). A equidade exige que os direitos dos titulares de dados, mesmo que não sejam sócios ou empregados, sejam respeitados com o mesmo rigor, impedindo que a busca por lucros utilize o dado como recurso ilimitado e desprotegido.

O terceiro princípio é a Prestação de Contas (*Accountability*), que exige que os agentes de governança assumam integralmente as consequências de seus atos e omissões, prestando contas de sua atuação de forma clara, concisa e tempestiva. A relevância deste princípio é amplificada pela LGPD, que impõe o dever de demonstrar a observância e o cumprimento das normas de proteção de dados, sendo um ponto crucial para a efetiva Governança de Dados. A *accountability* na proteção de dados não é passiva, mas ativa, exigindo a documentação e a auditabilidade de todos os processos de tratamento de dados

pessoais, desde a coleta até o descarte, conferindo à Governança um papel de constante vigilância interna.

Por fim, a Responsabilidade Corporativa impõe aos agentes o zelo pela viabilidade econômico-financeira, social e ambiental da organização, garantindo que a atividade empresarial, alinhada à função social da propriedade, atenda ao bem-estar da coletividade e não apenas ao lucro do empresário. Neste contexto, o tratamento ético e legal dos dados pessoais emerge como um valor não apenas regulatório, mas social, intrínseco à sustentabilidade do negócio e à sua função social.

Neste sentido, a doutrina assevera que a união de tais pilares é a própria chave da perenidade empresarial:

> A boa governança corporativa, lastreada nos seus princípios basilares de transparência, equidade, *accountability* e responsabilidade corporativa, é a garantia de que a corporação não apenas busca o lucro a curto prazo, mas se estrutura de forma a sobreviver e prosperar em um ambiente de crescentes exigências éticas e regulatórias. Quando aplicada ao universo de dados, ela transforma a proteção da privacidade de um fardo em um diferencial estratégico, essencial para a construção da confiança. A negligência com estes pilares, em especial a *accountability*, é o caminho mais rápido para a perda de reputação e a aplicação de sanções, demonstrando o custo da má gestão, que é sempre superior ao custo da conformidade. (Figueiredo, 2021, p. 60).

## 1.2 O COMPLIANCE COMO MECANISMO DE EXECUÇÃO DA GOVERNANÇA

O Compliance, que significa agir de acordo com a lei, uma instrução interna, um comando ou uma conduta ética, “atua como o principal instrumento de execução e materialização das diretrizes e princípios estabelecidos pela Governança” (Nogueira; Campos, 2025, p. 28).

Se a Governança é a inteligência estratégica que define o 'o quê' ético-legal da empresa, o *Compliance* é a inteligência operacional que define o 'como' esse desígnio será alcançado e mantido. O programa de *Compliance* traduz a filosofia da Governança em normas, procedimentos e controles práticos, garantindo que o comportamento diário de cada colaborador reflita o *Tone from the Top* estabelecido pela alta direção.

### 1.2.1 Origem, definição e elementos de um programa de *compliance*

O conceito moderno de *Compliance* tem suas raízes no contexto internacional, ganhando impulso em resposta a práticas ilícitas e escândalos corporativos, sendo o Foreign Corrupt Practices Act - FCPA dos EUA (1977) um marco significativo. No Brasil, a matéria foi formalizada pela Lei nº 12.846/2013 (Lei Anticorrupção), cujo regulamento, o Decreto nº 8.420/2015, destaca a importância dos programas de integridade (o termo legal para

compliance) “ao prever que sua existência e efetividade são levadas em conta na aplicação de sanções” (Tomazette, 2017, p. 55).

O Compliance, todavia, é mais do que a mera obediência à lei, ele busca a criação de uma cultura ética e de autorregulação na empresa, manifestando-se como um conjunto de controles internos que reforça a regulação estatal e auxilia os agentes econômicos a se manterem em conformidade com suas políticas corporativas (Nogueira; Campos, 2025, p. 30).

Tal perspectiva afasta o *Compliance* da mera legalidade formal e o aproxima da Ética Prática, estabelecendo um código de conduta que, muitas vezes, é mais rigoroso do que a lei em sentido estrito. Essa é a essência do conceito de Integridade Empresarial.

O foco se desloca da punição para a prevenção, mediante a internalização de valores:

> O verdadeiro propósito do *Compliance* é criar um ambiente onde a transgressão seja inaceitável. Para que se obtenha uma efetiva cultura de Compliance, a organização deve ir além da mera imposição de normas, buscando a internalização dos valores éticos pelos colaboradores, transformando a disciplina em um valor intrínseco e não apenas uma obrigação exógena. (Souza, 2022, p. 15).

Para que seja robusto e eficaz na prevenção, detecção e resposta a irregularidades, um programa de *Compliance* deve possuir elementos essenciais, conforme as diretrizes da Controladoria Geral da União (CGU). O Comprometimento da Alta Direção (Tone from the Top) é o elemento crucial e indispensável, visto que o apoio visível e inequívoco da liderança é que confere seriedade e garante o sucesso do programa. Este comprometimento se materializa através da elaboração de Padrões de Conduta e Códigos de Ética claros, aplicáveis a todos os níveis. O Código de Ética, por exemplo, não é apenas um documento protocolar; ele serve como a tradução formal dos princípios de Governança para a conduta diária, sendo o ponto de partida para qualquer programa de integridade, incluindo o de privacidade.

Além disso, a Análise e Gestão de Riscos (Risk Assessment) é fundamental, pois permite a identificação, o mapeamento e a mitigação proativa dos riscos aos quais a empresa está suscetível, sendo uma estratégia eficaz de gestão administrativa. Este componente é vital no contexto da LGPD, pois exige a aplicação de uma metodologia específica para riscos de privacidade, culminando, quando necessário, na elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD).

O ciclo se completa com a Difusão da Cultura Ética por meio de treinamentos e comunicação contínua, o estabelecimento de Canais de Denúncia abertos e com proteção ao denunciante, e o Monitoramento e Auditoria Contínua para a verificação constante da aplicação e atualização do programa com base em falhas e desempenho.

É crucial salientar, ademais, a conexão do *Compliance* com o Direito Penal, especialmente o denominado Criminal Compliance. Embora o foco da LGPD seja administrativo, a cultura de *compliance* surge, em grande parte, para prevenir ilícitos graves. A ausência de um programa de integridade eficaz pode, em tese, ter implicações na avaliação

da culpabilidade e das sanções aplicáveis, reforçando a seriedade com que a organização deve encarar suas obrigações, incluindo as relativas à proteção de dados.

## 1.3 A INTERDEPENDÊNCIA ENTRE GOVERNANÇA E COMPLIANCE

A relação entre Governança Corporativa e Compliance transcende a mera coexistência, configurando-se como um vínculo de codependência e sinergia indispensável para a consolidação da integridade empresarial. Em essência, a Governança define a filosofia, os princípios éticos e os objetivos estratégicos da organização, estabelecendo o "o quê" e o "porquê" da conduta corporativa. Por sua vez, o Compliance atua como o mecanismo de execução e instrumentalização, garantindo que esses princípios sejam aplicados e monitorados no cotidiano operacional, representando o "como" essa integridade é alcançada.

A união dessas estruturas promove a integridade e resulta em benefícios mútuos e mensuráveis para a companhia. Primeiramente, a combinação de uma governança robusta com um *Compliance* efetivo resulta em Maior Performance e Valor para a empresa, que demonstra melhor desempenho operacional e constrói uma imagem positiva e longeva no mercado.

Em segundo lugar, a gestão de riscos inerente ao *Compliance* atua como uma blindagem proativa, promovendo a Mitigação de Riscos e Sanções, reduzindo a probabilidade de fraudes, ilícitos e, consequentemente, minimizando as penalidades legais. Conforme observado, “uma empresa em *compliance* mostra que seus procedimentos são transparentes e são dominados por profissionais eficientes, com capacidade madura de gestão” (RSDE, 2023, p. 139). Esta maturidade de gestão, demonstrada pela eficácia do programa de Compliance, é o que traduz a Ética em Eficiência e, por consequência, em valor de mercado.

Por fim, essa atuação conjunta garante a Sustentabilidade Empresarial ao assegurar a conformidade com as regras que abrangem a responsabilidade social, ambiental e, de forma crescente, a LGPD, contribuindo decisivamente para a longevidade e perenidade da organização no mercado. A materialização dessa interdependência na Era da Informação é o que justifica o surgimento e a importância do *Compliance* Digital ou *Compliance* de Privacidade. Este não é apenas um módulo do *Compliance* geral, mas uma especialização vital que lida diretamente com o ativo mais estratégico da economia atual: o dado pessoal.

### 1.3.1 A Governança de Dados como Extensão da Governança Corporativa e a Base para a LGPD

A transição para a Governança de Dados é o ápice da discussão deste capítulo. Ela representa a extensão da Governança Corporativa e do *Compliance* tradicionais para o ambiente cibernético e regulatório da LGPD. Se a Governança define a estratégia e o *Compliance* a tática de integridade, a Governança de Dados define as regras de posse, uso, proteção e descarte dos dados pessoais.

A LGPD transformou a proteção de dados de uma obrigação regulatória em um verdadeiro pilar estratégico, exigindo a alocação de recursos, a designação de um Encarregado de Dados (DPO) e a criação de políticas internas que reflitam os princípios de boa-fé, finalidade e necessidade (LGPD, Art. 6º).

> No cenário da Lei Geral de Proteção de Dados, a governança é fundamental para estabelecer o tom ético e os direcionadores estratégicos, enquanto o *compliance* digital é o programa que materializa as exigências de segurança e privacidade. Sem o comando de uma, a outra é cega; sem a execução da outra, a primeira é vazia. A união é a única via para alcançar a *accountability* exigida pela legislação de dados. O *Compliance* Digital, portanto, é a resposta operacional da Governança Corporativa à necessidade de se proteger o direito fundamental à privacidade. (Cavalieri, 2020, p. 15, adaptado).

Neste sentido, a integração entre a ética corporativa (Governança) e a conformidade específica (*Compliance* de Privacidade) é o que permite à organização gerenciar o risco legal de forma eficiente. O TCC se debruçará sobre como esta estrutura de dupla finalidade – a Ética como valor intrínseco e a Eficiência como resultado mensurável – é o único caminho para a sustentabilidade jurídica e mercadológica sob a égide da LGPD. Este é o fundamento essencial que liga as bases teóricas à análise prática que se desenvolverá nos próximos capítulos.

## 2. A LGPD E O NOVO PARADIGMA DO *COMPLIANCE* DIGITAL

O presente capítulo tem por objetivo analisar o arcabouço normativo da Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018), posicionando-a como o marco legal que instituiu no Brasil um novo paradigma de conformidade, o *Compliance* Digital. Para tanto, parte-se da compreensão do direito fundamental à proteção de dados, passa-se pelos princípios e figuras centrais da lei e culmina-se na análise da Governança de Dados como instrumento estratégico de valor corporativo.

A digitalização acelerada da economia e a massificação do tratamento de dados pessoais por empresas e pelo Estado tornaram urgente a criação de um regime jurídico específico. Conforme apontam Dantas Filho e Silva (2025, p. 37), a LGPD representa não apenas uma resposta regulatória a pressões internacionais, mas uma transformação estrutural das relações entre titulares, controladores e operadores de dados no ambiente corporativo brasileiro, impondo novos deveres e criando um vocabulário jurídico para as organizações.

### 2.1 LGPD: O MARCO LEGAL DA PROTEÇÃO DE DADOS NO BRASIL

A Lei nº 13.709/2018, promulgada em 14 de agosto de 2018 e vigente desde setembro de 2020, representa o principal marco normativo brasileiro em matéria de proteção de dados pessoais. Sua inspiração declarada, remonta ao Regulamento Geral de Proteção de Dados europeu (GDPR), sem, contudo, reproduzir acriticamente o modelo estrangeiro, uma vez que se adaptou à realidade jurídica, institucional e econômica nacional.

A proteção de dados pessoais foi elevada ao status de direito fundamental pelo art. 5º, LXXIX, da Constituição Federal de 1988, introduzido pela Emenda Constitucional nº 115/2022. Assim, o dado pessoal deixou de ser tratado como mero insumo econômico para se tornar objeto de tutela constitucional, vinculando não apenas o Estado, mas também os agentes privados que operam no mercado.

A lei estrutura-se sobre o conceito central de dado pessoal, definido em seu art. 5º, I, como qualquer informação relacionada a pessoa natural identificada ou identificável. Além disso, distingue os dados pessoais sensíveis – aqueles referentes à origem racial, convicção religiosa, opinião política, saúde, vida sexual e dados genéticos ou biométricos – que recebem tratamento mais rigoroso em razão do potencial discriminatório que carregam (LGPD, art. 5º, II). Segundo Souza (2022, p. 10), essa distinção é "fundamentalmente relevante para a calibração dos riscos e das salvaguardas a serem implementadas pelos programas de *compliance* de privacidade".

A estrutura dos agentes de tratamento, composta pelo controlador e pelo operador, é outro pilar central da lei. O controlador é a pessoa natural ou jurídica a quem competem as decisões referentes ao tratamento dos dados (art. 5º, VI), ao passo que o operador realiza o tratamento em nome do controlador (art. 5º, VII). Ambos respondem solidariamente pelos danos decorrentes do tratamento inadequado, nos termos dos arts. 42 a 45 da LGPD, o que impõe às organizações a necessidade de mapeamento rigoroso de suas cadeias de tratamento.

A figura do Encarregado de Dados, ou *Data Protection Officer* (DPO), prevista no art. 41, representa a personificação do *Compliance* Digital dentro da estrutura organizacional. Trata-se de um elo indispensável entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), responsável por receber comunicações, orientar sobre a aplicação da lei e promover a cultura de proteção de dados internamente. Cavalieri (2020, p. 12) destaca que o DPO "não é apenas um cargo técnico, mas uma função de governança que deve estar integrada à estratégia de integridade da organização".

### 2.1.1 Fundamentos e princípios da LGPD

O art. 6º da LGPD elenca dez princípios que devem reger toda e qualquer atividade de tratamento de dados pessoais, sob a observância da boa-fé. Esses princípios não são meramente programáticos, possuem força normativa direta e servem de parâmetro tanto para a atuação da ANPD quanto para a responsabilização judicial e administrativa dos agentes de tratamento.

O princípio da finalidade (art. 6º, I) exige que o tratamento sirva a propósitos legítimos, específicos e informados ao titular, vedando o reaproveitamento dos dados para fins incompatíveis com o originalmente declarado. A adequação (art. 6º, II) complementa a finalidade ao exigir compatibilidade entre o tratamento e o contexto em que os dados foram coletados. Já a necessidade (art. 6º, III) limita o tratamento ao mínimo indispensável para a realização das finalidades declaradas, operacionalizando o princípio da minimização de dados consagrado no GDPR europeu.

Os princípios da transparência (art. 6º, VI) e do livre acesso (art. 6º, IV) garantem ao titular o direito de conhecer como seus dados são tratados, com quem são compartilhados e por quanto tempo são retidos. Esses princípios dialogam diretamente com o pilar da Transparência da Governança Corporativa, demonstrando que a LGPD não é um sistema paralelo, mas uma extensão normativa dos valores já consolidados pela literatura de Governança.

O princípio da segurança (art. 6º, VII) impõe a adoção de medidas técnicas e administrativas para proteger os dados de acessos não autorizados, destruição, perda, alteração

ou comunicação indevida. Conforme assinala Garcia (2024, p. 52), "a cibersegurança é o braço operacional do princípio da segurança, traduzindo-se em investimentos em infraestrutura, políticas de controle de acesso e planos de resposta a incidentes". A ausência dessas medidas não apenas expõe a organização a sanções administrativas, mas gera o chamado custo reputacional, cuja mensuração tende a superar os valores das multas aplicadas.

Por fim, o princípio da responsabilização e prestação de contas (art. 6º, X), *accountability,* é o mais relevante para a presente análise. Ele não se satisfaz com o mero cumprimento das normas; exige a demonstração ativa e documentada de que as obrigações estão sendo efetivamente observadas. Nas palavras de Souza (2022, p. 24):

O dever de accountability impõe às organizações que, além de alterar suas rotinas em fluxos de tratamentos de dados pessoais, providenciem a estruturação de um verdadeiro programa de compliance com foco nos dados pessoais, de modo a demonstrar efetivamente sua implementação por meio de registros robustos e coerentes de atividades voltadas à proteção de dados pessoais.

É esse princípio que conecta, de forma indissolúvel, a LGPD à estrutura de Governança Corporativa analisada no capítulo anterior, transformando a conformidade em um ativo intangível mensurável e estrategicamente valioso.

## 2.2 O CONCEITO DE *COMPLIANCE* DIGITAL E GOVERNANÇA DE DADOS

O *Compliance* Digital, também denominado *Compliance* de Privacidade ou *Privacy Compliance*, pode ser definido como o conjunto estruturado de políticas, processos, controles e práticas adotadas por uma organização para assegurar a conformidade com a legislação de proteção de dados, as regulamentações setoriais e os padrões internacionais de boas práticas em segurança da informação. Lóssio (2020, p. 45) o conceitua como "a adaptação do *compliance* tradicional às especificidades da sociedade da informação, onde o dado pessoal ocupa posição central tanto no modelo de negócio quanto na exposição a riscos".

A Governança de Dados, por sua vez, representa a dimensão estratégica desse processo, correspondendo ao conjunto de políticas, padrões e processos que determinam como os dados serão coletados, armazenados, utilizados, protegidos e descartados. Cavalieri (2020, p. 8) a define como "um ramo da governança voltado especificamente para a seara da proteção de dados pessoais, cujo desiderato maior está intrinsecamente ligado ao da governança de maneira geral: ações alinhadas ao interesse público e privado, com uma melhor e mais eficiente condução dos processos organizacionais". Bastos, Dias e Postal (2023, p. 4) destacam que o *Compliance* Digital não se restringe à adequação à LGPD, mas abrange um espectro mais amplo de inovações tecnológicas, incluindo a computação em nuvem, a inteligência artificial e o uso massivo de *big data*, todos com implicações diretas sobre os direitos dos titulares de dados. Os autores assinalam que:

> A inovação tecnológica impõe à organização o dever contínuo de revisão de seus programas de conformidade, uma vez que novos vetores de risco surgem com velocidade superior à capacidade regulatória do Estado. O *Compliance* Digital eficaz é, portanto, aquele que antecipa

> riscos ao invés de apenas reagir a sanções, operando como instrumento proativo de integridade.

Nesse contexto, a Governança de Dados materializa-se em elementos concretos: o mapeamento de dados (*data mapping*), que identifica todos os fluxos de informações pessoais na organização; a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), previsto no art. 38 da LGPD; a instituição de políticas de retenção e descarte; e a implementação de mecanismos de resposta a incidentes de segurança, conforme exigido pelo art. 48 da lei.

Campos e Carreiro (2024, p. 12) sublinham que, em tempos de disrupção digital, "a gestão de riscos deixou de ser uma função de suporte para se tornar uma competência essencial da liderança corporativa". As organizações que institucionalizam a Governança de Dados como parte integrante de sua estratégia corporativa demonstram maior resiliência diante de crises de privacidade e, consequentemente, preservam com mais eficácia sua reputação e seu valor de mercado.

### 2.2.1 Da conformidade reativa à gestão estratégica: a LGPD como vetor de valor

Por muito tempo, o *compliance* foi percebido pelas organizações como um custo inevitável da atividade regulada, uma obrigação imposta de fora para dentro, sem retorno mensurável. Essa perspectiva reativa, contudo, revelou-se equivocada à luz da experiência acumulada desde a vigência do GDPR na Europa e, mais recentemente, da LGPD no Brasil.

A conformidade proativa com a LGPD, estruturada sobre os pilares da Governança de Dados, transforma-se em diferencial competitivo. Dantas Filho e Silva (2025, p. 38) apontam que organizações com programas maduros de *compliance* de privacidade apresentam vantagens concretas: maior facilidade de acesso a mercados internacionais que exigem adequação às normas de proteção de dados; preferência por parte de consumidores e parceiros comerciais conscientes sobre privacidade; e menor exposição a sanções administrativas que podem alcançar, nos termos do art. 52 da LGPD, até R$ 50 milhões por infração.

A conformidade com a LGPD representa, portanto, uma oportunidade de construção de valor intangível. A confiança do titular no controlador, quando conquistada por meio de práticas transparentes e responsáveis, converte-se em ativo reputacional de difícil replicação. Conforme observa Garcia (2024, p. 55), "o custo reputacional de um incidente de segurança pode ser de 10 a 100 vezes superior ao custo das medidas preventivas que teriam evitado o evento", o que demonstra, com clareza, que a eficiência e a ética são indissociáveis na gestão de dados pessoais.

## 2.3 A RELAÇÃO ENTRE LGPD, GOVERNANÇA DE DADOS E CULTURA ÉTICA

A conformidade com a LGPD não se realiza por meio de documentos ou políticas isoladas. Ela exige, em sua essência, uma transformação cultural que permeie todos os níveis hierárquicos da organização. Assim como o *Compliance* Anticorrupção, analisado no primeiro capítulo, depende da internalização de valores éticos para ser efetivo, o *Compliance* Digital só produz resultados sustentáveis quando integrado à cultura organizacional.

Lóssio (2020, p. 62) argumenta que a proteção de dados pessoais na sociedade da informação deve ser compreendida não apenas como uma exigência legal, mas como uma expressão do respeito à dignidade humana. Quando as organizações internalizam essa perspectiva, o *Compliance* Digital deixa de ser um conjunto de procedimentos burocráticos e passa a ser uma manifestação concreta dos valores que sustentam a empresa.

A cultura de proteção de dados se constrói, na prática, por meio de treinamentos regulares das equipes, da clareza nas políticas internas, do engajamento da alta liderança (tone from the top) e da criação de canais seguros para reportar incidentes e dúvidas. Bastos, Dias e Postal (2023, p. 7) reforçam que "a tecnologia sozinha não protege dados; é a combinação de pessoas capacitadas, processos bem desenhados e ferramentas adequadas que constitui uma defesa eficaz".

Nesse sentido, a LGPD e a Governança Corporativa convergem para um mesmo ponto: a criação de organizações dignas de confiança. A empresa que trata dados pessoais com respeito, transparência e responsabilidade não apenas cumpre a lei, ela demonstra, em sua conduta cotidiana, que a ética é parte integrante de seu modelo de negócio. É sobre esse fundamento que o capítulo seguinte analisará as ferramentas concretas do *Compliance* Digital na era da inteligência artificial e da cibersegurança.

## 3. *COMPLIANCE* DIGITAL, CIBERSEGURANÇA E *ACCOUNTABILITY*: DA CONFORMIDADE LEGAL À GERAÇÃO DE VALOR

O terceiro e último capítulo desta monografia tem por finalidade integrar os aportes teóricos construídos nos capítulos anteriores com as ferramentas concretas e os desafios emergentes do *Compliance* Digital na contemporaneidade. Para tanto, examina-se a relação entre a cibersegurança e a proteção de dados, analisa-se o impacto da inteligência artificial sobre o tratamento de dados pessoais e as respostas do compliance, e demonstra-se de que modo a *accountability* constitui a síntese operacional entre a ética e a eficiência corporativa.

A convergência entre a Governança Corporativa, a LGPD e as novas tecnologias impõem às organizações a necessidade de repensar continuamente seus programas de integridade. Campos e Carreiro (2024, p. 3) afirmam que "a inovação e a disrupção digital redefiniram o ambiente de risco corporativo, tornando o *compliance* uma função estratégica e não mais apenas uma exigência regulatória". Esse reposicionamento transforma o *Compliance* Digital em um vetor de vantagem competitiva, capaz de gerar valor real e mensurável para as organizações.

### 3.1 *COMPLIANCE* DIGITAL E CIBERSEGURANÇA COMO PILARES DA PROTEÇÃO DE DADOS NA ERA DA INTELIGÊNCIA ARTIFICIAL

A cibersegurança constitui o fundamento técnico do *Compliance* Digital. Enquanto o *compliance* estabelece as políticas, os processos e as responsabilidades relacionadas à proteção de dados, a cibersegurança fornece as ferramentas e os controles técnicos necessários para tornar essas políticas efetivas no ambiente digital. Trata-se, portanto, de uma relação de complementaridade indispensável.

Garcia (2024, p. 51) conceitua a cibersegurança no contexto do *compliance* como "o conjunto de práticas, tecnologias e processos destinados a proteger sistemas, redes e dados de ataques, danos ou acessos não autorizados, com impacto direto sobre a reputação e o valor de mercado das organizações". O autor ressalta que o custo reputacional de um vazamento de dados, que inclui perda de clientes, queda do valor das ações, litígios e sanções regulatórias, invariavelmente supera o investimento que teria sido necessário para preveni-lo.

Nesse cenário, a emergência da inteligência artificial (IA) como ferramenta amplamente utilizada no tratamento de dados pessoais representa um novo e complexo desafio para o *Compliance* Digital. Os sistemas de IA aprendem a partir de grandes volumes de dados, muitas vezes sem que os titulares tenham consciência da extensão do uso de suas informações. Cecyn (2023, p. 18) alerta que "os riscos emanados por sistemas de inteligência artificial no tratamento de dados pessoais incluem a perpetuação de vieses discriminatórios, a tomada de decisões automatizadas sem supervisão humana adequada e a dificuldade de rastreabilidade dos processos decisórios".

A LGPD, ao prever no art. 20 o direito do titular à revisão de decisões tomadas exclusivamente com base em tratamento automatizado, antecipou parte dessa problemática. No entanto, o ritmo de evolução tecnológica é significativamente superior à capacidade de atualização normativa. Diante disso, o programa de *Compliance* Digital eficaz deve incorporar protocolos específicos para o uso de IA incluindo avaliações de impacto sobre privacidade (*Privacy Impact Assessment* – PIA), auditorias de algoritmos e mecanismos de explicabilidade das decisões automatizadas.

Cecyn (2023, p. 22) propõe que o programa de *compliance* seja estruturado para funcionar como uma barreira proativa diante dos riscos da IA contemplando:

> A realização de avaliações de risco específicas para sistemas de IA antes de sua implantação; a definição clara de responsabilidades entre controlador e operador nos processos automatizados; a implementação de mecanismos de auditoria e revisão periódica dos modelos de IA; e o estabelecimento de canais transparentes de comunicação com os titulares sobre o uso de tecnologias de automação em decisões que os afetem.

Bastos, Dias e Postal (2023, p. 6) acrescentam que a proteção de dados na era da IA exige, além das medidas técnicas tradicionais, o desenvolvimento de uma cultura organizacional de privacidade *by design* – conceito segundo o qual a proteção de dados deve ser incorporada ao processo de desenvolvimento de produtos e serviços desde a sua concepção, e não apenas acrescentada como camada posterior de conformidade.

## 3.2 GESTÃO DE RISCOS, DISRUPÇÃO DIGITAL E O PAPEL DO *COMPLIANCE* NAS ORGANIZAÇÕES

A gestão de riscos constitui o eixo operacional do *Compliance* Digital. Em um ambiente de crescente disrupção tecnológica, a identificação, avaliação e mitigação de riscos

relacionados ao tratamento de dados pessoais tornou-se uma competência crítica para qualquer organização que opere com informações de terceiros.

Campos e Carreiro (2024, p. 7) identificam três categorias principais de riscos no contexto do *compliance* digital: o risco regulatório, decorrente do descumprimento de obrigações legais e que pode resultar em sanções administrativas, multas e restrições operacionais; o risco operacional, associado a falhas técnicas, vulnerabilidades de sistemas e erros humanos que comprometam a integridade dos dados; e o risco reputacional, que emerge da perda de confiança dos titulares, clientes e parceiros comerciais em razão de incidentes de segurança ou práticas inadequadas de tratamento de dados.

A gestão eficaz desses riscos requer metodologias estruturadas. O Relatório de Impacto à Proteção de Dados Pessoais (RIPD), previsto no art. 38 da LGPD e regulamentado pela Resolução CD/ANPD nº 2/2022, é o principal instrumento formal de avaliação de risco no ordenamento brasileiro. Trata-se de documento que descreve os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como as medidas e salvaguardas adotadas para mitigá-los.

Dantas Filho e Silva (2025, p. 39) observam que a adoção do RIPD, embora não seja obrigatória para todos os tipos de tratamento, revela-se estrategicamente recomendável mesmo quando facultativa, pois constitui evidência documentada do cumprimento do princípio da *accountability*. Os autores destacam que organizações que elaboram RIPDs de forma proativa demonstram maturidade em sua governança de dados e tendem a receber tratamento mais favorável por parte da ANPD em eventual processo administrativo.

A disrupção digital, por sua vez, impõe ao *compliance* a necessidade de atualização contínua. O surgimento de novas tecnologias, como a computação em nuvem, a internet das coisas (IoT), o *blockchain* e a inteligência artificial, cria permanentemente cenários de risco que os programas de conformidade precisam absorver. Conforme apontam Campos e Carreiro (2024, p. 14), "o *compliance* digital eficaz é aquele que possui mecanismos de monitoramento contínuo e revisão periódica, capazes de identificar e responder a novas ameaças antes que estas se materializem em incidentes".

Lóssio (2020, p. 78) reforça esse argumento ao afirmar que a proteção de dados na sociedade da informação não pode ser tratada como um projeto com início, meio e fim, mas como um programa permanente de gestão de riscos, que acompanha a evolução tecnológica e regulatória e se adapta continuamente à realidade operacional da organização. Essa perspectiva é coerente com o requisito previsto no art. 50, §2º, VIII, da LGPD, que exige que o programa de governança em privacidade seja "atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas".

Nesse contexto, o papel do *compliance* deixa de ser meramente reativo – respondendo a incidentes após sua ocorrência – e passa a ser essencialmente preventivo, atuando como um sistema de inteligência organizacional que antecipa riscos e preserva o valor da empresa no longo prazo.

## 3.3 *ACCOUNTABILITY* COMO SÍNTESE ENTRE ÉTICA E EFICIÊNCIA: A LGPD COMO VETOR DE VALOR CORPORATIVO

O princípio da *accountability*, que percorre este trabalho desde sua análise no âmbito da Governança Corporativa até sua positivação na LGPD, representa a síntese conceitual entre a ética e a eficiência que a presente monografia se propôs a demonstrar. Não se trata de um princípio abstrato ou meramente declaratório; a *accountability* é, em essência, um compromisso de demonstração ativa, contínua e verificável da conformidade.

Souza (2022, p. 25) resume com precisão a dimensão operacional desse princípio: "a *accountability* exige que as organizações construam e mantenham um ecossistema documentado de conformidade, composto por políticas, procedimentos, registros de atividades de tratamento, relatórios de impacto, registros de incidentes, treinamentos realizados e evidências de revisões periódicas do programa". Cada um desses elementos representa, simultaneamente, uma obrigação ética e um instrumento de eficiência operacional.

A convergência entre ética e eficiência se manifesta de forma especialmente clara na gestão do custo reputacional. Garcia (2024, p. 58) demonstra que organizações com programas de *compliance* digital maduros e certificados sofrem impactos reputacionais significativamente menores em caso de incidentes de segurança, pois são capazes de demonstrar que agiram com diligência e boa-fé no tratamento dos dados. Essa capacidade de demonstração – que é, em essência, *accountability* – transforma o *compliance* em escudo reputacional e, consequentemente, em ativo financeiro.

A LGPD, ao prever em seu art. 52 um rol de sanções que inclui advertência, multa simples de até 2% do faturamento limitada a R$50 milhões por infração, multa diária, publicização da infração, bloqueio e eliminação de dados, além da suspensão parcial do banco de dados, cria um sistema de incentivos que torna a conformidade economicamente racional. A análise custo-benefício é inequívoca: o investimento em *compliance* digital é substancialmente inferior ao custo potencial das sanções e, sobretudo, do dano reputacional decorrente de um incidente.

Dantas Filho e Silva (2025, p. 40) acrescentam que, no mercado global, a conformidade com padrões elevados de proteção de dados tornou-se critério de seleção para parcerias comerciais e contratos com entidades públicas e privadas. Empresas que não demonstram adequação à LGPD são progressivamente excluídas de cadeias de fornecimento e de oportunidades de negócio, o que confere ao *compliance* digital uma dimensão de competitividade que vai muito além da mera evitação de sanções.

Cecyn (2023, p. 30) sintetiza esse raciocínio ao afirmar que o programa de *compliance* como medida de prevenção e mitigação de riscos no tratamento de dados pessoais:

> Não é apenas uma resposta à regulação estatal, mas uma afirmação dos valores da organização perante seus stakeholders. A empresa que protege dados com rigor e transparência comunica ao mercado que respeita as pessoas com quem se relaciona, construindo assim uma

> reputação de integridade que se converte, no longo prazo, em vantagem competitiva sustentável e em valor corporativo real.

É nesse sentido que a tese central desta monografia encontra sua confirmação: a interdependência entre Governança Corporativa e *Compliance* não é apenas uma conveniência teórica, mas uma necessidade prática que se torna ainda mais evidente no contexto da LGPD. A ética, operacionalizada pela Governança, e a eficiência, materializada pelo *Compliance* Digital, são faces indissociáveis de um mesmo compromisso com a sustentabilidade corporativa na era da informação.

A *accountability* é o ponto de confluência dessas duas dimensões: é ética porque exige transparência e responsabilidade perante os titulares de dados e a sociedade; é eficiência porque reduz riscos, preserva valor e consolida a reputação da organização no longo prazo. Demonstrar que se é confiável não é apenas uma obrigação legal, é o fundamento de qualquer modelo de negócio sustentável na economia digital.

## CONCLUSÃO

O percurso analítico traçado ao longo deste trabalho permite afirmar, com sólido fundamento teórico, que a Lei Geral de Proteção de Dados (LGPD) não instituiu uma nova obrigação legal isolada, mas sim incorporou ao Direito Empresarial brasileiro a proteção da privacidade como um valor estratégico indissociável da Governança Corporativa. A interdependência entre Governança e *Compliance* provou-se não apenas uma conveniência teórica, mas uma exigência prática para a sobrevivência das organizações na economia digital.

Ao longo do primeiro capítulo, demonstrou-se que os pilares da governança encontram sua materialização por meio dos programas de *compliance*. No segundo capítulo, a análise crítica da LGPD revelou um cenário dialético: se, por um lado, a conformidade normativa impõe altos custos estruturais, punindo especialmente as Pequenas e Médias Empresas (PMEs) com o ônus de contratação de profissionais qualificados (Souza, 2022); por outro, a ausência de adequação expõe as corporações a um "custo reputacional" devastador, capaz de aniquilar a confiança de investidores e consumidores (Garcia, 2024).

Ademais, o terceiro capítulo evidenciou que a disrupção tecnológica, capitaneada pela Inteligência Artificial e pela hiperconectividade, redefiniu o ambiente de risco corporativo. A delegação de decisões a algoritmos opacos frequentemente gera vieses e tratamentos discriminatórios que ferem as garantias fundamentais dos titulares (Cecyn, 2023). Frente a essa vulnerabilidade, o *Compliance* Digital transcende a mera postura reativa e assume o papel de escudo preventivo, exigindo das empresas a adoção de medidas contínuas, como o Relatório de Impacto à Proteção de Dados (RIPD) e a segurança cibernética estruturada desde o *design*.

Conclui-se, portanto, que a adequação à LGPD ressignifica a proteção de dados, alçando-a de um mero custo de adequação para um verdadeiro ativo intangível. A *Accountability* (prestação de contas e responsabilização) consolida-se como a síntese perfeita desta dinâmica: ela é estritamente ética, pois devolve ao titular a dignidade e o controle sobre suas informações; e é essencialmente eficiente, pois blinda o caixa da empresa contra multas e litígios. O *compliance*, enfim, comprova que no moderno mercado de dados, a ética e a eficiência são fatores interdependentes e inegociáveis para a perenidade corporativa.

# REFERÊNCIAS

BASTOS, Rodrigo Abolis; DIAS, Paulo Cezar; POSTAL, Ana Cristina Neves Valotto. O Compliance Digital – Inovação Tecnológica com Ênfase em Proteção de Dados. Revista de Direito Público da Procuradoria-Geral do Município de Londrina, v. 12, n. 1, 2023. Disponível em: https://aprolon.com.br/pkp/ojs/index.php/rdp-pgmlondrina/article/view/265. Acesso em: 20 abr. 2026.

BORGES, Luiz Ferreira Xavier; SERRÃO, Carlos Fernando de Barros. Aspectos de governança corporativa moderna no Brasil. Revista do BNDES, Rio de Janeiro, v. 12, n. 24, p. 195-214, dez. 2005.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20 abr. 2026.

BRASIL. Decreto nº 8.420, de 18 de março de 2015. Regulamenta a Lei nº 12.846, de 1º de agosto de 2013, e dispõe sobre os programas de integridade. Diário Oficial da União, Brasília, DF, 19 mar. 2015.

BRASIL. Lei nº 12.846, de 1º de agosto de 2013. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira. Diário Oficial da União, Brasília, DF, 2 ago. 2013.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 abr. 2026.

CAMPOS, Daniella; DOS REIS CARREIRO, Flávia. Compliance e gestão de riscos em tempos de inovação e disrupção digital. Revista de Gestão e Secretariado, v. 15, n. 4, p. e3743, 2024. Disponível em: https://ojs.revistagesec.org.br/secretariado/article/view/3743. Acesso em: 20 abr. 2026.

CAVALIERI, Davi Valdetaro Gomes. Governança de dados e programa de compliance digital na administração pública: contribuições da LGPD para a integridade governamental. In: LGPD e Administração Pública. 1. ed. São Paulo: Thomson Reuters Brasil, 2020.

CECYN, Victor Antonio. O Programa de Compliance como Medida de Prevenção e Mitigação de Riscos Emanados por Inteligências Artificiais no Tratamento de Dados Pessoais. São Paulo: Aya Editora, 2023. Disponível em: https://ayaeditora.com.br/livros/LF001C39.pdf. Acesso em: 20 abr. 2026.

DANTAS FILHO, Jerônimo Vieira; DA SILVA, Kauam Marcos. A Lei Geral de Proteção de Dados (LGPD) e Seu Impacto no Direito Empresarial: Desafios e Oportunidades para as Empresas na Era Digital. NATIVA – Revista de Ciências, Tecnologia e Inovação, v. 8, n. 3, p. 36-41, 2025. Disponível em: https://jiparana.emnuvens.com.br/riacti/article/view/1962. Acesso em: 20 abr. 2026.

FIGUEIREDO, Mateus de Carvalho. A aplicação da Lei Geral de Proteção de Dados na Governança Corporativa Brasileira. 2021. Monografia (Graduação em Direito) – Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2021.

GARCIA, Flúvio Cardinelle Oliveira. Cibersegurança, Compliance Digital e Custo Reputacional. Computação Brasil, n. 52, p. 51-60, 2024. Disponível em: https://journals-sol.sbc.org.br/index.php/comp-br/article/view/4603. Acesso em: 20 abr. 2026.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). Código das melhores práticas de governança corporativa. 5. ed. São Paulo: IBGC, 2015.

LOBREGAT, Christiane. Compliance no Brasil. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (Org.). Compliance: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018.

LÓSSIO, Cláudio Joel Brito. O Compliance Digital e a Proteção de Dados: Preservando Direitos na Sociedade da Informação. 2020. Dissertação (Mestrado em Direito) – Universidade Autónoma de Lisboa, Lisboa, 2020. Disponível em: https://www.proquest.com/openview/8c88784e6f92b51f251d37170acc4d7b/1. Acesso em: 20 abr. 2026.

NOGUEIRA, Andeise Silva Farias; CAMPOS, Izabeliza S. Compliance como ferramenta hábil à consolidação da governança corporativa e a sustentabilidade empresarial. Revista Brasileira de Direito Empresarial, v. 10, n. 2, p. 21-37, jan./jul. 2025.

RSDE. Revista Semestral de Direito Empresarial. Compliance e governança corporativa: estratégias para uma gestão administrativa eficaz. Rio de Janeiro, n. 32, p. 113-140, jan./jun. 2023.

SOUZA, Carolina Vilela de. Compliance digital: privacidade e proteção de dados à luz da Lei Geral de Proteção de Dados e os desafios de implementação. 2022. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade Federal de Uberlândia, Uberlândia, 2022.

TOMAZETTE, Marlon. Curso de direito empresarial: Teoria geral e direito societário. 8. ed. rev. e atual. São Paulo: Atlas, 2017.