LUCIANO CARVALHO MUCIO

ADEQUAÇÃO À LGPD E GERAÇÃO DE VALOR EMPRESARIAL NO ÂMBITO DO DIREITO NEGOCIAL: UMA ANÁLISE PELA ÓTICA DA GOVERNANÇA CORPORATIVA E DO COMPLIANCE

Londrina
2026

LUCIANO CARVALHO MUCIO

ADEQUAÇÃO À LGPD E GERAÇÃO DE VALOR EMPRESARIAL NO ÂMBITO DO DIREITO NEGOCIAL: UMA ANÁLISE PELA ÓTICA DA GOVERNANÇA CORPORATIVA E DO COMPLIANCE

Dissertação apresentada ao Programa de Pós-graduação em Direito Negocial - PPGDN da Universidade Estadual de Londrina - UEL, como requisito para a obtenção do título de Mestre.

Orientador: Prof. Dr. Tarcísio Teixeira

Londrina
2026

Ficha de identificação da obra elaborada pelo autor, através do Programa de Geração Automática do Sistema de Bibliotecas da UEL

CARVALHO MUCIO, LUCIANO.
Adequação à LGPD e Geração de Valor Empresarial no Âmbito do Direito Negocial: : uma análise pela ótica da governança corporativa e do compliance. / LUCIANO CARVALHO MUCIO. - Londrina, 2026.
93 f. : il.

Orientador: TARCISIO TEIXEIRA.
Dissertação (Mestrado em Direito Negocial) - Universidade Estadual de Londrina, Centro de Estudos Sociais Aplicados, Programa de Pós-Graduação em Direito Negocial, 2026.
Inclui bibliografia.

1. LGPD - Tese. 2. GOVERNANÇA CORPORATIVA - Tese. 3. COMPLIANCE - Tese. 4. DIREITO NEGOCIAL - Tese. I. TEIXEIRA, TARCISIO. II. Universidade Estadual de Londrina. Centro de Estudos Sociais Aplicados. Programa de Pós-Graduação em Direito Negocial. III. Título.

CDU 34

LUCIANO CARVALHO MUCIO

ADEQUAÇÃO À LGPD E GERAÇÃO DE VALOR EMPRESARIAL NO ÂMBITO DO DIREITO NEGOCIAL: UMA ANÁLISE PELA ÓTICA DA GOVERNANÇA CORPORATIVA E DO COMPLIANCE

Dissertação apresentada ao Programa de Pós-graduação em Direito Negocial da Universidade Estadual de Londrina - UEL, como requisito para a obtenção do título de Mestre.

_____

Prof. Orientador: Prof. Dr. Tarcisio Teixeira
Universidade Estadual de Londrina - UEL

_____

Prof. Dr. Clodomiro José Bannwart Junior
Universidade Estadual de Londrina - UEL

_____

Prof. Dra. Mirelle Neme Buzalaf
Universidade Estadual de Londrina - UEL

Londrina, 16 de junho de 2026

AGRADECIMENTOS

Agradeço, primeiramente, a Deus, pela saúde, discernimento e coragem para enfrentar esse desafio, além de ter me guiado e livrado de todo mal, nas mais de 60 viagens entre Maringá e Londrina realizadas.

À minha família, que, de modo amplo, sempre me incentivou em todos os meus projetos de vida, dando-me apoio incondicional.

Ao meu orientador, Prof. Dr. Tarcisio Teixeira, que por meio do Programa de Mestrado em Direito Negocial da UEL, me acolheu como seu orientando e foi essencial ao meu aprendizado em todos os sentidos, serei eternamente grato por tudo.

A todos os professores que ministraram as disciplinas cursadas, transmitindo conhecimento e trazendo discussões de alto nível para as aulas e que foram essenciais ao meu aprendizado e crescimento, meu muito obrigado.

Ao Chico, secretário do PPGDN, pela ajuda essencial para que eu pudesse sair do carro sempre que chegava para as aulas, meu muito obrigado.

Aos meus amigos de estágio docência, Paulo e Estéfano, que através da amizade e comprometimento, fizeram essa etapa do mestrado mais agradável e leve, meu muito obrigado.

Aos meus amigos Luciano e Thaise que entraram no Mestrado no mesmo processo seletivo que eu e foram, também, orientandos do Professor Tarcisio, agradeço as trocas e parcerias.

Aos muitos amigos e amigas que fiz durante todo o mestrado nas diversas disciplinas que cursei, obrigado pela amizade, pelas trocas, pelas ajudas, por tudo, serei eternamente grato a todos.

“Sempre faça tudo com muito amor e com muita fé em Deus, que um dia você chega lá. De alguma maneira, você chega lá".
(*Ayrton Senna da Silva).*

RESUMO

MUCIO, Luciano Carvalho. **Adequação à LGPD e Geração de Valor Empresarial no Âmbito do Direito Negocial:** uma análise pela ótica da governança corporativa e do *compliance*. 2026. 93 folhas. Dissertação apresentada ao Programa de Pós-Graduação em Direito Negocial da Universidade Estadual de Londrina – UEL. Londrina, 2026.

A relevância dos temas da privacidade e da proteção de dados aumentou sobremaneira em nossos tempos, especialmente pelo incremento tecnológico que se tem visto, tendo como consequência a digitalização das relações sociais. Com isso, nasce, por parte do Estado, a necessidade de regulação dessas relações com vistas a preservar a privacidade das pessoas. Nesse sentido, a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/18) insere-se no ordenamento jurídico brasileiro como instrumento de tutela do direito fundamental à privacidade, contudo, produz impactos no ambiente empresarial – os quais serão o foco principal deste trabalho – especialmente no âmbito do direito negocial, ao influenciar práticas contratuais, estruturas organizacionais e estratégias corporativas. Nesse contexto, a presente dissertação tem como problemática analisar se a LGPD pode ser compreendida como instrumento de geração de valor empresarial no âmbito da governança corporativa e do *compliance*, ou limita-se a ser um mecanismo de controle regulatório imposto às empresas. Para isso, tem-se como hipótese que a adequação à LGPD, embora decorrente de imposição normativa, pode transcender a lógica do custo regulatório, convertendo-se em ativo estratégico quando integrada à governança corporativa e ao *compliance*. A metodologia utilizada foi a pesquisa qualitativa, baseada em doutrinas, jurisprudência, legislações, entrevista, artigos de revistas, documentos normativos e pesquisas produzidas por empresas de porte mundial. Nesse intento, partiu-se apresentando uma breve correlação entre o tema proposto nesta dissertação e o direito negocial. Após, apresentou-se um histórico sobre o tema da privacidade, bem como, sua definição. Na sequência, a LGPD veio a comento através de seus fundamentos, princípios, da sua convergência com os temas da responsabilidade civil e da governança corporativa. Após, foi apresentado o tema da governança corporativa, seguido por *compliance* e *compliance* de dados. Por fim, investiga-se as condições sob as quais a adequação à LGPD pode gerar valor econômico,

reputacional e competitivo para as organizações. Conclui-se que a adequação à LGPD pelas empresas quando alinhada a estruturas adequadas de governança corporativa e *compliance*, pode contribuir para a geração de vantagens competitivas, mitigação de riscos e fortalecimento das relações negociais, evidenciando sua relevância no contexto empresarial contemporâneo, capaz de gerar valor econômico, reputacional e institucional.

Palavras-chave: Lgpd; Governança corporativa; *Compliance*; Direito negocial.

ABSTRACT

MUCIO, Luciano Carvalho. **LGPD Adherence and Business Value Generation in the Scope of Business Law:** an analysis from the perspective of corporate Governance and compliance. 2026. 93 pages. Dissertation presented to the Postgraduate Program in Business Law of the State University of Londrina – UEL. Londrina, 2026.

The relevance of privacy and data protection has increased significantly in recent times, especially due to the technological advancements that have led to the digitalization of social relations. As a result, the State has developed the need to regulate these relations in order to safeguard individuals' privacy. In this context, the Brazilian General Data Protection Law (Law No. 13,709/18 – LGPD) is incorporated into the Brazilian legal system as an instrument for the protection of the fundamental right to privacy. However, it also produces impacts on the business environment—which constitutes the main focus of this study—particularly within the scope of business law, as it influences contractual practices, organizational structures, and corporate strategies. Within this framework, this dissertation addresses the following research problem: whether the LGPD can be understood as an instrument for generating business value within the scope of corporate governance and compliance, or whether it is limited to functioning as a regulatory control mechanism imposed on companies. To this end, the hypothesis is that compliance with the LGPD, although arising from a legal obligation, may transcend the logic of regulatory cost and become a strategic asset when integrated into corporate governance and compliance structures. The methodology adopted is qualitative research, based on legal doctrine, case law, legislation, interviews, academic journal articles, regulatory documents, and studies produced by globally recognized companies. To achieve its objectives, the study initially presents a brief correlation between the proposed theme and business law. Subsequently, it provides a historical overview of the concept of privacy, as well as its definition. Thereafter, the LGPD is analyzed through its foundations and principles, as well as its convergence with the fields of civil liability and corporate governance. The study then addresses corporate governance, followed by compliance and data compliance. Finally, it investigates the conditions under which compliance with the LGPD can generate economic, reputational, and competitive value for organizations. It is concluded that compliance with the LGPD, when aligned with appropriate

corporate governance and compliance structures, can contribute to the generation of competitive advantages, risk mitigation, and the strengthening of business relations, thereby demonstrating its relevance in the contemporary business environment as a mechanism capable of generating economic, reputational, and institutional value.

Keywords: LGPD; Corporate Governance; Compliance; Business Law.

LISTA DE FIGURAS

Figura 1 – Estrutura de Governança Corporativa..... 39
Figura 2 – Etapas da implementação da Governança Corporativa no âmbito da proteção de dados..... 46
Figura 3 – Plano de Integridade e Compliance.....63
Figura 4 – Ciclo de atividades do Data Protection Impact Assessment (DPIA)..... 68
Figura 5 – Percentual de empresas que consideram certificações em privacidade um fator de compra..... 78

LISTA DE TABELAS

Tabela 1 – Cronologia da Proteção de Dados no Brasil 23

Tabela 2 – Níveis de gerenciamento na Governança de Dados..... 50

Tabela 3 – Princípios de *Compliance* 58

Tabela 4 – Definição de operador, controlador e encarregado de dados na LGPD... 72

Tabela 5 – Empresas que já receberam multas relativas à proteção de dados..... 83

LISTA DE ABREVIATURAS E SIGLAS

ANPD **–** AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS

CDC **–** CÓDIGO DE DEFESA DO CONSUMIDOR

COAF **–** CONSELHO DE CONTROLE DE ATIVIDADES FINANCEIRAS

COINTELPRO **–** *COUNTER INTELLIGENCE PROGRAM*

CVM **–** COMISSÃO DE VALORES MOBILIÁRIOS

DPIA **–** *DATA PROTECTION IMPACT ASSESSMENT*

DPO **–** *DATA PROTECTION OFFICER*

FATCA **–** *FOREIGN ACCOUNT TAX COMPLIANCE ACT*

FCPA **–** *FOREIGN CORRUPT PRACTICES ACT*

GDPR **–** GENERAL DATA PROTECTION REGULATION

IBGC **–** INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA

IBM **–** *INTERNATIONAL BUSINESS MACHINES CORPORATION*

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

ONU **–** ORGANIZAÇÃO DAS NAÇÕES UNIDAS

PIA **–** *PRIVACY IMPACT ASSESSMENT*

SGPI – SISTEMA DE GESTÃO DE PRIVACIDADE DA INFORMAÇÃO

SUMÁRIO

INTRODUÇÃO 14

1 A PROTEÇÃO DE DADOS PESSOAIS COMO ELEMENTO ESTRUTURANTE DO DIREITO NEGOCIAL CONTEMPORÂNEO 17

2 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E SUA INTERFACE COM A RESPONSABILIDADE CIVIL E A GOVERNANÇA CORPORATIVA 19

2.1 O Direito à Privacidade Como Princípio da Proteção de Dados 19
2.2 LGPD: Fundamentos, Princípios e Responsabilidade Civil 24
2.2.1 Fundamentos da Lei Geral de Proteção de Dados Pessoais 25
2.2.2 Princípios da Lei Geral de Proteção de Dados Pessoais 28
2.2.3 Responsabilidade Civil no Contexto da Lei Geral de Proteção de Dados Pessoais 29
2.3 Convergência Entre LGPD e Governança Corporativa 33

3 GOVERNANÇA CORPORATIVA: HISTÓRICO, DEFINIÇÃO, ESTRUTURA, PRINCÍPIOS E SUA IMPORTÂNCIA PARA AS EMPRESAS 34

3.1 Histórico da Governança Corporativa 34
3.2 Definição de Governança Corporativa 37
3.3 Estrutura de Governança Corporativa 39
3.4 Princípios de Governança Corporativa 40
3.4.1 Princípio da Equidade 41
3.4.2 Princípio da Responsabilização (*Accountability*) 42
3.4.3 Princípio da Transparência 42
3.4.4 Princípio da Sustentabilidade 43
3.4.5 Princípio da Integridade 43
3.5 Implementação da Governança Corporativa na Proteção de Dados 44
3.6 Importância da Governança Corporativa na Geração de Valor Para as Empresas 51

4 *COMPLIANCE, COMPLIANCE* DE DADOS E A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LEI 13.709/18 54

4.1 Definição, Histórico, Princípios e Funções do *Compliance* 54
4.2 Programa de Integridade e *Compliance* 61
4.3 Compliance de Dados 64
4.4 *Compliance* e a Lei Geral de Proteção de Dados Pessoais 69

5 A ADEQUAÇÃO À LGPD COMO ESTRATÉGIA DE GOVERNANÇA E *COMPLIANCE* NA GERAÇÃO DE VANTAGEM COMPETITIVA EMPRESARIAL . 74

5.1 Identificação, Prevenção, Mitigação e Correção de Riscos 75
5.2 Oportunidade de Negócios e Vantagem Competitiva 76
5.3 Valorização da Marca, da Reputação e da Imagem Empresarial 79
5.4 Eficiência Operacional e Atração de Investimentos 81
5.5 Limitação de Responsabilidade e Mitigação de Gastos com Vazamentos de Dados 82

CONCLUSÃO 85

REFERÊNCIAS 87

INTRODUÇÃO

A evolução tecnológica vista nos últimos anos fez com que ocorresse uma crescente digitalização das relações sociais e empresariais, remodelando o modo como as pessoas executam algumas tarefas cotidianas, tais como compras, comunicação, relacionamentos e educação. Assim, os dados pessoais deixaram de ser meros registros deixados pelos seus titulares em decorrência dessa nova metodologia, para se tornarem objeto de interesse econômico, haja vista que a digitalização acelerada das relações sociais e comerciais colocou essas informações no coração das estratégias empresariais e, como consequência, apresentou uma questão que não podia ser ignorada: como garantir que esse movimento não viesse acompanhado de violações sistemáticas à privacidade das pessoas?

Nesse contexto, o Estado passa a se preocupar com o tema da privacidade e a segurança dos titulares de dados, com a correta utilização desses pelas empresas, fato que ocasiona a criação de leis em diversos países com vistas à proteção da privacidade dos titulares desses dados e da necessária adequação das empresas a esses regramentos, impondo requisitos para que o tratamento de dados seja efetuado.

A Lei Geral de Proteção de Dados Pessoais – Lei 13.709/18 surge nesse contexto, posicionando-se como elemento principal para equilibrar as relações entre empresas e titulares de dados, trazendo em seu bojo princípios, fundamentos, direitos e deveres a serem cumpridos pelas empresas que tratam dados, impondo que estas estejam em conformidade com seus ditames, ao passo que esta conformidade[1] passou a alterar diretamente o cotidiano das empresas, seja na forma como estruturam seus contratos, como gerenciam riscos e como organizam seus processos internos.

Para muitas organizações, essa adaptação foi sentida, a princípio, como mais um custo imposto pela regulação estatal, e é compreensível que assim fosse, haja vista que, adequar-se a uma nova lei exige tempo, investimento e mudança de cultura. O que este trabalho pretende explorar, porém, é justamente o que acontece quando se vai além dessa primeira impressão.

[1] A conformidade, no contexto da Lei Geral de Proteção de Dados Pessoais (LGPD), consiste na adequação sistemática e estruturada dos processos, políticas e práticas internas de uma organização às exigências legais, com o objetivo de assegurar o pleno cumprimento dos princípios, direitos e obrigações estabelecidos pela legislação de proteção de dados.

Uma leitura mais atenta da legislação e de seus desdobramentos práticos sugere que a conformidade com a LGPD pode gerar efeitos que superam a lógica da sanção e do controle. Empresas que levam a sério a proteção de dados tendem a desenvolver estruturas de governança mais sólidas, programas de *compliance* mais maduros e, não raramente, uma posição mais competitiva no mercado. A proteção de dados, nesse sentido, começa a conversar diretamente com o direito empresarial e com as escolhas estratégicas das organizações.

É a partir dessa tensão — entre custo regulatório e oportunidade estratégica — que se formula o problema central desta dissertação: a LGPD pode ser compreendida como um instrumento de geração de valor empresarial no âmbito da governança corporativa e do *compliance*, ou se resume a um mecanismo de controle imposto às empresas?

A hipótese que orienta este estudo é a de que, quando integrada a práticas estruturadas de governança corporativa e *compliance*, em especial ao *compliance* de dados, a LGPD tem o potencial de assumir um papel estratégico relevante para as organizações.

Do ponto de vista metodológico, a pesquisa é qualitativa e se apoia em doutrinas, jurisprudências, legislações, entrevista, artigos de revistas, documentos normativos e pesquisas produzidas por grandes empresas. A intenção é construir uma interpretação organizada, estruturada e lógica sobre a relação entre proteção de dados, governança corporativa, *compliance* e criação de valor no ambiente empresarial para que seja possível responder à pergunta norteadora desta dissertação.

Assim, a presente dissertação está estruturada da seguinte forma: num primeiro momento, apresentou-se a relação entre o tema proposto e o direito negocial. Na sequência, o tema da privacidade foi trazido através do histórico da preocupação com a privacidade que se viu em acontecimentos em diversos países. Após, a LGPD foi discutida através de seus fundamentos, princípios e da sua convergência com a responsabilidade civil e com a governança corporativa. Ato contínuo, foram abordados os temas da governança corporativa, do *compliance* e do *compliance* de dados. Ao final, verificou-se em que condições a adequação à LGPD pode gerar valor econômico, reputacional e competitivo para as empresas.

Vale registrar, por fim, que embora a LGPD tenha como núcleo a proteção de um direito fundamental, o recorte adotado neste trabalho é predominantemente

mercadológico. O foco recai sobre os efeitos da adequação normativa nas relações empresariais e negociais, especialmente no que diz respeito à geração de vantagens competitivas e à valorização das organizações perante o mercado.

1 A PROTEÇÃO DE DADOS PESSOAIS COMO ELEMENTO ESTRUTURANTE DO DIREITO NEGOCIAL CONTEMPORÂNEO

Antes de serem propriamente discutidos os temas principais da presente dissertação, faz-se necessário entender a correlação que se tem entre o tema aqui abordado e os parâmetros principais do direito negocial, haja vista que essa vertente constitui a espinha dorsal do programa no qual esta pesquisa está sendo desenvolvida, dedicada a estudar os negócios jurídicos que ocorrem através da autonomia que os sujeitos de uma relação jurídica têm para autorregular a criação, modificação ou extinção de direitos, dentro de parâmetros definidos pelo ordenamento jurídico positivo[2].

Nesse sentido, a Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei 13.709 de 2018 consolidou o tema da proteção de dados em nosso ordenamento jurídico, representando, além da tutela da privacidade, a redefinição das bases do direito negocial, haja vista a importância adquirida pelos dados pessoais, proporcionada pela digitalização das relações humanas, seja no âmbito empresarial ou pessoal com o consequente aumento da disponibilização de dados nessas relações, os quais passaram a ter posição central sendo, inclusive, fator de vantagem competitiva às empresas, como será visto, mais adiante, pela ótica da governança corporativa e do *compliance*.

Em complemento às questões relativas à tutela da privacidade que a LGPD busca implementar, cabe denotar que a disponibilização pelos titulares e o consequente tratamento de dados pessoais realizado pelas organizações constituem contratos que, em última análise, fazem parte do escopo do direito negocial. Orlando Gomes nos apresenta quatro princípios do direito contratual, quais sejam: o da autonomia da vontade, do consensualismo, da força obrigatória e o princípio da boa-fé[3].

No que se refere ao princípio da autonomia da vontade, este se revela como o poder que os contratantes têm, mediante declaração de vontade, de verem reconhecidos os efeitos contratuais pactuados e tutelados pela ordem jurídica. Já a ideia do princípio do consensualismo é informar que o simples consentimento basta para formar o contrato. Relativo ao princípio da força obrigatória, tem-se que o contrato

---

[2] AMARAL, Francisco. **Direito Civil:** Introdução. 10 ed. São Paulo: Saraiva Educação, 2018. p.465.
[3] GOMES, Orlando. **Contratos.** Atualizado por AZEVEDO, Antônio Junqueira de; MARINO, Francisco Paulo de Crescenzo. 26 ed. Rio de Janeiro: Forense, 2009. p.25.

é lei entre as partes e, por fim, o princípio da boa-fé significa dizer que as partes devem manter, durante a vigência do contrato, a lealdade e a confiança recíprocas[4].

Com este cenário em vista, a proteção de dados preconizada pela LGPD, deixa de configurar mero limite regulatório à proteção de dados pessoais, para se consolidar como elemento estruturante das relações negociais, ao condicionar o exercício da autonomia privada, redefinindo novos padrões de boa-fé objetiva e impactando diretamente a validade, a eficácia e a responsabilidade advindas dos negócios jurídicos realizados no contexto digital, além de ser uma possibilidade de geração de valor para as empresas.

[4] GOMES, Orlando. **Contratos.** Atualizado por AZEVEDO, Antônio Junqueira de; MARINO, Francisco Paulo de Crescenzo. 26 ed. Rio de Janeiro: Forense, 2009. p.25, 37, 38, 43.

2 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E SUA INTERFACE COM A RESPONSABILIDADE CIVIL E A GOVERNANÇA CORPORATIVA

Para que se possa tratar do contexto empresarial onde a adequação à Lei Geral de Proteção de Dados Pessoais – Lei 13.709/18 pode gerar valor para as empresas que a ela se adequam, é necessário, primeiramente, tratar das origens do tema da proteção de dados, falando sobre privacidade e o porquê leis como a LGPD se tornaram importantes e vieram a ser implementadas.

Assim, primeiramente, será demonstrada a origem acerca do tema da privacidade, bem como das leis inerentes à proteção de dados, servindo de arcabouço histórico-conceitual, para que, num segundo momento, sejam trazidas discussões sobre a própria LGPD e sua relação com a responsabilidade civil e a governança corporativa.

Na sequência, temas como governança corporativa e *compliance* farão parte das discussões, culminando, por fim, nas vantagens que as empresas agregam ao se adequarem à LGPD.

2.1 O Direito à Privacidade Como Princípio da Proteção de Dados

As principais leis sobre proteção de dados, apesar de relativamente recentes, têm origens em fatos históricos que ocorreram há muitos anos, sendo a principal preocupação dessas leis proteger a privacidade das pessoas. No que toca esse tema, tem-se que a noção moderna de privacidade começou a se desenvolver a partir do século XVI, quando transformações na organização arquitetônica das residências possibilitaram maior distinção entre classes sociais dispostas em sociedade. Nesse contexto, o anseio de ter uma vida mais resguardada foi uma exigência, à época, da burguesia, demonstrada através da escolha arquitetônica de suas casas[5].

Outro acontecimento importante e afeto ao tema da privacidade das pessoas relaciona-se à primeira constituição dos Estados Unidos da América, cuja aprovação ocorreu no ano de 1787, 11 anos após a independência, e que, com a proposição da Declaração de Direitos (*Bill of Rights*) no ano de 1789 foram propostas 10 emendas à

[5] QUEIROZ, Renata Capriolli Zocatelli. **A proteção de dados pessoais: A LGPD e a disciplina jurídica do Encarregado de Proteção de Dados Pessoais.** Orientador: Professor Titular Dr. Álvaro Villaça Azevedo. 2021. 137 f. Tese (Doutorado em Direito) – Programa de Pós-Graduação em Direito da Faculdade de Direito da Universidade de São Paulo. São Paulo, 2021. Versão eletrônica, p.20.

recém constituição elaborada, dentre as quais, a quarta emenda buscava garantir a privacidade dos americanos no que se referia às suas casas, documentos e bens, demonstrando assim o respeito a questões da vida pessoal que deveriam ser preservadas[6].

Ato contínuo, acontecimento de relevante importância para a consolidação da ideia de que a privacidade deveria ser resguardada, foi evidenciado em 1890, ano em que Samuel Warren e Louis Brandeis publicaram na *Harvard Law Review* um artigo intitulado *The Right to Privacy,* cujo intento era dar luz à perda da privacidade que vinha ocorrendo por conta do avanço no uso daquilo que foi denominado pelos autores como “fotografias instantâneas” iniciando um debate jurídico sobre o tema[7].

Em âmbito mundial, no ano de 1948, a Declaração dos Direitos Humanos da ONU, incluiu em seu artigo 12 o tema da privacidade, cujo teor integral era:

> Ninguém sofrerá interferências arbitrárias em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem ataques à sua honra e reputação. Toda pessoa tem direito à proteção da lei contra tais interferências ou ataques[8].

Assim, pode-se notar que mesmo antes da preocupação com a proteção de dados pessoais, como conhecemos hoje em dia, a percepção no que concerne à privacidade das pessoas nasce de acontecimentos muito anteriores que permeiam o desenvolvimento das sociedades, demonstrando assim, ser uma inquietação social de longa data.

Nesse diapasão, cabe denotar que a proteção de dados pessoais, especificamente, teve o seu marco inicial há 56 anos com a elaboração da Lei de Proteção de Dados pelo estado alemão de Hesse, no ano de 1970, sendo este o primeiro instrumento em nível mundial dedicado exclusivamente ao tema em comento, tendo como precursores acontecimentos sociais ocorridos na segunda metade da década de 1960. Nesse intervalo de cinquenta anos, o tema da proteção de dados se

---

[6] NATIONAL ARCHIVES. **A Declaração de Direitos:** Uma Transcrição. Revisado em 28 de abril de 2025. Disponível em: https://www.archives.gov/founding-docs/bill-of-rights-transcript. Acesso em: 30 jun. 2025.

[7] UNIVERSITY OF MICHIGAN. Information and Technology Services. Safe Computing. **History of Privacy Timeline.** Disponível em: https://safecomputing.umich.edu/protect-privacy/history-of-privacy-timeline. Acesso em: 7 jun. 2025.

[8] NAÇÕES UNIDAS (1948). **Declaração Universal dos Direitos Humanos.** Disponível em: https://www.un.org/en/about-us/universal-declaration-of-human-rights. Acesso em: 8 de ago. 2025.

sedimentou fortemente, principalmente pelo aumento expressivo que se viu no tratamento de dados pessoais atrelado, principalmente, pelo aumento da capacidade tecnológica e da importância mercadológica que esses dados carregam em si, no que tange à possibilidade de serem usados pelas empresas na oferta assertiva de seus produtos[9].

Ainda no âmbito europeu, é necessário dizer que após a Lei de Hesse, houve expressivos desenvolvimentos legislativos que aumentaram a abrangência dos cuidados relativos à proteção de dados. Um desses novos passos, se deu no ano de 1995, com a Diretiva 95/46, através da qual, não só a Alemanha, mas todos os países que compõem o bloco da União Europeia, passaram a elaborar suas próprias leis sobre o tema da proteção de dados, o que proporcionou a criação de uma diversidade de ordenamentos sobre proteção de dados pessoais, ocasionando, como consequência, a descentralização jurídica sobre o assunto, que foi resolvida com a promulgação, em 2016, da *General Data Protection Regulation (GDPR)*, cujo objetivo foi unificar o entendimento sobre a proteção de dados nos países que fazem parte do bloco europeu[10].

De maneira sintética, a importância reconhecida à proteção dos dados pessoais, bem como, o modo como estes deveriam ser tratados, deram origem a diversos marcos regulatórios pelo mundo, tendo esse movimento iniciado, como visto, na Alemanha no ano de 1970, através dos quais, direitos e garantias aos titulares foram estabelecidos, ao passo que, limites ao uso dessas informações, seja por agentes públicos ou privados, foram também impostos.

Nos Estados Unidos, o marco regulatório sobre o tema da privacidade teve início com a entrada em vigor da *Privacy Act* no ano de 1974, lei esta que teve como tema central o tratamento de informações pessoais, cuja criação foi influenciada por problemas relacionados à espionagem política, sendo os principais acontecimentos, os escândalos de Watergate[11] e o Programa de Contrainteligência (COINTELPRO) cujo foco era o combate à vigilância ilegal por parte de partidos políticos de oposição e também de indivíduos considerados subversivos, de modo a recuperar a confiança

---

[9] DONEDA, Danilo. **Panorama Histórico da Proteção de Dados Pessoais.** *In*: BIONI, Bruno. Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021, p.30.

[10] DONEDA, Danilo. **Panorama Histórico da Proteção de Dados Pessoais.** *In*: BIONI, Bruno. Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021, p.37.

[11] Para saber mais sobre o Escândalo de Watergate recomendo a leitura em: https://www.britannica.com/event/Watergate-Scandal/Watergate-trial-and-aftermath.

no governo por parte dos cidadãos[12].

Ademais, a *Privacy Act* teve como base um relatório intitulado “Registros, Computadores e os Direitos dos Cidadãos: Relatório do Comitê Consultivo da Secretaria Sobre Sistemas Automatizados de Dados” publicado pelo departamento de Saúde, Educação e Bem-Estar dos Estados Unidos, o qual foi o primeiro estudo abrangente afeto ao tema da privacidade relativa ao uso de tecnologias pelas empresas em substituição aos sistemas de papel[13].

No Brasil, também tivemos uma evolução legislativa até a promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei 13.709/18 que trata efetivamente do tema da proteção de dados. O primeiro intento nesse sentido veio no ano de 1988 com a promulgação da Constituição da República Federativa do Brasil, que em seu artigo 5º, inciso X, nos apresenta que:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> X – São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação[14].

Após esse indicativo constitucional, um novo impulso no tema da proteção de dados pessoais foi dado no ano de 2012, com o Projeto de Lei nº 4.060/12 de autoria do deputado Milton Monti, que tratava “do tratamento de dados pessoais e dava outras providências”, projeto que, posteriormente, deu origem à LGPD[15]. Já em 2013, o Projeto de Lei nº330 de 2013 tinha a seguinte ementa “dispor sobre a proteção, o tratamento e o uso de dados pessoais”[16].

Além desses projetos, no ano de 2014 tivemos a promulgação da Lei nº 12.965, conhecida como Marco Civil da Internet, cuja ementa tem a seguinte descrição:

---

[12] OFFICE OF PRIVACY AND CIVIL LIBERTIES. **Overview of the Privacy Act:** 2020 Edition. Atualizado em 4 de outubro de 2022. Disponível em: https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/introduction. Acesso em: 30 jun. 2025.

[13] OFFICE OF PRIVACY AND CIVIL LIBERTIES. **Overview of the Privacy Act:** 2020 Edition. Atualizado em 4 de outubro de 2022. Disponível em: https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/introduction. Acesso em: 30 jun. 2025.

[14] BRASIL. **Constituição da República Federativa do Brasil.** Brasília, DF, 1988.

[15] BRASIL. **Projeto de Lei 4060. Dispõe sobre o tratamento de dados pessoais, e dá outras providências**. Brasília, DF, 2012.

[16] BRASIL. **Projeto de Lei do Senado nº330. Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências**. Brasília, DF, 2013.

“estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil”, e tinha como princípios para disciplinar o uso da internet no país, a proteção da privacidade e a proteção dos dados pessoais, na forma da lei[17].

O artigo 7º dessa lei trata assim as questões relativas aos dados pessoais:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
>
> X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais; [18].

Ademais, o mesmo instituto trata em sua segunda seção da proteção aos registros, aos dados pessoais e às comunicações privadas, de modo que, mesmo antes de termos uma lei que viabilizasse a proteção de dados pessoais de modo estrito (a LGPD), diversos direitos, nesse sentido, já eram assegurados aos usuários de internet através da Lei nº 12.965.

A tabela a seguir apresenta os principais acontecimentos na esfera jurídica, em ordem cronológica, sobre o tema da proteção de dados no Brasil, a partir da promulgação da Constituição Federal no ano de 1988:

Tabela 1: Cronologia da Proteção de Dados no Brasil

ANO	ACONTECIMENTO
1988	Direito à privacidade garantido pela Constituição Federal.
2010	Consulta Pública Ministério da Justiça sobre o anteprojeto de lei de proteção de dados.
2013	Projeto de Lei nº330 buscava dispor sobre proteção, tratamento e uso de dados.
2018	Publicação da LGPD – prazo de 18 meses para

[17] BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 9 maio 2025.
[18] BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 9 maio 2025.

	entrar em vigor.
2019	MP nº 869 estabeleceu a criação da ANPD e a *vacatio legis* de 24 meses para a LGPD
2020	Lei nº 14.010 manteve o início da vigência da LGPD para agosto de 2020
2020	LGPD entra em vigor em 18 de setembro.
2021	Entram em vigor as sanções administrativas com multas e advertências.

Fonte: elaborado pelo autor.

Traçado esse panorama inicial, pode-se verificar que, para chegar às leis referentes à proteção de dados como as conhecemos hoje, tanto no Brasil quanto em nível mundial, diversos acontecimentos históricos ocorreram, de modo que estes, pleitearam a atenção dos entes públicos para o tema da privacidade das pessoas, mostrando que a exposição pública de aspectos privados inerentes à vida de cada um, pode proporcionar, de alguma forma, prejuízos, sejam de ordem moral ou material.

Nesse sentido, e pela evolução do tema, é que se chega na possibilidade desses danos serem causados por empresas que não se adequem aos preceitos da Lei nº 13.709/18 de modo que, ao contrário, para aquelas que estão em conformidade, além de não terem problemas jurídicos, reputacionais, financeiros, dentre outros, o simples fato de terem cuidado com os dados pessoais de seus clientes torna-se, uma vantagem competitiva como será demonstrado no decorrer desse texto. Passemos a diante, apresentado aspectos relativos à Lei Geral de Proteção de Dados Pessoais, propriamente dita.

2.2 LGPD: Fundamentos, Princípios e Responsabilidade Civil

Apresentado um breve histórico acerca do tema da privacidade, bem como, das principais leis que tratam do tema da proteção de dados que surgiram na Europa, nos Estados Unidos e no Brasil, cabe agora demonstrar aspectos relativos à Lei Geral de Proteção de Dados Pessoais – Lei 13.709/18, principalmente aqueles afetos aos fundamentos, princípios e responsabilidade civil, para que, num segundo momento, se possa entender o motivo pelo qual se torna vantajoso para as empresas se adequarem aos ditames da lei.

De maneira introdutória, com o objetivo de demonstrar quais são os

fundamentos e princípios da LGPD, cabe aqui uma breve diferenciação terminológica, diferenciando o que vem a ser um e outro, de modo que possamos entender os motivos pelos quais tais fundamentos e princípios foram elencados.

No entendimento de Miguel Reale[19] “o fundamento é o valor ou fim objetivado pela regra de direito, é a razão de ser da norma, sendo impossível conceber-se uma regra jurídica desvinculada da finalidade que legitima sua vigência e eficácia”. Já o conceito de princípios para o jurista Celso Antônio Bandeira de Mello é assim delineado:

> O princípio é um mandamento nuclear de um sistema, verdadeiro alicerce dele, disposição fundamental que se irradia sobre diferentes normas, compondo-lhes o espírito e servindo de critério para a sua exata compreensão e inteligência, exatamente para definir a lógica e a racionalidade do sistema normativo, no que lhe confere a tônica e lhe dá sentido harmônico[20].

Apresentadas as diferenças entre fundamentos e princípios, entendemos que estes são normas diretivas que orientam a aplicação e interpretação da lei, enquanto aqueles são os motivos e valores que levaram o legislador a criar a lei.

2.2.1 Fundamentos da Lei Geral de Proteção de Dados Pessoais

Sendo os fundamentos para a proteção de dados pessoais uma questão inerente à Lei Geral de Proteção de Dados Pessoais, que apontam o porquê da existência da lei, portanto, aquilo que este dispositivo entende como inegociável e que, almeja garantir, passa-se a apresentar e discutir o conteúdo do artigo segundo da LGPD, o qual elenca o rol desses fundamentos, são eles: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais[21].

---

[19] REALE, Miguel. **Lições Preliminares de Direito**. 25 ed. 21 tiragem. São Paulo: Saraiva, 2001, p.106.
[20] MELLO, Celso Antônio Bandeira de. **Curso de Direito Administrativo.** 17 ed. São Paulo: Malheiros, 2004, p.451.
[21] BRASIL. Lei nº 13.709, de 14 de agosto de 2018 — Lei Geral de Proteção de Dados Pessoais (LGPD). **Dispõe sobre a proteção de dados pessoais** [...]. Brasília, DF: Presidência da República,

Sobre o fundamento relativo ao respeito à privacidade, esse permeia discussões sociais e jurídicas há muito tempo como já delineado anteriormente. Antes, as empresas colocavam seus produtos e serviços no mercado, faziam a publicidade, contudo, sem ter acesso muito detalhado a gostos, preferências, históricos de compras dos consumidores, dentre outras informações, contudo, hoje em dia, a cada nova interação com uma determinada empresa, seja no âmbito digital ou no físico, dados são coletados e retroalimentam as bases de dados das empresas que, em regra, objetivam que cada um de nós consumamos cada vez mais[22].

Cabe acrescentar que, com a utilização massiva da tecnologia nos tempos atuais, o cruzamento de dados cadastrais, análises em redes sociais, históricos de compras no ambiente virtual dentre outras ferramentas, tornaram-se uma forma que as empresas encontraram para traçar perfis de compradores, gostos, interesses, para direcionar ofertas de produtos ou serviços[23].

> Experiência comum a todos nós que utilizamos a internet para realizar compras, nos comunicar, contratar serviços, ou apenas para pesquisas de qualquer natureza: a insistente intrusão em nossas vidas privadas com oferta de produtos ou serviços, propagandeados durante toda a navegação, mesmo depois de já termos deixado de procurar por aquele objeto ou serviço. Nossos dados são incessantemente compartilhados entre os players que fazem parte de quase todas as cadeias de consumo. Nossas pegadas digitais, ao navegar, deixamos nossos "rastros" de dados em redes sociais, bancos, blogs, sites jornalísticos, por todo e qualquer serviço digital por onde passamos. Dados pessoais, relativos a nosso comportamento, nossas expectativas, interesses, intenções e até mesmo sobre nossas emoções, são alvo caro desta nova economia, coletados de forma indiscriminada e para finalidades que nem sempre nos trarão algum benefício dentro de um modelo de capitalismo de vigilância. Imaginemos agora, que uma dada empresa tenha acesso a este rico histórico de navegação e consiga também acesso a outros conjuntos de dados relacionados aos mesmos indivíduos e que, ao serem processados, revelem a capacidade aquisitiva do indivíduo, suas preferências e gostos, além de outras informações sobre seus bens, vínculo empregatício, renda, etc. Não é difícil pensar o valor que essas informações podem representar para empresas (ou até mesmo outras pessoas) que busquem identificar determinados perfis comportamentais para oferta de produtos e serviços personalizados[24].

2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 9 maio 2025.

[22] ROSA, Glaucio Monteiro. Privacidade e Proteção de Dados: uma abordagem histórica e evolucionista. *In*: BARRETO, Gileno Gurjão; ANTONIO, André Luiz Sucupira; LIMA, André Gustavo Bastos. **Governança em privacidade e proteção de dados:** uma visão integrada aos negócios empresariais. 1.ed. Curitiba: Editorial Casa, 2022. p.64

[23] VAINZOF, Rony. Capítulo 1 – Disposições Preliminares. *In*: MALDONADO, Viviane Nobre; BLUM, Renato Opice. **LGPD:** Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2019. p.23.

[24] ROSA, Glaucio Monteiro. Privacidade e Proteção de Dados: uma abordagem histórica e evolucionista. *In*: BARRETO, Gileno Gurjão; ANTONIO, André Luiz Sucupira; LIMA, André Gustavo Bastos. **Governança em privacidade e proteção de dados:** uma visão integrada aos negócios

Fica evidenciado, nesse caso, que a capacidade tecnológica das empresas para cruzar dados, tendo objetivos primordialmente econômicos, coloca a privacidade das pessoas em risco haja vista que, cada vez mais, estas disponibilizam informações de cunho pessoal na internet de forma isolada, mas que com um cruzamento eficiente feito por corporações interessadas, acabam por entregar mais do que necessário de sua vida privada à terceiros.

Daí então a LGPD trazer o respeito à privacidade como um fundamento de primeira ordem, a ser seguido no tratamento de dados pelas empresas, dada a sua importância.

Em relação ao segundo fundamento, tem-se que é através dele que os titulares de dados terão a garantia de que, em regra, poderão controlar os dados que disponibilizam na internet, efetuando uma autoproteção dinâmica durante todo o relacionamento que tiverem com as empresas com as quais compartilharam seus dados[25].

E de fato, esse fundamento é de suma importância, uma vez que, sem ele, a lei não disciplinaria sobre a possibilidade de que os titulares pudessem gerenciar as informações que compartilham em ambientes virtuais, de modo que, ficaria somente sob a responsabilidade das empresas realizar essa gestão, o que aumentaria sobremaneira a dependência e os riscos dos titulares dos dados compartilhados e que serão tratados.

Pertinente ao inciso III que traz o fundamento que garante a liberdade de expressão, de informação, de comunicação e de opinião, observa-se que estes já se apresentavam no Marco Civil da Internet, Lei nº 12.965/14, possibilitando que o espaço virtual seja um meio no qual as pessoas se informem, se comuniquem e emitam opiniões, contudo, a lei postula que ao exercerem sua liberdade de expressão, os dados que possam ser coletados, não sejam utilizados por qualquer empresa em ações que causem a perda da privacidade e/ou da liberdade dessas pessoas[26].

---

empresariais. 1.ed. Curitiba: Editorial Casa, 2022. p.63-64

[25] ROSA, Glaucio Monteiro. Privacidade e Proteção de Dados: uma abordagem histórica e evolucionista. *In*: BARRETO, Gileno Gurjão; ANTONIO, André Luiz Sucupira; LIMA, André Gustavo Bastos. **Governança em privacidade e proteção de dados:** uma visão integrada aos negócios empresariais. 1.ed. Curitiba: Editorial Casa, 2022. p.24.

[26] TEIXEIRA, Tarcisio. GUERREIRO, Ruth Maria. **Lei Geral de Proteção de Dados Pessoais:** comentada artigo por artigo. 4.ed. São Paulo: SaraivaJur, 2022. p.45.

No que tocam aos incisos IV e VII percebe-se que estes fundamentos apenas consagram aquilo que já está posto em nossa Carta Magna, mantendo para o contexto da proteção de dados, direitos inerentes às pessoas, quais sejam, à proteção de sua intimidade, honra, imagem, dignidade, dentre outros relativos à personalidade. Já os incisos V e VI fundamentam o direito que as empresas têm de se desenvolver, inovarem e concorrerem no mercado onde o tratamento de dados, quando realizado de forma efetiva, entrega vantagem competitiva.

Vistos os fundamentos, passa-se a apresentar, na sequência, os princípios que regem a Lei 13.709/18 com vistas a trazer entendimento sobre algumas das principais razões pelas quais as empresas devem estar adequadas ao conteúdo da lei de modo a evitar problemas de ordem reputacional, sancionatória, financeira, dentre outros.

2.2.2 Princípios da Lei Geral de Proteção de Dados Pessoais

Como definido anteriormente, os princípios indicam o modo como uma lei deve ser aplicada, nessa toada, a LGPD traz em seu artigo sexto o rol daqueles que são os princípios norteadores da aplicação da lei[27]. Como se percebe, a própria lei explica os princípios que congrega, desta feita, não se faz necessário traçar comentários adicionais sobre os mesmos haja vista o modo autoexplicativo que são trazidos.

Contudo, fazendo uma breve observação, estes constituem o alicerce normativo que orienta o tratamento de dados, buscando garantir aos titulares que, as empresas que irão tratá-los, não podem fazê-lo como bem entenderem, sem nenhuma

[27] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X – Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

régua de regulação, de modo que, questões como finalidade, transparência e responsabilização sobre o que foi coletado devem ser estritamente obedecidas.

Fato à parte, o *caput* do artigo, informa que um dos princípios que devem ser resguardados no tratamento de dados pessoais é o da boa-fé, o qual se apresenta como uma relação jurídica que tem como base a ética recíproca entre as partes, de modo a exigir o respeito mútuo, onde através desse princípio, cada um deve respeitar a personalidade da outra parte como se sua fosse, já que ambas têm a mesma dignidade[28].

Ademais, salienta o autor supracitado que a boa-fé se divide entre subjetiva e objetiva, sendo aquela um estado psicológico na crença de que existe um comportamento por parte de outrem conforme o direito, e esta, é o comportamento correto, portanto o esperado[29].

Apresentados os fundamentos e princípios que congregam a Lei Geral de Proteção de Dados Pessoais, visto que são de suma importância para entender as bases da lei e o que ela busca proteger, passa-se a elaborar o tema da responsabilidade civil no contexto da proteção de dados, pois trata-se de um dos pilares para o resultado que aqui se busca alcançar, visto que a aplicação de responsabilidades às empresas perante o tratamento de dados que estas executam de forma ineficaz é um dos grandes motivadores à adequação, pois se adequar aos ditames da lei é, em última análise, mitigar a possibilidade de problemas de ordem jurídica, ou de outra natureza, que possam comprometer a atividade empresarial. Isso tudo pois a LGPD não se restringe a abordagens técnicas ou administrativas, mas também define deveres jurídicos ao criar mecanismos de imputação de responsabilidade que possam impactar a atividade empresarial.

Isto posto, doravante, é feito um paralelo entre tratamento de dados e reparação de danos, demonstrando que a responsabilidade civil atua como instrumento de conformidade compatível, ao passo que, por isso, acaba por incentivar a adoção de modelos de governança e controle.

2.2.3 Responsabilidade Civil no Contexto da Lei Geral de Proteção de Dados Pessoais

---

[28] TOMASEVICIUS FILHO, Eduardo. **O princípio da Boa-fé no Direito Civil.** São Paulo: Almedina, 2020. p. 85-86.

[29] TOMASEVICIUS FILHO, Eduardo. **O princípio da Boa-fé no Direito Civil.** São Paulo: Almedina, 2020. p.87

Antes de apresentar o contexto da responsabilidade civil no âmbito da Lei 13.709/18, é cediço lançar mão de conceitos básicos e afetos ao tema para sedimentar o entendimento do que virá posteriormente.

Nesta esteira, este instituto representa o dever de reparação de um dano, atribuindo tal obrigação ao sujeito pertencente a uma relação jurídica que promove a lesão e, como consequência, faz com que a outra parte experimente uma mudança e/ou prejuízo em seu *status quo.* Assim, a gênese desse instrumento jurídico compõe o princípio que vincula o dever de indenizar à figura que causou o prejuízo, não importando se o gerador do dano teve, ou não, culpa em relação ao resultado, de qualquer modo, estando o sujeito na obrigação de compensar um dano, fica configurada a responsabilidade civil do mesmo[30].

Em complemento, é importante apontar que existem no ordenamento jurídico três principais tipos de responsabilidade civil, quais sejam: objetiva, subjetiva e pelo risco, como será demonstrado.

No tipo subjetivo, a responsabilidade de que o causador do dano deva ressarcir a vítima depende fundamentalmente da culpa, sendo a prova de que o agente assim agiu, o pressuposto indispensável para que o dever de indenizar seja imputado. Assim, a responsabilidade do causador nasce somente em virtude de uma ação realizada com dolo ou culpa[31].

No que tange à responsabilidade objetiva, esta decorre de atividade ilícita, dano e nexo causal, sendo a culpa não necessária para que ela seja caracterizada, podendo este elemento fazer parte da conduta do agente que causou o dano, ou não[32].

Não menos importante, na responsabilização pelo risco, o efeito jurídico que carrega a obrigação de reparar danos não tem conexão com um comportamento antijurídico ou culposo, podendo ocorrer inclusive mediante um ato lícito, ou ainda, pelo risco inerente ao exercício de uma atividade que cause danos injustos a terceiros, havendo em decorrência da atividade danosa a devida reparação dos danos experimentados pelo ofendido correndo por conta daquele que provocou o prejuízo[33].

Em seção própria sobre o tema da responsabilidade e do ressarcimento de

---

[30] PEREIRA, Caio Mario da Silva. **Responsabilidade Civil.** Atualizado por Gustavo Tepedino. 13. ed, - Rio de Janeiro: Forense, 2022. p.31.
[31] GONÇALVES, Carlos Roberto. **Responsabilidade Civil.** 21.ed. São Paulo: SaraivaJur, 2022. p.57.
[32] CAVALIERI FILHO, Sergio. **Programa de Responsabilidade Civil**. 10. ed. São Paulo: Atlas, 2012. p.150.
[33] ROSENVALD, Nelson. **As Funções da Responsabilidade Civil**: a reparação e a pena civil. São Paulo: Atlas, 2013. p.37.

danos, a LGPD apresenta o modo como a lei responsabiliza o controlador e o operador que, em virtude do tratamento de dados que estejam executando, causarem danos de ordem patrimonial, moral, individual ou coletivo.

O artigo 42 da Lei 13.709/18 infere que se o dano - seja de ordem patrimonial, moral, individual ou coletivo - que for causado ao titular de dados tiver relação com a execução da atividade profissional do controlador ou do operador de dados coletados, estes estão obrigados proceder com a reparação daquilo que causaram[34].

A responsabilidade civil relativa às informações pessoais propriamente ditas, tem papel crucial na manutenção do equilíbrio entre as partes que estão envolvidas em uma relação comercial, principalmente quando essa relação ocorre em um ambiente tecnológico, pois, a tecnologia facilita a possibilidade de que perfis e preferências de consumo sejam delineados, de modo que, a partir daí, o titular tenha sua privacidade invadida, seja pelo uso de algoritmos ou outras tecnologias preditivas podendo, inclusive, afetar relações sociais, afetivas ou outras de foro privado dos titulares[35].

Por sua vez, o artigo 43 apresenta as hipóteses nas quais os agentes de tratamento de dados não serão responsabilizados, eximindo-os, portanto, da responsabilidade de ressarcir. Essa possibilidade é prevista pois os titulares de dados podem demandar uma empresa para que seja ressarcido de algum dano sofrido, acreditando erroneamente ter sido essa organização que realizou o tratamento, quando pode ter sido outra[36].

Já o artigo 44 da LGPD traz em seu conteúdo a questão da irregularidade no tratamento de dados pessoais, definindo que será irregular quando a manipulação não observar as leis ou quando não oferecer a segurança que, do ponto de vista do titular do dado, é esperada[37].

Por fim, o artigo que encerra a seção da lei relativa à responsabilidade civil, carrega o entendimento de que, no âmbito das relações de consumo, quaisquer

---

[34] BRASIL. **Lei nº 13.709. Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília, DF, 14 de agosto de 2018.

[35] BRUNO, Marcos Gomes da Silva. Capítulo VI – Dos Agentes de Tratamento de Dados Pessoais. *In*: MALDONADO, Viviane Nobre; BLUM, Renato Opice. **LGPD:** Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2019. p.257. E-book.

[36] BRUNO, Marcos Gomes da Silva. Capítulo VI – Dos Agentes de Tratamento de Dados Pessoais. *In*: MALDONADO, Viviane Nobre; BLUM, Renato Opice. **LGPD:** Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2019. p.261. E-book.

[37] BRASIL. **Lei nº 13.709. Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília, DF, 14 de agosto de 2018.

violações sofridas pelo titular no que se refere a seus dados, estarão cobertas também por aquela legislação[38].

Outro aspecto de suma importância entre a Lei Geral de Proteção de Dados Pessoais e o instituto da responsabilidade civil que precisa ser ventilado, é a questão referente à natureza da responsabilidade no contexto da LGPD, pois, nos artigos desta lei não fica evidenciado se a responsabilidade civil adotada é de cunho objetivo ou subjetivo.

De um lado estão aqueles que defendem a responsabilidade objetiva sob o argumento embasado nas influências e semelhanças que a Lei 13.709/18 apresenta perante o Código de Defesa do Consumidor, como exemplo a semelhança do caput do artigo 43 da LGPD com o §3º dos artigos 12 e 14 do CDC[39].

No outro espectro apresentam-se os defensores da responsabilidade subjetiva, na qual a culpa pelo dano que gera a responsabilidade de indenizar, é um fundamento da LGPD, pelo fato desta estar pautada em deveres por parte daqueles que irão manipular dados, o que coaduna com o fato de que se o legislador criou uma série de deveres de cuidado, à falta desses cuidados, verifica-se a culpa daqueles operadores responsáveis pelo tratamento danoso[40].

A despeito de terem sido pontuados os vieses tanto da responsabilidade subjetiva, quanto da objetiva que permeiam o instituto da Lei Geral de Proteção de Dados Pessoais, a opinião deste autor é de que a responsabilidade civil daquele que está tratando dados é afeta ao risco da atividade, pois entendo que o proveito econômico que é auferido por aquele que trata dados é o principal motivador para que o faça, de modo que, assim, não há que se falar em culpa, ou a falta dela, mas sim, de uma escolha por assim proceder, importando em que o responsável pelo tratamento toma para si todos os riscos inerentes de tal decisão.

Para encerrar o tema da responsabilidade civil afeta à Lei Geral de Proteção de Dados Pessoais, apresenta-se um precedente do Superior Tribunal de Justiça no julgamento do AResp 2130619/SP, no qual verifica-se que o entendimento do egrégio

---

[38] BRUNO, Marcos Gomes da Silva. Capítulo VI – Dos Agentes de Tratamento de Dados Pessoais. *In*: MALDONADO, Viviane Nobre; BLUM, Renato Opice. **LGPD:** Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2019. p.264. E-book.

[39] TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. **Fundamentos do Direito Civil:** Responsabilidade Civil. 2 ed. Rio de Janeiro: Forense, 2021. E-book. p.436.

[40] TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. **Fundamentos do Direito Civil:** Responsabilidade Civil. 2 ed. Rio de Janeiro: Forense, 2021. E-book. p.437.

tribunal é de que o dever de indenizar nasce somente após a comprovação efetiva do dano experimentado pelo titular do dado que vazou, de modo que, o simples vazamento sem consequências danosas não modificou o *status quo* do titular, desta feita, não gera o dever de indenizar[41].

A análise da responsabilidade civil no escopo da LGPD mostra que a não adequação aos seus ditames pode gerar riscos regulatórios, jurídicos, financeiros, reputacionais e estratégicos para as empresas. Assim, a respectiva adequação não pode ser encarada somente como uma obrigação legal, mas sim, como parte do sistema de governança corporativa das empresas, haja vista que essa ferramenta congrega mecanismos de prevenção, controle, transparência e responsabilização que tocam diretamente as bases da LGPD, demonstrando que há interdependência entre eles.

Assim, num primeiro momento, serão apresentados os moldes como o tema da governança é elaborado no contexto da Lei Geral de Proteção de Dados, para que num segundo momento, seja discutido com um pouco mais de profundidade o tema da governança corporativa, propriamente dito.

2.3 Convergência Entre LGPD e Governança Corporativa

Para encerrarmos o capítulo referente à Lei Geral de Proteção de Dados Pessoais, serão delineados os pontos em que a lei toca o tema da governança corporativa, sem maiores definições sobre esse tema, cuja explanação mais ampla, será apresentada a partir do próximo capítulo.

Assim, observa-se que os artigos 50 e 51 da referida lei em exame tocam a temática das boas práticas e da governança, as quais ensejam a boa aplicação da lei, podendo ser pensadas de modo individual por cada empresa, ou através de associações, trazendo benefícios relevantes diante de uma uniformização de condutas sendo, inclusive, essencial para a manutenção das empresas a adaptação

---

[41] PROCESSUAL CIVIL E ADMINISTRATIVO. INDENIZAÇÃO POR DANO MORAL. VAZAMENTO DE DADOS PESSOAIS. DADOS COMUNS E SENSÍVEIS. DANO MORAL PRESUMIDO. IMPOSSIBILIDADE. NECESSIDADE DE COMPROVAÇÃO DO DANO.
I - Trata-se, na origem, de ação de indenização ajuizada por particular contra concessionária de energia elétrica pleiteando indenização por danos morais decorrentes do vazamento e acesso, por terceiros, de dados pessoais.
V - O vazamento de dados pessoais, a despeito de se tratar de falha indesejável no tratamento de dados de pessoa natural por pessoa jurídica, não tem o condão, por si só, de gerar dano moral indenizável. Ou seja, o dano moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações.

e revisão constantes de seus processos pertinentes ao tratamento de dados, fazendo com que se mantenham conformes a lei[42].

> Há claramente um estímulo para que os agentes da iniciativa pública e privada formulem suas próprias regras e se autorregulem de acordo com as condições e peculiaridades da organização, e a sua forma de funcionamento. Isso porque, embora a LGPD seja soberana, a depender do setor econômico as normas de segurança e os padrões técnicos serão diferentes[43].

Ainda sobre esse tema, ao estimular a adoção de padrões técnicos que facilitem o controle dos dados pelos próprios titulares, através da implementação do que é conhecido como *privacy dashboard* (ferramenta na qual o próprio titular controla quais dados deseja permitir que o controlador tenha acesso), a lei aponta para uma oportunidade na qual as empresas possam se diferenciar, ganhar reputação e agregar valor em sua relação com os clientes, simplesmente cumprindo o que a lei institui, ganhando, ao final, vantagem competitiva[44].

3 GOVERNANÇA CORPORATIVA: HISTÓRICO, DEFINIÇÃO, ESTRUTURA, PRINCÍPIOS E SUA IMPORTÂNCIA PARA AS EMPRESAS

Nesta altura, já vistos os principais tópicos atinentes à privacidade e à Lei Geral de Proteção de Dados Pessoais que tocam o objetivo desta dissertação, passa-se agora à exposição dos aspectos relativos à governança corporativa, pois este é assunto de grande relevância para a gestão das organizações que seguem boas práticas de gestão com vistas a alcançar o equilíbrio de interesses entre todos os *stakeholders*, e também, como consequência, gerar valor e resultado para as empresas.

3.1 HISTÓRICO DA GOVERNANÇA CORPORATIVA

Para traçarmos um histórico da governança corporativa é necessário entender, primeiramente, como eram as relações empresariais no que tange a propriedade.

---

42 TEIXEIRA, Tarcisio. GUERREIRO, Ruth Maria. **Lei Geral de Proteção de Dados Pessoais:** comentada artigo por artigo. 4.ed. São Paulo: SaraivaJur, 2022. p.174-178.

43 JIMENE, Camila do Valle. Capítulo VII – Da segurança e das boas práticas. *In*: MALDONADO, Viviane Nobre; BLUM, Renato Opice. **LGPD:** Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2019. p.284. E-book.

44 TEIXEIRA, Tarcisio. GUERREIRO, Ruth Maria. **Lei Geral de Proteção de Dados Pessoais:** comentada artigo por artigo. 4.ed. São Paulo: SaraivaJur, 2022. p.177-178.

Inicialmente, a maioria das empresas tinham como seus proprietários famílias ou indivíduos que exerciam o controle integral. Contudo, com o início da negociação da propriedade dessas companhias no mercado de capitais, visualizou-se a dispersão dessa propriedade, nascendo a necessidade de separar propriedade e gestão, movimento este que ganhou maior volume especialmente após a segunda guerra mundial[45].

Com essa separação, a gestão passou a ser realizada por executivos, gestores e conselheiros que, muitas vezes, passaram a tomar decisões relativas à empresa em benefício próprio, de modo que, para minimizar esse conflito de interesses, foram sugeridas práticas de monitoramento, controle e divulgação das informações empresariais, fazendo com que a governança corporativa fosse difundida cada vez mais no meio empresarial[46].

Assim, a governança corporativa baseia-se em um conjunto de restrições que orientam as ações daqueles que administram uma determinada empresa, com o intuito de reduzir a alocação indevida de recursos dos investidores e, como consequência, obter melhores resultados, refletindo principalmente, no preço das ações desta empresa no mercado de capitais[47].

Cabe salientar que a implantação de um sistema de governança corporativa gera custos, porém, proporciona benefícios, seja pela sua valorização mercadológica, ou pela contenção dos conflitos de agência que, como consequência, proporcionam bons resultados contábeis (resultados financeiros) e de controle interno[48].

Marcos históricos estabeleceram o desenvolvimento do instituto da governança ao redor do mundo. Em 1976, Jensen e Meckling publicaram estudos realizados com

---

[45] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Portal do Conhecimento.** Disponível em: https://www.ibgc.org.br/conhecimento/governanca-corporativa. Acesso em: 01 set. 2025.

[46] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Portal do Conhecimento.** Disponível em: https://www.ibgc.org.br/conhecimento/governanca-corporativa. Acesso em: 01 set. 2025.

[47] MACHADO, Luiz Kennedy Cruz; PRADO, José Willer do; RAUBER, Laurí Luis; CARVALHO, Eduardo Gomes; SANTOS, Antônio Carlos dos. **A influência da governança corporativa no desempenho financeiro, na oportunidade de crescimento e no valor de mercado das firmas: uma análise com modelagem de equações estruturais.** Enfoque: Reflexão Contábil, Maringá/Pr, volume 39, número 2, p.29. Disponível em: https://periodicos.uem.br/ojs/index.php/Enfoque/article/view/45852 Acesso em 10 set 2025.

[48] MACHADO, Luiz Kennedy Cruz; PRADO, José Willer do; RAUBER, Laurí Luis; CARVALHO, Eduardo Gomes; SANTOS, Antônio Carlos dos. **A influência da governança corporativa no desempenho financeiro, na oportunidade de crescimento e no valor de mercado das firmas:** uma análise com modelagem de equações estruturais. Enfoque: Reflexão Contábil, Maringá/Pr, volume 39, número 2, p.29. Disponível em: https://periodicos.uem.br/ojs/index.php/Enfoque/article/view/45852 Acesso em 10 set 2025.

o foco em empresas britânicas e americanas, de modo que com esses estudos se deu origem à Teoria da Firma ou Teoria do Agente-Principal, que se caracterizavam quando o sócio (principal) contratava outra pessoa (agente) para a administração da empresa, os quais tinham a tendência de agir de forma a maximizar seus próprios benefícios (maiores salários, estabilidade, poder) agindo em interesse próprio, e não de acordo com os interesses do principal[49].

Nos anos 1990 originaram-se diversas discussões acadêmicas, legislativas e entre investidores, em decorrência de escândalos contábeis ocorridos na década anterior em importantes empresas, com isso, em 1992 foi publicado na Inglaterra o Relatório Cadbury, considerado o primeiro código de boas práticas de governança corporativa, e no mesmo ano, nos Estados Unidos, foi publicado o primeiro código de governança por uma empresa, a *General Motors*[50].

Assim, uma das razões fundamentais para o desenvolvimento da governança corporativa é combater os conflitos de agência, que podem ocorrer de três modelos distintos, quais sejam: no relacionamento entre acionistas e corporação, na atuação da diretoria executiva e na constituição dos conselhos administrativos[51].

Referente ao relacionamento entre acionistas e corporação, quando há a abertura de capital de uma empresa ocorre a separação entre propriedade e gestão. Nesse contexto, os acionistas minoritários passam a ter maior dificuldade no acesso a informações relativas à gestão da empresa. Em relação à diretoria executiva, a atuação desta passou a trazer conflitos com os interesses dos acionistas, principalmente, naquilo que permeia à instituição de autobenefícios exagerados, gestão de curto prazo com foco no pagamento de bônus, manipulação de resultados, dentre outros conflitos. Por fim, os conselhos de administração cuja formação tem o objetivo de atuarem nos interesses dos acionistas, passaram a não seguir tais diligências, de modo que, com a instituição da governança corporativa esses conselhos passaram a ser avaliados e cobrados[52].

---

[49] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Portal do Conhecimento.** Disponível em: https://www.ibgc.org.br/conhecimento/governanca-corporativa. Acesso em: 01 set. 2025.

[50] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Portal do Conhecimento.** Disponível em: https://www.ibgc.org.br/conhecimento/governanca-corporativa. Acesso em: 01 set. 2025.

[51] DA ROCHA, Claudia. Capítulo 3 – Boas práticas e governança corporativa na ótica da Lei Geral de Proteção de Dados. *In*: TEIXEIRA, Tarcisio. **Empresas e implementação da LGPD – Lei Geral de Proteção de Dados Pessoais.** 2. ed. rev., ampl. e atual. São Paulo: Editora Juspodivm, 2022. p.87.

[52] DA ROCHA, Claudia. Capítulo 3 – Boas práticas e governança corporativa na ótica da Lei Geral de Proteção de Dados. *In*: TEIXEIRA, Tarcisio. **Empresas e implementação da LGPD – Lei Geral de**

No Brasil, nos anos 1950 e 1960 havia o predomínio do acionista controlador familiar, contudo, já nos anos 1970 se desenvolveram os primeiros conselhos de administração autônomos e com divisão do poder entre os acionistas e aqueles que faziam a gestão das empresas, no dia a dia, em empresas como Mappin, Docas de Santos, Monteiro Aranha e Villares. Ato contínuo, em 1976 foi sancionada a Lei das Sociedades Anônimas, que dentre outras coisas, prevê a prática de divisão de poderes entre o conselho administrativo e a diretoria, e oferece cinco linhas orientativas, quais sejam: proteção do acionista minoritário; responsabilidade do acionista controlador; diversificação dos instrumentos de fiscalização; diferenciação entre companhia aberta e fechada; e definição dos interesses fundamentais que a sociedade anônima representa[53].

A seu turno, a abertura do mercado e as privatizações que ocorreram nos anos 1990 impulsionaram o movimento por boas práticas, de modo que, em 1995 foi criado o Instituto Brasileiro de Conselheiros em Administração (IBCA), que em 1999 passou a se chamar Instituto Brasileiro de Governança Corporativa (IBGC). Cabe pontuar que no início do século 21, o tema da governança corporativa ganhou ainda mais evidência com o acontecimento de escândalos corporativos envolvendo empresas norte-americanas como a *Enron*, a *WorldCom* e *Tyco*, que influenciaram a aprovação da Lei *Sarbanes-Oxley*, que trouxe em seu bojo definições acerca do tema[54].

Seguindo, será demonstrada a definição do que vem a ser governança corporativa.

3.2 Definição de Governança Corporativa

Como marco conceitual, o Código das Melhores Práticas de Governança Corporativa, em sua sexta edição define governança corporativa da seguinte forma:

> Governança Corporativa é um sistema formado por princípios, regras, estruturas e processos pelo qual as organizações são dirigidas e monitoradas, com vistas à geração de valor sustentável para a organização, para seus sócios e para a sociedade em geral. Esse sistema baliza a atuação dos agentes de governança e demais indivíduos de uma organização na

Proteção de Dados Pessoais. 2. ed. rev., ampl. e atual. São Paulo: Editora Juspodivm, 2022. p.87-88.

[53]BITTENCOURT, Carlos Magno Andrioli. **Governança corporativa e compliance:** planejamento e gestão estratégica. Curitiba: Contentus, 2020. Edição eletrônica. p.16.

[54] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Portal do Conhecimento.** Disponível em: https://www.ibgc.org.br/conhecimento/governanca-corporativa. Acesso em: 01 set. 2025.

> busca pelo equilíbrio entre os interesses de todas as partes, contribuindo positivamente para a sociedade e para o meio ambiente[55].

De outra banda, a Organização para a Cooperação e o Desenvolvimento Econômico (OCDE) em sua cartilha sobre os Princípios de Governação Corporativa do G20, indica que a governança corporativa envolve a dinâmica estabelecida entre a administração, os órgãos societários, os acionistas e demais interessados das organizações, além de estabelecer a estrutura e os mecanismos com os quais a organização é conduzida, definindo os objetivos e determinando os instrumentos necessários para alcançá-los, juntamente com as ferramentas que irão acompanhar este desempenho[56].

Ademais, importa dizer que a governança envolve sócios/acionistas, conselhos, diretorias, além de, auditoria independente, sendo um artifício robusto caracterizado por mecanismos de incentivos e monitoramento, cujo objetivo principal é garantir que o comportamento de todos os responsáveis pela administração da empresa, seja ético e afeto aos interesses dos acionistas[57].

A governança corporativa institui o modo como uma empresa é dirigida pelos executivos, considerando, dentre outros aspectos, como as contas são prestadas, como se dá o relacionamento entre sócios, gestores, órgãos ou pessoas que fiscalizam e monitoram a gestão, além daqueles que se relacionam com a empresa (funcionários, público, consumidores, fornecedores, comunidade em torno, o fisco e a sociedade em geral[58].

Como um fim em si mesma, a governança objetiva, em última análise, ser um sistema capaz de blindar os administradores, conselheiros, gestores e diretores de uma organização de tomarem decisões alheias aos interesses exclusivos da empresa e dos sócios.

---

[55] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das Melhores Práticas de Governança Corporativa**, 6a edição, São Paulo: [s.n.], 2023. p.17. Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=24640. Acesso em: 12 ago. 2025.

[56] ORGANIZAÇÃO PARA A COOPERAÇÃO E O DESENVOLVIMENTO ECONÔMICO. **Princípios de Governança Corporativa do G20/OCDE.** OCDE: Paris, 2024. p.7. Disponível em: https://www.oecd.org/content/dam/oecd/pt/publications/reports/2023/09/g20-oecd-principles-of-corporate-governance-2023_60836fcb/58478f0f-pt.pdf. Acesso em: 01 set. 2025

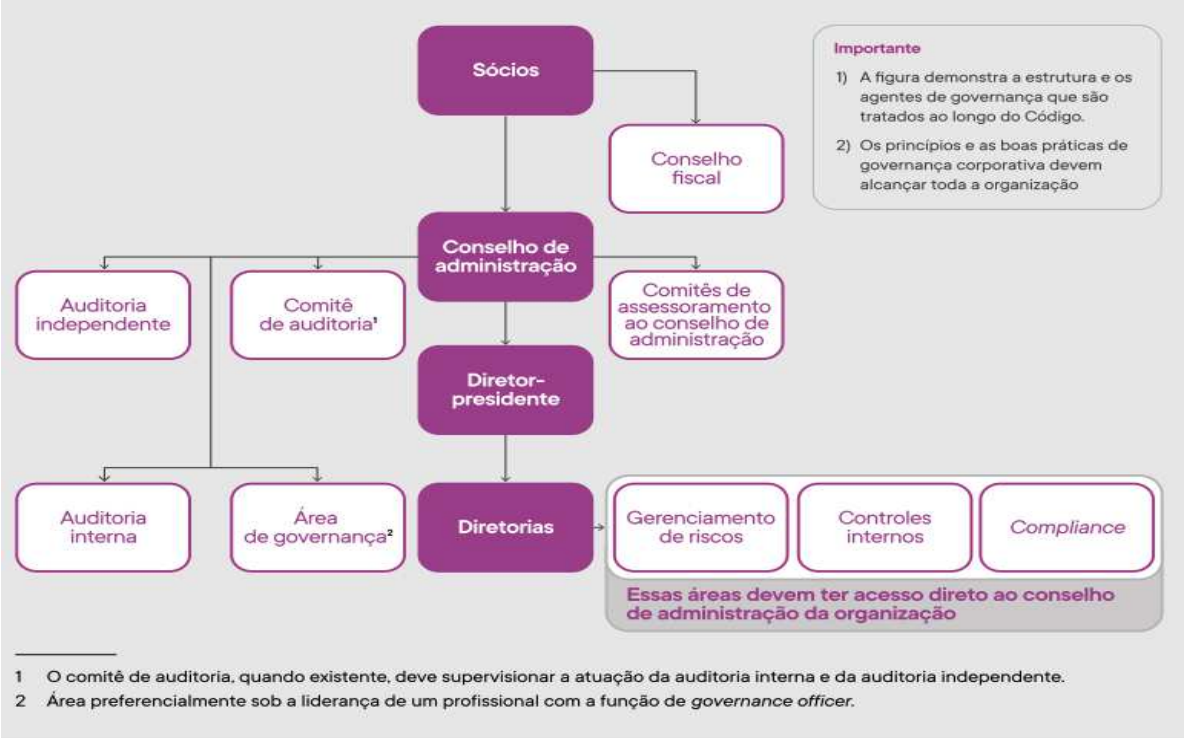
[57] TEIXEIRA, Tarcisio. **Direito Empresarial Sistematizado**. 12. ed. São Paulo: SaraivaJur, 2024. p. 164-165.

[58] PRADO, Roberta Nioac. **Manual prático e teórico da empresa familiar:** organização patrimonial, planejamento sucessório, governança familiar e corporativa e estratégias societárias e sucessórias (Governança jurídica). São Paulo: SaraivaJur, 2023. p.8.

3.3 Estrutura de Governança Corporativa

Definido o que vem a ser o instituto da governança corporativa, apresenta-se, na sequência, um organograma que demonstra as partes que compõem uma estrutura de governança, bem como as relações existentes entre elas:

Figura 1 - Estrutura de Governança Corporativa.



Fonte: Instituto Brasileiro de Governança Corporativa[59].

Verifica-se o posicionamento dos sócios no topo do organograma, haja vista a responsabilidade que esses têm de zelar pelos interesses organizacionais e apresentar pautas fundamentais para o desenvolvimento da organização. Dentre as funções dos sócios estão: a) a escolha/destituição de conselheiros administrativos; b) aprovar remuneração de administradores; c) deliberar sobre assuntos financeiros importantes, bem como aqueles relacionados ao estatuto/contrato social da empresa; d) alterar a estrutura acionária ou societária da empresa[60].

Por sua vez, o conselho de administração tem o viés de ser o responsável pela manutenção do propósito, dos valores, do objeto social e da governança da

[59] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). **Código das Melhores Práticas de Governança Corporativa.** 6. ed. São Paulo: IBGC, 2023. p. 20. Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=24640. Acesso em: 9 maio 2025.
[60] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das Melhores Práticas de Governança Corporativa**, 6a edição, São Paulo: [s.n.], 2023. p.23. Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=24640. Acesso em: 12 ago. 2025.

organização. Além disso, é a partir das deliberações desse conselho que são definidas estratégias corporativas (e o acompanhamento do cumprimento dessas). Por fim, é através deste ente de governança que a gestão executiva e os sócios se conectam[61].

Por fim, as diretorias executam as estratégias aprovadas pelo conselho administrativo, buscando meios para o alcance dos objetivos, sejam financeiros ou não[62].

Com o histórico, conceito, bem como a espinha dorsal de uma estrutura de governança corporativa delineados, doravante é fundamental apresentar os princípios relativos ao tema da governança.

3.4 Princípios de Governança Corporativa

Como já visto neste texto, os princípios delimitam como algo deve ser utilizado/aplicado no contexto em que se estabelecem, e para os quais esse algo foi criado, seja uma lei, um regulamento, um contrato, um estatuto ou outro regimento qualquer.

> Os Princípios não são vinculativos e não têm por objetivo fornecer prescrições pormenorizadas para a legislação nacional. Os Princípios não substituem nem devem ser considerados como substitutos à legislação e a regulamentação nacionais. Em vez disso, procuram identificar objetivos e sugerir vários meios para os alcançar, envolvendo normalmente elementos de legislação, regulamentação, regras de admissão à negociação em bolsa, acordos de autorregulação, compromissos contratuais, compromissos voluntários e práticas comerciais. A aplicação dos Princípios por uma jurisdição dependerá do contexto jurídico e regulamentar nacional. Os Princípios têm por objetivo fornecer uma referência sólida, mas flexível, para que os legisladores (*Policy Makers*), e os participantes no mercado desenvolvam as suas próprias estruturas de Governança Corporativa. Para se manterem competitivas num mundo em mudança, as sociedades têm de inovar e adaptar as suas práticas de Governança Corporativa para satisfazerem novas exigências e aproveitarem novas oportunidades. Tendo em conta os custos e os benefícios da regulamentação, os governos têm uma importante responsabilidade na definição de um quadro regulamentar eficaz, que preveja uma flexibilidade suficiente para permitir que os mercados funcionem eficazmente e respondam às novas expectativas dos acionistas e das partes interessadas. Os próprios Princípios são de natureza evolutiva e são revistos à luz de alterações significativas das circunstâncias, a fim de manterem o seu papel de principal padrão internacional de apoio aos legisladores no domínio da Governança Corporativa[63].

---

[61] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das Melhores Práticas de Governança Corporativa**, 6a edição, São Paulo: [s.n.], 2023. p.31. Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=24640. Acesso em: 12 ago. 2025.

[62] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das Melhores Práticas de Governança Corporativa**, 6a edição, São Paulo: [s.n.], 2023. p.53. Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=24640. Acesso em: 12 ago. 2025.

[63] ORGANIZAÇÃO PARA A COOPERAÇÃO E O DESENVOLVIMENTO ECONÔMICO. **Princípios de Governança Corporativa do G20/OCDE.** OCDE: Paris, 2024. p.7. Disponível em:

Com o instituto da governança corporativa não é diferente, esta se reveste de princípios que devem ser preservados e aplicados durante a prática dessa ferramenta de gestão. Assim, de acordo com o Instituto Brasileiro de Governança Corporativa, são cinco os princípios a serem seguidos, quais sejam: princípio da integridade, da transparência, da equidade, da responsabilização e da sustentabilidade, os quais serão demonstrados de modo independente na sequência.

Para o escopo deste trabalho iremos pautar nossa discussão formulando um pouco mais sobre os princípios que o IBGC relaciona, contudo, é possível que sejam encontrados na doutrina outros princípios afetos ao tema da governança corporativa, podendo alguns desses princípios ter o mesmo objetivo dos apontados anteriormente, contudo, com nomenclaturas distintas, como exemplo: princípio da eticidade, princípio da moralidade, princípio do ativismo societário, princípio da independência dos administradores, princípio da responsabilidade do administrador, princípio da razoabilidade e princípio da função social da empresa[64].

De fato, é através de ações coerentes e que atendam estritamente os interesses organizacionais que se pode vislumbrar a possibilidade de que uma empresa está sendo bem gerida e tendo seus recursos utilizados em prol da sua própria longevidade e na geração de retorno aos acionistas.

3.4.1 Princípio da Equidade

Este princípio busca tratar de forma igual os acionistas majoritários e minoritários, os sócios, outros interessados na empresa, sem que haja discriminação entre eles, de modo que todos possam exercer suas funções, bem como, cumprir com as obrigações pertinentes ao cargo e, também, gozar dos direitos inerentes à função que possuem[65].

Um exemplo de mecanismo de governança corporativa utilizado para manter a equidade é o *tag along*, que protege o acionista minoritário de grandes vendas de ações realizadas pelos majoritários e a consequente mudança societária não

---

https://www.oecd.org/content/dam/oecd/pt/publications/reports/2023/09/g20-oecd-principles-of-corporate-governance-2023_60836fcb/58478f0f-pt.pdf. Acesso em: 01 set. 2025.

[64] LOBO, Jorge. **Princípios de Governança Corporativa.** Revista do Ministério Público. Rio de Janeiro: MPRJ, número 31, jan./mar. 2009. Disponível em: https://www.mprj.mp.br/documents/20184/2716675/Jorge_Lobo.pdf. Acesso em: 28 de ago. 2025.

[65] NEVES, Edmo Colnaghi. **Fundamentos de governança corporativa:** riscos, direito e *compliance*. Curitiba: Editora InterSaberes, 2021. Edição eletrônica. p. 92.

esperada, de sorte que com o uso dessa ferramenta, os acionistas minoritários passam a ter o direito de vender suas ações em condições semelhantes com as quais os majoritários venderam as suas ações[66].

Fica claro através desse exemplo que o não cumprimento da equidade entre os envolvidos diretamente na gestão de uma companhia pode trazer consequências indesejadas, principalmente àqueles que têm menor influência na gestão como um todo por serem donos de uma fatia menor das ações.

3.4.2 Princípio da Responsabilização (*Accountability*)

Esse princípio aduz que as funções dos envolvidos na gestão da organização devem ser realizadas com diligência, independência, objetivando a geração de valor no longo prazo e garante que cada um assuma a responsabilidade pelas consequências dos seus atos e omissões. Ademais, a prestação de contas da atuação de todos os envolvidos é uma determinação deste princípio[67].

Verifica-se, por meio desse princípio, uma maneira de blindagem para que medidas arbitrárias que influenciem a organização como um todo sejam tomadas por aqueles que, seja qual for o nível que estejam alocados, terão que prestar contas e se responsabilizar pelo que decorre em virtude de seus atos.

No contexto da gestão de dados pessoais que são tratados, este princípio se apresenta de modo essencial, principalmente por ser o tratamento de dados eivado de importância na medida que um possível vazamento pode gerar consequências catastróficas à organização como um todo, seja de ordem jurídica, reputacional ou, principalmente, econômica.

3.4.3 Princípio da Transparência

Por força deste princípio, informações relativas a processos, indicadores, auditorias, desempenho econômico-financeiro, dentre outros dados, devem ser apresentados pela alta administração a todos os interessados na organização, especialmente para os acionistas, mais do que isso, é desejoso que a gestão da

---

66 NEVES, Edmo Colnaghi. **Fundamentos de governança corporativa:** riscos, direito e *compliance*. Curitiba: Editora InterSaberes, 2021. Edição eletrônica. p. 93.

67 INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das Melhores Práticas de Governança Corporativa**, 6a edição, São Paulo: [s.n.], 2023. p.18. Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=24640. Acesso em: 12 ago. 2025.

empresa tenha como agenda a disponibilização dessas informações de modo recorrente trazendo clareza do que está sendo feito com o dinheiro investido na empresa[68].

Não é nosso objetivo aqui esgotar todo o conteúdo sobre os princípios, contudo, entidades reguladoras brasileiras como é o caso da CVM (Comissão de Valores Mobiliários), tem nesse princípio um dos pilares da sua atuação de modo a assegurar a proteção dos investidores e garantir a eficiência do mercado, exigindo que informações das empresas de capital aberto sejam, com uma determinada frequência, disponibilizadas de forma pública.

3.4.4 Princípio da Sustentabilidade

Este princípio preconiza que os gestores devem zelar sempre pela viabilidade econômica das organizações que administram, reduzir externalidades negativas, ao passo que, devem aumentar as positivas referentes ao capital institucional seja ele, financeiro, intelectual, humano, social ou reputacional. Para isso, os administradores devem considerar que as companhias estão alocadas em uma relação de interdependência com a sociedade, com a economia e com o ambiente e a sociedade que a cerca[69].

No contexto da proteção de dados, é de extrema importância que esse princípio de governança seja seguido, pois, com a importância que os dados pessoais têm na sociedade contemporânea, um simples vazamento pode afetar de modo profundo e negativo toda a credibilidade que uma determinada companhia tem junto a seus clientes, mesmo que em virtude desse incidente não sejam ocasionados prejuízos diretos aos titulares de dados.

3.4.5 Princípio da Integridade

Através do princípio da integridade as organizações devem aprimorar a cultura ética no dia a dia da empresa em todas as esferas administrativas, para que, com isso, decisões não sejam tomadas com interesses conflitantes, mantendo a coerência

---

[68] ASSI, Marcos. **Governança, riscos e compliance:** mudando a conduta nos negócios. São Paulo: Saint Paul Editora, 2017. Edição eletrônica. p.20.

[69] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das Melhores Práticas de Governança Corporativa**, 6a edição, São Paulo: [s.n.], 2023. p.18. Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=24640. Acesso em: 12 ago. 2025.

entre discurso e ação, preservando a lealdade e o cuidado com as partes interessadas[70].

Escândalos corporativos normalmente são ocasionados por condutas atípicas no que diz respeito à integridade dos envolvidos, impactando consideravelmente as empresas, inclusive, levando algumas dessas empresas à insolvência. Assim, consolidar uma cultura ética é um dos meios de evitar esses acontecimentos, e para que isso seja implementado, é necessária dedicação contínua da alta administração.

Apresentar o tema da governança corporativa tem o viés de demonstrar que a adoção de práticas estruturadas de gestão, controle, transparência e prestação de contas são capazes de melhorar o desempenho, a reputação e, como consequência, a longevidade das organizações.

> Assim, as boas práticas de governança corporativa fazem com que princípios se tornem recomendações objetivas, de modo a alinhar interesse com a finalidade de preservar e otimizar o valor econômico da corporação, contribuindo para a sua longevidade e o bem comum[71].

Com a apresentação dos princípios da governança corporativa apresentados, passa-se a explorar a relação entre este tema e a privacidade de dados.

3.5 Implementação da Governança Corporativa na Proteção de Dados

Vistos o histórico, o conceito, a estrutura e os princípios da governança corporativa será apresentado, na sequência, como se dá a implementação desta no âmbito da proteção de dados.

No que toca à implementação da governança corporativa no terreno da proteção de dados, a Lei Geral de Proteção de Dados Pessoais, permite que controladores e operadores possam criar, individualmente ou em conjunto, suas próprias regras de boas práticas e governança voltadas à proteção de dados pessoais. Tais regras, todavia, devem ser elaboradas levando em consideração aspectos como a natureza e a finalidade do tratamento, além do volume dos dados a serem tratados, bem como os riscos e benefícios associados a essa atividade[72].

---

[70] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das Melhores Práticas de Governança Corporativa**, 6a edição, São Paulo: [s.n.], 2023. p.18. Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=24640. Acesso em: 12 ago. 2025.

[71] DA ROCHA, Claudia. Capítulo 3 – Boas práticas e governança corporativa na ótica da Lei Geral de Proteção de Dados. *In*: TEIXEIRA, Tarcisio. **Empresas e implementação da LGPD – Lei Geral de Proteção de Dados Pessoais.** 2. ed. rev., ampl. e atual. São Paulo: Editora Juspodivm, 2022. p.92.

[72] JIMENE, Camila do Valle. Capítulo VII – Da segurança e das boas práticas. *In*: MALDONADO,

Ademais, no escopo da LGPD, os programas de privacidade devem ser proporcionais à estrutura e à complexidade das operações da organização, considerando, também, a sensibilidade dos dados tratados e os possíveis impactos em caso de incidentes, mostrando que não é razoável exigir o mesmo rigor para organizações de tamanhos distintos[73].

Verifica-se, em complemento, que a própria LGPD em seu artigo 50, inciso I, apresenta os requisitos mínimos para que um programa de privacidade seja implementado[74].

A figura 2 representa esses requisitos para a implementação da governança corporativa no campo da proteção de dados, organizados em quatro etapas fundamentais, são elas: preparação da organização, análise organizacional, implementação e monitoramento.

Figura 2: Etapas da implementação da Governança Corporativa no âmbito da proteção de dados.

Viviane Nobre; BLUM, Renato Opice. **LGPD:** Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2019. p.285. E-book.

[73] JIMENE, Camila do Valle. Capítulo VII – Da segurança e das boas práticas. *In*: MALDONADO, Viviane Nobre; BLUM, Renato Opice. **LGPD:** Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2019. p.285. E-book.

[74] I - Implementar programa de governança em privacidade que, no mínimo:
a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
g) conte com planos de resposta a incidentes e remediação; e
h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

Fonte: André Gustavo Bastos Fagundes[75].

Em relação às quatro etapas apresentadas anteriormente, temos que[76]:

> I) Preparação da organização - a) demonstrar o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; b) ser aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta; II) Análise Organizacional - c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados; III) Implementação - d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade; e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular; f) esteja integrado à sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos; g) conte com planos de resposta a incidentes e remediação; e IV) Monitoramento - h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

Sobre essa estrutura apresentada, nota-se que a implementação da governança em proteção de dados não é apenas a criação de normas internas, mas sim, trata-se de um processo dinâmico e contínuo, que tem como ponto de partida o comprometimento institucional e a capacidade de adaptação às mudanças regulatórias, tecnológicas e organizacionais. Como vantagem dessa adoção, a

[75] LIMA, André Gustavo Bastos; FAGUNDES, Vladimir. Implementação da Governança em Privacidade e Proteção de Dados. In: BARRETO, Gileno Gurjão; ANTONIO, André Luiz Sucupira; LIMA, André Gustavo Bastos. **Governança em privacidade e proteção de dados:** uma visão integrada aos negócios empresariais. 1.ed. Curitiba: Editorial Casa, 2022. p.19.

[76] LIMA, André Gustavo Bastos; FAGUNDES, Vladimir. Implementação da Governança em Privacidade e Proteção de Dados. *In*: BARRETO, Gileno Gurjão; ANTONIO, André Luiz Sucupira; LIMA, André Gustavo Bastos. **Governança em privacidade e proteção de dados:** uma visão integrada aos negócios empresariais. 1.ed. Curitiba: Editorial Casa, 2022. p.19.

organização que agrega a governança corporativa no que toca o tema da privacidade, ganha com a incorporação de cultura de proteção de dados em seu dia a dia.

Ademais, observa-se que as quatro etapas descritas possuem caráter interdependente, de modo que falhas em uma delas podem comprometer a eficácia de todo o programa de governança. A preparação inadequada, por exemplo, pode resultar em políticas meramente formais, sem efetividade prática; uma análise organizacional superficial pode levar à adoção de medidas desproporcionais ou insuficientes; já a implementação sem integração à governança corporativa tende a gerar iniciativas isoladas e pouco sustentáveis.

Por fim, o monitoramento contínuo revela-se essencial para garantir a atualização e a melhoria constante do programa, permitindo a identificação de vulnerabilidades, a correção de falhas e o fortalecimento da confiança dos titulares e do mercado nas práticas adotadas pela organização.

A seu turno, a norma NBR ISO/IEC 27701[77] apresenta os atributos que facilitam, sob a ótica da governança corporativa, a adequação das empresas à Lei Geral de Proteção de Dados Pessoais, que em seu contexto, ela denomina como um Sistema de Gestão de Privacidade da Informação – SGPI, são eles:

a) Entendendo a organização e seu contexto: a organização deve determinar o seu papel como um controlador de dados pessoais (incluindo a condição de controlador conjunto de dados pessoais) e/ou como um operador de dados pessoais. A organização deve determinar os fatores externos e internos que são pertinentes para o seu contexto e que afetam a sua capacidade de alcançar os resultados pretendidos do seu SGPI;

b) Entendendo as necessidades e as expectativas das partes interessadas: a organização deve incluir entre as suas partes interessadas, aquelas partes que têm interesses ou responsabilidades associados ao tratamento de dados pessoais, incluindo os titulares de dados pessoais;

c) Determinando o escopo do sistema de gestão da segurança da informação: ao determinar o escopo do SGPI, a organização deve incluir o tratamento de dados pessoais;

d) Sistema de gestão da segurança da informação: a organização deve

[77] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27701:2019** – Técnicas de segurança — Extensão para a ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes. Rio de Janeiro: ABNT, 2019.

estabelecer, implementar, manter e melhorar continuamente um SGPI.

No âmbito da União Europeia, o GDPR, em seu artigo 24, atribui aos controladores o dever de implementar medidas técnicas e organizacionais, de modo a trazer mais segurança e para comprovar que o tratamento de dados está em conformidade com o regulamento. Ainda a lei europeia sobre proteção de dados, estatui que as medidas que forem implementadas devam ser revisadas e atualizadas por meio de políticas e códigos de conduta, além de serem possíveis de demonstração[78].

Em semelhança com a LGPD, o GDPR no artigo 40, alínea 1, através dos estados-membros, também incentiva a elaboração de códigos de conduta destinados a contribuir para a correta aplicação da lei, tendo em conta as especificidades dos vários setores de transformação e as necessidades específicas das micro, pequenas e médias empresas[79].

Em seu artigo 40, alínea 2, aponta que associações e outras entidades que representam categorias de controladores ou processadores podem elaborar, alterar ou ampliar códigos de conduta, com o objetivo de especificar a aplicação da lei de proteção de dados no contexto europeu, no que diz respeito aos seguintes temas: a) processamento justo e transparente; b) os interesses legítimos perseguidos pelos controladores em contextos específicos; c) a coleta de dados pessoais; d) a pseudonimização de dados pessoais; e) as informações fornecidas ao público e aos titulares dos dados; f) o exercício dos direitos dos titulares dos dados; g) as informações fornecidas às crianças, a proteção destas e a forma como o consentimento dos responsáveis legais pelas crianças deve ser obtido; h) a notificação de violações de dados pessoais às autoridades de supervisão e a comunicação dessas violações de dados pessoais aos titulares dos dados; i) a transferência de dados pessoais para países terceiros ou organizações internacionais; j) ou procedimentos extrajudiciais e outros procedimentos de resolução de litígios para

---

[78] UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas físicas 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 – GDPR).** Jornal Oficial da União Europeia, L119, 4 maio 2016.

[79] UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas físicas 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 – GDPR).** Jornal Oficial da União Europeia, L119, 4 maio 2016.

resolver litígios entre controladores e titulares de dados relativamente ao tratamento, sem prejuízo dos direitos dos titulares de dados nos termos dos artigos 77 e 79[80].

Há de se ressaltar, todavia, que a governança da proteção de dados, é uma espécie do gênero governança corporativa, que relaciona diversas disciplinas tendo como prioridade: a qualidade de dados coletados, gerência, melhoria e monitoramento do uso desses dados. Para atingir tal nível de governança é necessário que as empresas definam objetivos organizacionais e processos que envolvam, principalmente, as áreas de tecnologia e de negócios[81].

A Portaria 58/2016[82] que dispõe sobre os procedimentos complementares para o compartilhamento de bases de dados oficiais entre órgãos e entidades da administração pública federal direta e indireta e as demais entidades controladas direta ou indiretamente pela União, em seu artigo 2º, inciso VI, define governança da privacidade da proteção de dados como o conjunto de políticas, processos, pessoas e tecnologias cujo objetivo é estruturar e administrar os ativos de informação, de modo a aprimorar a eficiência dos processos de gestão e da qualidade dos dados, com o fito de promover eficiência operacional e garantir que informações que suportam a tomada de decisão sejam confiáveis.

Um estudo da consultoria KPMG intitulado “Conselho de Administração: prioridades para a agenda 2024”, assim preleciona sobre a abrangência da governança de dados[83]:

> A governança de dados abrange o cumprimento a leis e regulamentos específicos para cada setor da indústria, bem como normas e regulamentos de privacidade que estabelecem como os dados pessoais – de clientes, funcionários ou fornecedores – são processados, armazenados, coletados e

---

[80] UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas físicas 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 – GDPR).** Jornal Oficial da União Europeia, L119, 4 maio 2016.

[81] BARBIERI, Carlos; FARINELLI, Fernanda. **Uma visão sintética e comentada do Data Management Body of Knowledge (DMBOK).** FUMSOFT. 16 abr. 2024.Disponível em:https://www.researchgate.net/publication/297699158_Uma_visao_sintetica_e_comentada_do_Data_Management_Body_of_Knowledge_DMBOK. Acesso em: 13 abr. 2026.

[82] BRASIL. **Portaria nº 58/2016 da Secretaria de Tecnologia da Informação do Ministério do Planejamento, Desenvolvimento e Gestão**. Disponível em https:// www.gov.br/conarq/pt-br/legislacao-arquivistica/portarias-federais/portaria-no-58-de-23-de-dezembrode2016#:~:text=Disp%C3%B5e%20sobre%20os%20procedimentos%20complementares,direta%20ou%20indiretamente%20pela%20Uni%C3%A3o. Acesso em 19 abr. 2026.

[83] KPMG Board Leadership Center. **Conselho de Administração:** prioridades para a agenda de 2024. Disponível em: https://kpmg.com/br/pt/insights/2024/02/conselho-de-administracao-2024.html. Acesso em: 10 abr. 2026.

> utilizados. A governança de dados também inclui políticas e protocolos relativos à ética de dados, em particular, o gerenciamento do atrito entre o modo como a empresa pode utilizar os dados dos clientes de uma forma legalmente permitida e as expectativas do cliente sobre como seus dados serão utilizados. Gerenciar esses desafios impõe riscos significativos à reputação e à confiança das empresas, representando um desafio crítico para a liderança.

A tabela a seguir apresenta, dentro da governança de dados, os níveis de gerenciamento, bem como suas responsabilidades e quem são os responsáveis por cada tarefa.

Tabela 2: Níveis de gerenciamento na Governança de Dados.

NÍVEL	RESPONSABILIDADES	RESPONSÁVEIS
Executivo	- Oferecer patrocínio; - Prover apoio financeiro; - Apoiar o programa de Governança de Dados;	- Gerência Executiva
Estratégico	- Estabelecer Políticas e Procedimentos; - Estabelecer Políticas de Governança de Dados, procedimentos e padrões para áreas de negócios, processos de negócios e tecnologia;	- Gerência de Governança de Dados; - Gestores de Dados;
Gestor de Dados	- Acompanhar as aplicações de Governança de Dados nas áreas; - Facilitar e gerenciar a interação de Governança de Dados;	- Gestores de Informações de projetos/áreas envolvidas; - Gestor de Dados;
Execução	- Implementar e executar as políticas e procedimentos; - Projetar e implementar as políticas de dados e procedimentos nos processos específicos de negócios e aplicações; - Executar as políticas de dados e procedimentos nos processos e aplicações no dia a dia.	- Gestores de Dados; - Equipes de projetos que implementam processos de negócios e aplicações; - Qualquer ator que “impacta” a informação nos processos de negócios do dia a dia.

Fonte: elaborado pelo autor[84].

Isto posto, pode-se constatar que a implementação da governança corporativa, no âmbito da proteção de dados, não se caracteriza apenas pela institucionalização de diretrizes advindas da lei, mas sim, é composta de um sistema estruturado e

[84] Adaptado de BARBIERI, Carlos. **Uma visão sintética e comentada do Data Management Body of Knowledge** (DMBOK). Funsoft: Belo Horizonte, 2013.

contínuo. Com efeito, a construção de um programa de governança em privacidade de dados exige a integração entre áreas da empresa, definição clara de responsabilidades e alinhamento estratégico com os objetivos da empresa, impactando a cultura organizacional e comprometimento da alta gestão.

Em complemento, a governança de dados sendo um desdobramento da governança corporativa, tem papel essencial na qualidade da informação, na mitigação de riscos e no fortalecimento da confiança entre organização, titulares de dados e o mercado.

Nesse sentido, a consolidação de práticas eficazes de governança em proteção de dados não somente atende às exigências legais, mas também, projeta-se como um fator de grande relevância para a geração de valor para as empresas, o que será visto a seguir.

3.6 Importância da Governança Corporativa na Geração de Valor Para as Empresas

A governança corporativa tornou-se, ao longo do tempo, elemento essencial para a gestão das organizações, sejam elas públicas, privadas, de capital aberto ou fechado, haja vista que através desse mecanismo a gestão se torna mais responsável, clara e eficaz. No Brasil, a utilização da governança ganhou força especialmente após a fundação do IBGC e de alguns fatos que ocorreram no mundo corporativo, principalmente com a privatização de grandes estatais e da abertura de capitais de grandes empresas até então particulares.

A adoção das ferramentas de governança corporativa, desde as mais simples até as mais elaboradas, melhora o desempenho organizacional contribuindo também para que o resultado das empresas seja mais relevante refletindo, especialmente, através do resultado financeiro, além do social, ambiental, reputacional e outros[85].

Ademais, quando negócios de grande porte incorporam os mecanismos de governança em sua gestão, seja por exigência regulatória ou não, estas empresas tornam-se mais atrativas ao investimento, o que facilita a captação de recursos e reduz

[85] MACHADO, Luiz Kennedy Cruz; PRADO, José Willer do; RAUBER, Laurí Luis; CARVALHO, Eduardo Gomes; SANTOS, Antônio Carlos dos. **A influência da governança corporativa no desempenho financeiro, na oportunidade de crescimento e no valor de mercado das firmas:** uma análise com modelagem de equações estruturais. Enfoque: Reflexão Contábil, Maringá/Pr, volume 39, número 2, p.20. Disponível em: https://periodicos.uem.br/ojs/index.php/Enfoque/article/view/45852 Acesso em 10 set. 2025.

o custo de aquisição de capital, contribuindo, por consequência, com a melhora no desempenho operacional, aumentando valor e rentabilidade[86].

Outrossim, a construção de reputação empresarial é, sobremaneira, facilitada com a adoção de práticas de governança, visto que esse valor é construído por meio das percepções acumuladas que os interessados/envolvidos nesta organização têm em relação ao negócio. O caráter reputacional espelha as interações, respaldadas em integridade e moralidade, que as empresas têm com seus fornecedores, clientes, investidores, a comunidade, dentre outros entes direta ou indiretamente ligados a ela[87].

Nessa toada, os relatórios emitidos pelos gestores (princípio da transparência) têm contribuição efetiva para que a reputação corporativa seja sempre majorada, influenciando, como já visto, diretamente o valor de mercado dessas organizações. É também notório que a inclusão da sustentabilidade corporativa (princípio da sustentabilidade) como um objetivo estratégico a ser alcançado pela gestão, impacta diretamente no desempenho financeiro empresarial[88].

Neste contexto, a governança surge como ponto central para orientar as decisões empresariais, reduzindo assimetrias informacionais, melhorando a coordenação entre os diversos níveis de gestão da empresa e fornecendo mecanismos de modo a ampliar a eficiência e a transparência, ao passo que conflitos de interesse sejam eliminados ou, ao menos, reduzidos[89].

Em complemento, o ambiente no qual as empresas contemporâneas estão alocadas é extremamente dinâmico e competitivo, exigindo cada vez mais velocidade

---

[86] MACHADO, Luiz Kennedy Cruz; PRADO, José Willer do; RAUBER, Laurí Luis; CARVALHO, Eduardo Gomes; SANTOS, Antônio Carlos dos. **A influência da governança corporativa no desempenho financeiro, na oportunidade de crescimento e no valor de mercado das firmas:** uma análise com modelagem de equações estruturais. Enfoque: Reflexão Contábil, Maringá/Pr, volume 39, número 2, p.20. Disponível em: https://periodicos.uem.br/ojs/index.php/Enfoque/article/view/45852 Acesso em 10 set. 2025.

[87] MAZZIONI, Sady. ASCARI, Camila. RODOLFO, Noele Martinuzo. DAL MAGRO, Cristian Baú. **Reflexos das práticas ESG e da adesão aos ODS na reputação corporativa e no valor de mercado.** Revista Gestão Organizacional. v.16, n. 3. 2023. p.61-62 Disponível em: https://bell.unochapeco.edu.br/revistas/index.php/rgo/article/view/7394. Acesso em: 2 out. 2025.

[88] MAZZIONI, Sady. ASCARI, Camila. RODOLFO, Noele Martinuzo. DAL MAGRO, Cristian Baú. **Reflexos das práticas ESG e da adesão aos ODS na reputação corporativa e no valor de mercado.** Revista Gestão Organizacional. v.16, n. 3. 2023. p.63 Disponível em: https://bell.unochapeco.edu.br/revistas/index.php/rgo/article/view/7394. Acesso em: 2 out. 2025.

[89] MAIER, Jerry Antonio Raitz. FERREIRA, Hugo Silva. **A Governança Corporativa e suas contribuições para as finanças empresariais: a importância da Governança Corporativa e do Chief Financial Officer (CFO) para as finanças empresariais.** Revista Científica Multidisciplinar O Saber. v.7, ed. Especial. Disponível em: https://submissoesrevistarcmos.com.br/rcmos/article/view/664/1427 Acesso em: 2 out. 2025.

nas respostas às demandas de mercado. Nesse espectro, ter uma gestão de informação/dados competente desempenha papel central, pois a articulação de dados favorece a inovação, o aprendizado organizacional e os processos internos, neste diapasão, as áreas de marketing e publicidade são bastante beneficiadas.

Quando a tecnologia entra nessa balança, haja vista a velocidade com que esta se desenvolve, transformando toda a sociedade, surgem novas demandas a serem administradas como a gestão de dados dos clientes, por exemplo, fazendo com que surjam regulações pelo Estado, e assim, nasçam novas funções e cargos responsáveis por essa operacionalização, podendo-se citar no âmbito do tratamento de dados pessoais os operadores e os encarregados de dados, além da figura essencial do *Data Protection Officer*, que será abordada mais adiante, para que as empresas possam cumprir com as atividades relativas ao *compliance* de dados[90].

Visto o modo como a governança corporativa pode afetar o valor das empresas, na sequência passa-se a apresentar o tema do *compliance e do compliance* de dados e a relação destes com a LGPD, haja vista que possuem estreita conexão com o tema abordado neste capítulo.

[90] MAIER, Jerry Antonio Raitz. FERREIRA, Hugo Silva. **A Governança Corporativa e suas contribuições para as finanças empresariais: a importância da Governança Corporativa e do Chief Financial Officer (CFO) para as finanças empresariais.** Revista Científica Multidisciplinar O Saber. v.7, ed. Especial. Disponível em: https://submissoesrevistarcmos.com.br/rcmos/article/view/664/1427 Acesso em: 2 out. 2025.

4 *COMPLIANCE, COMPLIANCE* DE DADOS E A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LEI 13.709/18

Fazendo um paralelo com o tema da governança corporativa apresentado anteriormente, o *compliance* deixou de atuar apenas como mecanismo preventivo contra a corrupção (como será visto), passando a exercer relevante função de gestão empresarial e efetivando a governança corporativa, contribuindo para a concretização dos princípios da equidade, transparência e prestação de contas, além de auxiliar na prevenção de sanções jurídicas e no fortalecimento da relação entre empresa e *stakeholders*.

Ao assegurar o cumprimento de processos internos, a definição de responsabilidades e a gestão de riscos, o *compliance* fortalece a transparência organizacional e reduz a ocorrência de irregularidades em diversas áreas das empresas, de modo que a implementação de um programa de *compliance* deve ser vista como investimento estratégico, capaz de proteger a reputação empresarial, evitar prejuízos financeiros e atender às exigências legais e de mercado[91].

4.1 DEFINIÇÃO, HISTÓRICO, PRINCÍPIOS E FUNÇÕES DO *COMPLIANCE*

A definição de *compliance* deriva do termo em inglês "*to comply*" que pode significar: cumprir, executar, satisfazer. Contudo, a tradução literal não define exatamente o que é esse instituto pois, para ter um sentido melhor definido, deve ser entendido que as empresas devem estar em compliance (*comply to*), que nesse caso, tem o viés de estar em conformidade com alguma lei, norma, regulamento (cumprindo, executando, satisfazendo). Ademais, o termo agrega princípios de integridade e conduta ética, de modo que, ter cultura de *compliance* é mais do que conhecer as normas, é ser correto, idôneo, ao passo que, estar em *compliance*, é estar em conformidade com leis e regulamentos[92].

Por sua vez, não estar em *compliance* oferece riscos às organizações, senão vejamos:

> Risco de *compliance* é o risco de sanções legais ou regulamentares, perdas

[91] ANDRADE, Renato Campos. **Compliance como realizador do ESG:** construção dos pilares com foco no ambiental [livro eletrônico]. São Paulo: Editora Dialética, 2024. p.11.
[92] BLOK, Marcela. **Compliance e Governança Corporativa.** 4. ed. Rio de Janeiro: Freitas Bastos, 2023. Versão eletrônica.

> financeiras ou mesmo perdas reputacionais decorrentes da falta de cumprimento de disposições legais, regulamentares, códigos de conduta etc. Entretanto, *compliance* vai além das barreiras legais e regulamentares, incorporando princípios de integridade e conduta ética. Portanto, deve-se ter em mente que, mesmo que nenhuma lei ou regulamento seja descumprido, ações que tragam impactos negativos para os "stakeholders" (acionistas, clientes, empregados etc.) podem gerar risco reputacional e publicidade adversa, comprometendo a continuidade de qualquer entidade. Para qualquer instituição, confiança é um diferencial de mercado. Em geral, as leis tentam estabelecer controles e maior transparência, mas estar em conformidade apenas com as leis não garante um ambiente totalmente em *compliance*. A efetividade do *compliance* está diretamente relacionada à importância que é conferida aos padrões de honestidade e integridade na instituição. O *compliance* deve começar pelo "topo" da organização, com o apoio da alta administração para a disseminação da cultura de *compliance*, com as atitudes dos executivos seniores, que devem "liderar pelo exemplo", e com o comprometimento dos colaboradores, que devem se conduzir pela ética e idoneidade[93].

De modo geral, *compliance* envolve um conjunto de regras e modelos de procedimentos éticos que tem o condão de orientar o comportamento de empresas e seus colaboradores, transcendendo para preocupações como marca, nome e reputação, através da adoção de procedimentos de controle de riscos e preservação de valores intangíveis que se coadunam com a estrutura societária, o compromisso efetivo da liderança e a estratégia da empresa. Como consequência, a prática do *compliance* acarreta mudança de mentalidade organizacional no ponto em que, mesmo que nenhuma lei esteja sendo descumprida, impactos negativos às partes interessadas na empresa sejam suprimidos, contribuindo com a manutenção da imagem e reputação organizacional[94].

No contexto corporativo, pode-se definir o *compliance* como a obediência às normas sobre prevenção e combate aos crimes e atos fraudulentos e corruptos, impondo aos obrigados sanções administrativas e até mesmo criminais[95].

No âmbito público, o *compliance* é visto, dentre outros institutos, no artigo 37 da Constituição Federal que apresenta os princípios que são obedecidos pela administração pública direta e indireta em seu funcionamento, são eles: princípio da legalidade, impessoalidade, moralidade, publicidade e eficiência[96], assim

---

[93] FEDERAÇÃO BRASILEIRA DE BANCOS – FEBRABAN. **Função de *Compliance*.** Coleção Instituto Febraban de Educação. p.11. Disponível em: https://www.febraban.org.br/7rof7swg6qmyvwjcfwf7i0asdf9jyv/sitefebraban/funcoescompliance.pdf. Acesso em: 12 out. 2025.

[94] FREITAS, Daniel Paulo Paiva. **Proteção e governança de dados.** Curitiba: Contentus, 2020. p.46.

[95] FEDERAÇÃO BRASILEIRA DE BANCOS – FEBRABAN. **Função de *Compliance*.** Coleção Instituto Febraban de Educação. p.11. Disponível em: https://www.febraban.org.br/7rof7swg6qmyvwjcfwf7i0asdf9jyv/sitefebraban/funcoescompliance.pdf. Acesso em: 12 out. 2025.

[96] BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da

explicados[97]: a) Princípio da Legalidade: a administração segue as determinações das legislações, que em última análise, é a vontade expressa pelo povo através dos seus representantes; b) Princípio da Impessoalidade: estabelece que o trato com o interesse público por parte das pessoas seja imparcial, impedindo discriminações e privilégios; c) Princípio da Moralidade: fundamenta as práticas de integridade da administração pública, apresentando padrões de probidade, ética, boa-fé, decoro, lealdade e honestidade aplicados no seio da administração; d) Princípio da Publicidade: reflete a transparência e a participação popular nos atos administrativos; e) Princípio da Eficiência: traz elementos de aprimoramento à gestão pública que possibilitam a transposição de práticas burocráticas por práticas mais simples e efetivas.

Traçando um breve histórico, o *compliance* surgiu no início do século XX nos Estados Unidos em um período no qual agências reguladoras começaram a ser capitaneadas pelo governo norte-americano; no mesmo período ocorreu a promulgação do *Food and Drug Act* no ano de 1906, com o intento de fiscalizar e regular atividades empresariais relacionadas à alimentação e à indústria farmacêutica da época. Já nos anos 1970, foi implementado um novo ordenamento jurídico naquele país, denominado *Foreign Corrupt Practices Act - FCPA* com o intuito de punir atos de corrupção[98] dentro e fora do país, desmotivando a concorrência desleal e protegendo as empresas americanas e o mercado de capitais[99].

Outra lei importante promulgada no território americano com o objetivo de frear fraudes empresariais foi a *Sarbanes-Oxley*, no ano de 2002. Esta lei surgiu no bojo de escândalos financeiros que selaram a falência da Enron Corporation[100] e da WorldCom, tendo como objetivo principal proteger investidores e melhorar a precisão e a confiabilidade das demonstrações financeiras das empresas de capital aberto.

República, 1988.

97 FREITAS, Daniel Paulo Paiva. **Proteção e governança de dados.** Curitiba: Contentus, 2020. p.53-54.

98 Investigações apontaram que pagamentos ilegais a políticos, partidos e agentes públicos estrangeiros realizados somente na década de 1970 somaram mais de 300 milhões de dólares e, é nesse contexto, que surgiu a FCPA.

99 TEIXEIRA, Tarcísio. KASEMIRSKI, André Pedroso. Capítulo 1 - *Compliance* (conformidade) de dados pessoais para microempresas: autorregulação regulada e requisitos para efetividade. *In:* **Empresas e implementação da LGPD – Lei Geral de Proteção de Dados Pessoais.** 2. ed. rev., ampl. e atual. São Paulo: Editora Juspodivm, 2022, p.25-28.

100 Fundada em 1985, sempre foi vista como uma empresa modelo no que tange a gestão. Tinha como atividade principal a exploração de gás natural e produção de energia, contudo com o tempo passou a diversificar seus ativos. Em 2001 pediu concordata com dívidas aproximadas de 22 bilhões de dólares, que foram por muitos anos encobertas através de fraudes contábeis.

Ainda no contexto americano, no ano de 2014 a Lei *Foreign Account Tax Compliance* Act – FATCA entrou em vigor com o intuito de combater a evasão fiscal[101].

No Brasil, entre a década de 1990 e o início dos anos 2000, o tema do *compliance* ganhou força especialmente através de exigências advindas da Comissão de Valores Mobiliários (CVM) e do Banco Central. Ato contínuo, esse instituto passou a ser, posteriormente, exigido de empresas públicas, sociedades de economia mista e suas subsidiárias[102].

O *compliance* é tratado no Brasil em diversas leis, dentre as principais pode-se citar:

> a) Lei 9.613/1998: dispõe sobre os crimes de lavagem ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos; cria o Conselho de Controle de Atividades Financeiras – COAF;
> b) Resolução 2.554/1998: determina a implantação de controles internos em instituições reguladas pelo Banco Central;
> c) Lei 12.529/2011: estrutura o Sistema Brasileiro de Defesa da Concorrência; dispõe sobre a prevenção e repressão às infrações contra a ordem econômica;
> d) Lei 12.846/2013 (Lei Anticorrupção): dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira;
> e) Decreto 11.129/2022: Regulamenta a Lei 12846/2013[103].

Essas leis objetivam prevenir crimes de corrupção, contra a ordem econômica, lavagem de dinheiro, dentre outros convergentes a atos de corrupção e que possam causar danos a uma grande coletividade.

Tendo sido definido e apresentado um breve histórico do instituto do *compliance*, passaremos a demonstrar os princípios inerentes a ele, os quais apresentam o modo como essa ferramenta deve ser elaborada e mantida pelas corporações para que seja efetiva ao que se propõe. A tabela a seguir apresenta dez princípios de *compliance* trazendo uma breve explicação daquilo que cada um deles congrega e impõe que as empresas mantenham em seus programas de *compliance*.

---

101 TEIXEIRA, Tarcísio. KASEMIRSKI, André Pedroso. Capítulo 1 - *Compliance* (conformidade) de dados pessoais para microempresas: autorregulação regulada e requisitos para efetividade. *In:* **Empresas e implementação da LGPD – Lei Geral de Proteção de Dados Pessoais.** 2. ed. rev., ampl. e atual. São Paulo: Editora Juspodivm, 2022, p.25-28.

102 ANDRADE, Renato Campos. ***Compliance* como realizador do ESG:** construção dos pilares com foco no ambiental. São Paulo: Editora Dialética, 2024. ePub.

103 ANDRADE, Renato Campos. ***Compliance* como realizador do ESG:** construção dos pilares com foco no ambiental. São Paulo: Editora Dialética, 2024. ePub.

Tabela 3: Princípios de Compliance

Princípio 1	O conselho de administração é responsável por acompanhar o gerenciamento do risco de compliance da instituição devendo aprovar a política do mesmo, inclusive no que concerne ao documento que estabelece uma área de compliance permanente e efetiva. No mínimo, uma vez ao ano, o conselho de administração deve avaliar a efetividade do gerenciamento do risco de compliance.
Princípio 2	A alta administração é responsável pelo gerenciamento do risco de Compliance.
Princípio 3	A alta administração é responsável por estabelecer e divulgar a política de compliance da instituição, de forma a assegurar que ela está sendo observada e deve manter o conselho de administração informado a respeito do gerenciamento do risco de compliance.
Princípio 4	A alta administração é responsável por estabelecer uma área de compliance permanente e efetiva como parte da política da mesma.
Princípio 5	A área de compliance deve ser independente, pressupondo quatro elementos básicos: Status formal; Existência de um coordenador responsável pelos trabalhos de gerenciamento do risco de compliance; Ausência de conflitos de interesse; Acesso a informações e pessoas no exercício de suas atribuições.
Princípio 6	A área de compliance deve ter os recursos necessários ao desempenho de suas responsabilidades de forma eficaz.
Princípio 7	A área de compliance deve ajudar a alta administração no gerenciamento efetivo do risco de compliance, por meio de: Atualizações e recomendações; Manuais de compliance para determinadas leis e regulamentos; Identificação e avaliação do risco de compliance, inclusive para novos produtos e atividades; Responsabilidades estatutárias em relação ao combate à corrupção, à lavagem de dinheiro e ao financiamento ao terrorismo, bem como relações com reguladores; Implementação do programa de compliance.
Princípio 8	O escopo e a extensão das atividades da área de compliance devem estar sujeitos à revisão periódica por parte da auditoria interna.
Princípio 9	As instituições devem atender às exigências legais e regulamentares aplicáveis nas jurisdições em que operam, e a organização e a estrutura da área de compliance, bem como suas responsabilidades, devem estar de acordo com as regras de cada localidade.
Princípio 10	O compliance deve ser encarado como uma atividade central para o gerenciamento de risco em um banco. Nesse contexto, algumas atividades podem ser terceirizadas, mas devem ficar sob a responsabilidade do “chefe” do compliance.

Fonte: Compliance e Governança Corporativa[104].

Trazendo os princípios do *compliance,* para o contexto do tratamento de dados e da Lei Geral de Proteção de Dados Pessoais, as empresas que coletam e fazem uso de dados de seus clientes têm neles um guia para a gestão dessa área específica.

No que tange ao primeiro princípio, no contexto da LGPD, significa garantir que as entidades que efetuam tratamento de dados tenham estrutura para prevenir, detectar e responder a violações de dados pessoais acompanhando todas as ações relativas ao tratamento de dados dos clientes. Relativo ao segundo princípio, este aponta que a alta administração é responsável pelo desenvolvimento de fluxos de tratamento de dados com vistas a melhor controlar o que está sendo feito. Quanto ao terceiro princípio, a alta gestão responsável pelo tratamento de dados deve elaborar códigos de conduta e conceder treinamento a todos os funcionários no que toca o tema da proteção de dados.

Pelo quarto princípio, infere-se que para a proteção de dados é essencial que a empresa tenha responsáveis no dia a dia para monitorar os dados coletados, lidar com possíveis incidentes e manter contato com o encarregado de dados. Sobre o quinto princípio, pode-se concluir que a área na empresa que cuida do tratamento de dados deve ser independente, diminuindo qualquer possibilidade de ocorrência de conflitos de interesses entre os responsáveis.

Traçando-se um paralelo entre o sexto princípio e sua utilização em um ambiente em que é realizado tratamento de dados pessoais, pode-se entender que, no contexto da LGPD, é necessário contar com a utilização de ferramentas para o bom tratamento de dados, dentre elas, ferramentas de gestão do consentimento, controle de acesso, *data mapping*, dentre outras. Já em relação ao sétimo princípio, este denota que a alta gestão deve se manter atualizada sobre impactos relativos ao tratamento de dados, além de, receber a contribuição técnica no que tange a gestão de riscos de novos produtos e seus impactos na proteção de dados, dentre outros aspectos.

O oitavo princípio, infere que para o contexto da LGPD essa auditoria possa verificar se controles de segurança e procedimentos afetos ao tratamento de dados estão sendo cumpridos de modo eficaz. Já o nono princípio, é a gênese do compliance

---

[104] BLOK, Marcela. **Compliance e Governança Corporativa**. 4. ed. Rio de Janeiro: Freitas Bastos, 2023. Versão eletrônica.

no contexto da proteção de dados, na medida em que determina o cumprimento às legislações. Por fim, o décimo princípio, aponta que empresas terceirizadas poderão ser contratadas para o tratamento de dados, contudo é a empresa que contratou esses terceirizados que, via de regra, responderá por falhas, incidentes e violações.

Apresentados os princípios do *compliance*, cabe demonstrar as funções deste como ferramenta de governança corporativa, são elas:

> 1. Acompanhar a legislação aplicável às atividades da instituição, atentando para os aspectos inerentes às questões que produzam riscos regulatórios que possam afetar os negócios, sugerindo a devida adequação destes aspectos aos normativos internos; 2. Ter como princípio em situações de análise a aplicação de métodos e procedimentos que visem, de forma ordenada: proteger os recursos da entidade, obter informações oportunas e confiáveis, promover a eficiência operacional no processo e assegurar a observância das leis, normas e políticas vigentes; 3. Promover maior integração com as áreas de controles internos, risco operacional e auditoria interna; 4. Assegurar que todas as informações requeridas pelos reguladores sejam fornecidas pelas várias áreas da instituição, com tempestividade, fidedignidade, qualidade e integridade; 5. Ter os gestores como aliados/multiplicadores do entendimento de que a atividade de controle não se confunde com a da auditoria interna, bem como, de que a aplicabilidade do controle e a atualização dos fluxos dos processos são de responsabilidade do gestor e não do compliance; 6. Alinhar os instrumentos e procedimentos às melhores práticas de mercado, desenvolvendo um trabalho mais próximo e pró-ativo com os órgãos reguladores; 7. Desenvolver um trabalho cada vez mais próximo das áreas de negócio, aumentando o conhecimento relacionado à estratégia de negócios e produtos; 8. Atuar de forma independente e colaborativa, com apoio da alta administração e com uma estrutura reconhecida como geradora de valor para as instituições; 9. Mobilizar recursos adequados para o trabalho de disseminação dos valores e princípios de compliance (incluindo todos os níveis hierárquicos), objetivando uma atuação preventiva e consciente de cada colaborador em relação ao tema; 10. Identificar e utilizar sistemas que auxiliem efetivamente na "função de *compliance*"[105].

Ademais, o *compliance* contribui para a geração de valor organizacional de diversas maneiras, dentre as quais se destacam: a maior qualidade e celeridade nas interpretações regulatórias, bem como na elaboração de políticas e procedimentos internos; o aprimoramento da relação com órgãos reguladores, inclusive mediante avaliações positivas em processos de supervisão; o fortalecimento do relacionamento com acionistas e clientes; a adoção de decisões empresariais alinhadas às normas de conformidade; a maior rapidez na adequação de produtos às exigências regulatórias; a disseminação de elevados padrões éticos e de uma cultura de compliance em toda a organização; além do monitoramento contínuo das falhas,

[105] FEDERAÇÃO BRASILEIRA DE BANCOS – FEBRABAN. **Função de *Compliance*.** Coleção Instituto Febraban de Educação. p.27. Disponível em: https://www.febraban.org.br/7rof7swg6qmyvwjcfwf7i0asdf9jyv/sitefebraban/funcoescompliance.pdf. Acesso em: 15 abr. 2026.

correções e situações de não conformidade identificadas[106].

Assim, implementar um programa de *compliance* no contexto da LGPD, torna-se indispensável para a mitigação de riscos, além de ser ferramenta para preservar a imagem e a reputação das empresas, como será visto.

4.2 Programa de Integridade e *Compliance*

Um programa de integridade e *compliance* consiste na organização e no aprimoramento de mecanismos já existentes dentro da instituição, voltados, dentre outros objetivos, à prevenção e ao enfrentamento da corrupção. Trata-se de um conjunto de processos e políticas elaborado para assegurar que as condutas organizacionais estejam em conformidade com princípios éticos, normas internas, legislação vigente e regulamentações aplicáveis.

Considerando que cada organização possui estruturas próprias e métodos particulares de tomada de decisão, a definição e a implementação das funções relacionadas à integridade e ao *compliance* não seguem um padrão definido. Contudo, via de regra, um programa de integridade e *compliance* obedece a quatro pilares principais, quais sejam: comprometimento da alta direção, indicação dos responsáveis pelo programa, análise de riscos e integridade e, por fim, monitoramento contínuo.

No que tange o indispensável comprometimento da alta direção na criação de um programa de *compliance*, tem-se que este ato é o responsável por criar as bases do programa, haja vista que para os funcionários dos escalões mais baixos, o comportamento da alta direção passa a ser considerado o ideal, passando a ser reproduzido, seja por lealdade ou respeito dos liderados. Observa-se como exemplos de comprometimento da alta direção: a) viabilizar o programa de *compliance* perante o público externo e interno, demonstrando a importância para a organização e pedindo o comprometimento de todos; b) apoiar todas as fases de implementação; c) adotar postura ética e cobrar o mesmo de todos colaboradores; d) aprovar e supervisionar as políticas de integridade[107].

---

[106] FEDERAÇÃO BRASILEIRA DE BANCOS – FEBRABAN. **Função de *Compliance*.** Coleção Instituto Febraban de Educação. p.8. Disponível em: https://www.febraban.org.br/7rof7swg6qmyvwjcfwf7i0asdf9jyv/sitefebraban/funcoescompliance.pdf. Acesso em: 15 abr. 2026.

[107] BRASIL. Instituto Nacional de Tecnologia da Informação (ITI). **Programa de Integridade e Compliance**. Brasília, DF: ITI, 2018. Disponível em: https://www.gov.br/iti/pt-br/acesso-a-informacao/institucional/Programa_de_Integridade_e_Compliance___Assinado_1.pdf. Acesso em: 22

Ademais, a efetividade do programa de *compliance* também depende do comprometimento da alta direção, pois os colaboradores somente percebem a conformidade como verdadeira diretriz institucional quando ela é demonstrada “de cima para baixo”, e não apenas como uma política formal sem aplicação prática.

Nesse contexto, o *compliance* destaca a importância da postura ética dos dirigentes na construção da cultura organizacional, além disso estar diretamente ligado à alta administração garante a autonomia na fiscalização do cumprimento das normas internas e legais, inclusive em relação a gestores e chefias. Por fim, instrumentos como códigos de ética, canais de denúncia, auditorias e treinamentos somente possuem efetividade quando acompanhados de uma cultura ética sólida disseminada pela liderança da empresa[108].

Desta feita, a atuação ética da alta direção contribui para a formação de uma cultura de integridade corporativa, influenciando o comportamento dos demais colaboradores por meio do exemplo. Assim, sem o efetivo apoio e comprometimento da alta administração, os programas de integridade tendem a perder eficácia, comprometendo o engajamento dos demais integrantes da organização[109].

A respeito da indicação dos responsáveis pelo programa, tem-se que esta pessoa ficará responsável por acompanhar e monitorar as ações e medidas de integridade a serem implementadas, tendo autonomia e agindo com imparcialidade para o cumprimento de sua função. Tangente à análise de riscos, é através dela que se conhece as áreas da empresa mais sensíveis, cujos controles de integridade devam ser implementados com mais ou menos rigor. Por fim, o monitoramento contínuo fará com que o programa de integridade e *compliance* possa ser atualizado, ajustando-o conforme as novas necessidades, riscos e processos da empresa[110].

Os responsáveis indicados para a implementação do programa de integridade e *compliance* terão suas atividades pautadas nas seguintes etapas[111]: a) análise do ambiente interno, sendo essa a base do programa que apresenta as características

---

abr. 2026.

[108] ANDRADE, Renato Campos. **Compliance como realizador do ESG:** construção dos pilares com foco no ambiental [livro eletrônico]. São Paulo: Editora Dialética, 2024. p.11.

[109] ANDRADE, Renato Campos. **Compliance como realizador do ESG:** construção dos pilares com foco no ambiental [livro eletrônico]. São Paulo: Editora Dialética, 2024. p.11.

[110] BRASIL. Instituto Nacional de Tecnologia da Informação (ITI). **Programa de Integridade e Compliance**. Brasília, DF: ITI, 2018. Disponível em: https://www.gov.br/iti/pt-br/acesso-a-informacao/institucional/Programa_de_Integridade_e_Compliance___Assinado_1.pdf. Acesso em: 22 abr. 2026.

[111] FREITAS, Daniel Paulo Paiva. **Proteção e governança de dados.** Curitiba: Contentus, 2020. p.66-67.

da empresa naquele momento, como valores éticos, recursos humanos, nível de integridade, dentre outras; b) análise de riscos: mapeia os riscos inerentes a atividade empresarial à luz das obrigações pertinentes à atividade; c) elaboração de documentos: nessa etapa o código de conduta, que concentra a missão e os valores éticos a serem seguidos, e o código de procedimentos, que aponta o modo como o código de conduta será cumprido, são elaborados; d) canais de denúncia e sistemas de premiação, que são meios de comunicação internos para que funcionários ou terceiros possam denunciar possíveis irregularidades; e) procedimentos sancionatórios: embasarão a aplicação de sanções em caso de irregularidades descobertas; f) comunicação de diretrizes: para que haja a difusão pela empresa (e fora dela, em relação a terceiros interessados) dos códigos que foram elaborados; g) avaliação, monitoramento e auditoria que assegurarão a efetividade do programa.

A figura a seguir apresenta um plano de integridade e *compliance*, que contempla em um documento único, as medidas que devem ser implementadas, com vistas a prevenir, detectar e tratar eventuais quebras de integridade que possam ocorrer:

Figura 3: Plano de Integridade e *Compliance.*

Fonte: Programa de Integridade e *Compliance*[112].

[112] BRASIL. Instituto Nacional de Tecnologia da Informação (ITI). **Programa de Integridade e Compliance**. Brasília, DF: ITI, 2018. Disponível em: https://www.gov.br/iti/pt-br/acesso-a-informacao/institucional/Programa_de_Integridade_e_Compliance___Assinado_1.pdf. Acesso em: 22

Ademais, um programa de *compliance*, apesar de exigir investimentos, como tempo e dinheiro, tem como retorno os seguintes efeitos organizacionais[113]:

> a) auxiliam na análise mais acurada do comportamento dos funcionários;
> b) ajudam a prevenir atos ilícitos e antiéticos;
> c) estimulam a rápida reação em situações críticas de forma eficaz e eficiente;
> d) melhoram a qualidade, eficiência e consistência dos serviços;
> e) transmitem segurança para os funcionários, para que possam relatar problemas e esperar investigações e ações corretivas;
> f) ajudam na melhora da comunicação interna;
> g) criam processos que permitem a imediata e profunda investigação de acusações;
> h) apresentam compromisso da empresa com conduta ética e de responsabilidade corporativa;
> i) minimizam perdas financeiras, sejam relativas às indenizações, impostos e eventuais multas a serem aplicadas;
> j) ajudam a consolidar ou melhorar a reputação da empresa em relação à integridade e qualidade, aumentando ainda sua competividade no mercado.

Isto posto, fica demonstrado que implementar um programa de integridade e *compliance* é um instrumento base que, como consequência, pautará a ética, a transparência, além de, manter a conformidade organizacional com as leis vigentes, sendo, para além de um conjunto de regras, um mecanismo capaz de prevenir irregularidades, identificar riscos e promover maior segurança nas relações institucionais e negociais.

Neste intento, o comprometimento da alta direção, bem como a definição dos responsáveis, a adequação da gestão e o monitoramento contínuo são cruciais para a efetividade do programa e sua constante adaptação às transformações, de sorte que, o plano de integridade e *compliance* torna-se uma importante ferramenta de governança.

Ato contínuo, o tema do *compliance* de dados, que é uma vertente do *compliance* empresarial, será apresentado.

4.3 COMPLIANCE DE DADOS

A segurança da informação tem sido encarada nos últimos tempos como um dos principais pilares do *compliance* de dados, principalmente no que toca a proteção de dados pessoais. Essa questão tem se tornado cada dia mais relevante, tanto que

abr. 2026.

[113] FREITAS, Daniel Paulo Paiva. **Proteção e governança de dados.** Curitiba: Contentus, 2020. p.65.

o Supremo Tribunal Federal[114] reconheceu a proteção de dados como direito fundamental autônomo, decisão essa que foi depois acolhida na Emenda Constitucional nº115/2022, que inclui no artigo quinto da Constituição Federal[115] a proteção de dados pessoais, tornando-a uma cláusula pétrea. Esses fatos reforçam o papel crucial da governança, transparência e *compliance* de dados no dia a dia das organizações que tratam informações pessoais.

Por sua vez, o aumento de vazamentos de dados decorrentes de falhas humanas e ataques cibernéticos sofisticados mostra que ainda há muito o que ser feito nesta seara pelas organizações públicas e privadas. Nesse intento, a LGPD busca estabelecer diretrizes essenciais ao fortalecimento da segurança dos dados pessoais e ao enfrentamento de desafios impostos pela crescente complexidade do ambiente digital[116].

Conforme já abordado anteriormente, estar em *compliance* significa estar em conformidade com leis, regulamentos, regimentos que devem ser cumpridos pelas empresas, além de, manter atitudes idôneas e responsáveis em todos os níveis da gestão. Nesse viés, uma empresa que mantém regras desse instituto definidas, mantendo suas atividades de modo ao cumprimento estrito das leis, agrega para si uma série de benefícios, seja melhorando a percepção dos envolvidos na organização ou reduzindo a possibilidade de sanções promovidas pelo Estado.

Assim, respectivo ao tratamento de dados, surge o *compliance* de dados que nada mais é que estar em conformidade com as legislações concernentes à proteção de dados, desenvolver estratégias, adotar metodologias para esse cumprimento e agir com responsabilidade em todo o processo de tratamento de dados.

> Uma das grandes novidades que as legislações recentes sobre proteção de dados trouxeram foi a adoção da sistemática de *compliance* como critério interno de conexão entre os vários institutos da legislação. O sistema de gestão de *compliance* de dados aparece nessa legislação como expressão do principio da *accountability* e como meio de proteção dos direitos subjetivos/fundamentais de dados. No caso do Brasil, naturalmente, estamos falando da Lei Geral de Proteção de Dados (LGPD), a Lei 13.709, de 14 de agosto de 2018[117].

---

[114] O STF firmou esse entendimento ao julgar medidas cautelares (ADIs 6387, 6388, 6389, 6393, 6390) que suspenderam uma MP que obrigava o repasse de dados de telefonia ao IBGE.

[115] Art. 1º O caput do art. 5º da Constituição Federal passa a vigorar acrescido do seguinte inciso LXXIX: "Art. 5º .... LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".

[116] FRAZÃO, Ana; PINTO, Mariana. Compliance de Dados e Incidentes de Segurança. *In:* PINHEIRO, Caroline da Rosa. **Compliance entre a teoria e a prática.** Indaiatuba, SP: Editora Foco, 2022. p.10.

[117] SAAVEDRA, Giovani Agostini. *Compliance* de Dados. *In:* BIONI, Bruno. **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021. Edição Eletrônica. p.1103.

Desta feita, o *compliance* de dados tem como interesse proteger a empresa, os administradores, os colaboradores entre outros envolvidos na organização no que toca o tratamento de dados pessoais, através da orientação aos colaboradores, da melhoria da conduta do negócio no que diz respeito ao tratamento de dados que executa, do monitoramento daquilo que se pretende controlar, proteger e evitar em matéria de dados pessoais, além do aprimoramento contínuo com foco na conformidade com as legislações que tratam do tema da proteção de dados, incluindo a prevenção de incidentes, detecção e correção nas situações em que o *compliance* de dados tenha falhado[118].

No campo da prevenção de incidentes, esta envolve uma análise do ambiente empresarial capaz de avaliar as medidas tecnológicas e organizacionais que, ajustadas ao perfil e ao porte da empresa em questão e também ao grau de risco dos tratamentos de dados que esta efetua, possam ser consideradas suficientes à prevenção efetiva de incidentes[119].

> É sabido que a construção de um programa de conformidade tende a ser tarefa árdua, marcada por uma série de custos e um processo de implementação complexo. Isso porque a instituição de um robusto programa de *compliance* de dados exige a contratação de especialistas, a elaboração de um código de ética e de conduta, a avaliação permanente dos riscos, o investimento contínuo no treinamento de empregados, a contratação ou o treinamento de um encarregado de proteção de dados, o investimento em mecanismos de controle interno e de tecnologia da informação, dentre outros investimentos relacionados ao cumprimento da LGPD[120].

Nesse viés, por mais que a LGPD seja um elemento de adequação capitaneado pela tutela da ANPD, adequar-se é parte de uma oportunidade maior que envolve a cooperação entre agentes e a criação de instituições fortes que sejam compatíveis com a tutela de dados pessoais, traduzida para um cenário ideal como um diferencial competitivo entre agentes que atuam no mesmo mercado[121].

---

[118] VIEIRA, Lucas Pacheco. ***Compliance* de Dados Pessoais**. Revista de Direito e as Novas Tecnologias. v.22, 2024, p.3. Disponível em: https://www.researchgate.net/profile/Lucas-Vieira-12/publication/382217030_COMPLIANCE_DE_DADOS_PESSOAIS/links/6691f503af9e615a15e309c0/COMPLIANCE-DE-DADOS-PESSOAIS.pdf. Acesso em: 15 out. 2025.

[119] FRAZÃO, Ana; PINTO, Mariana. Compliance de Dados e Incidentes de Segurança. *In:* PINHEIRO, Caroline da Rosa. **Compliance entre a teoria e a prática.** Indaiatuba, SP: Editora Foco, 2022. p.10.

[120] FRAZÃO, Ana; CARVALHO, Angelo Prata de. **A LGPD e a necessidade de adequação emergencial das estruturas empresariais. Passos preliminares e fundamentais para a conformidade.** Disponível em: https://www.professoraanafrazao.com.br/files/publicacoes/2021-03-04-A_LGPD_e_a_necessidade_de_adequacao_emergencial_das_estruturas_empresariais_Passos_preliminares_e_fundamentais_para_a_conformidade.pdf. Acesso em 24 abr. 2026.

[121] FRAZÃO, Ana; PINTO, Mariana. Compliance de Dados e Incidentes de Segurança. *In:* PINHEIRO,

Ademais, a adequação à LGPD perpassa minimamente por quatro etapas essenciais de *compliance* de dados, são elas: a avaliação preliminar dos fluxos de tratamentos de dados e dos riscos associados; a adequação da estrutura organizacional que comportará a estratégia de adequação, ponto em que o encarregado de dados será indicado e as áreas da empresa serão capacitadas; a implementação de estratégias de comunicação interna e externa; a adaptação dos ambientes digital e físico no que tange à nova preocupação com a segurança dos dados[122].

Assim, para o contexto do tratamento e proteção de dados, algumas ferramentas são essenciais para a completude de um sistema de *compliance*, dentre elas pode-se citar: a) Análise de Riscos[123]; b) *Data Mapping*[124]; c) *Privacy Impact Assessment (PIA)*[125]; e d) *Data Protection Impact Assessments (DPIA)*[126]. No contexto do tratamento de dados, sem prejuízo das outras metodologias, o DPIA é uma das mais completas para o sistema de *compliance*. A figura a seguir demonstra com clareza as atividades sequenciais do DPIA iniciando na descrição do escopo e terminando no monitoramento e revisão[127].

Caroline da Rosa. **Compliance entre a teoria e a prática.** Indaiatuba, SP: Editora Foco, 2022. p.10.

[122] FRAZÃO, Ana; CARVALHO, Agelo Prata de. **A LGPD e a necessidade de adequação emergencial das estruturas empresariais. Passos preliminares e fundamentais para a conformidade.** Disponível em: https://www.professoraanafrazao.com.br/files/publicacoes/2021-03-04-A_LGPD_e_a_necessidade_de_adequacao_emergencial_das_estruturas_empresariais_Passos_preliminares_e_fundamentais_para_a_conformidade.pdf. Acesso em 24 abr. 2026.

[123] É através da análise de riscos que se conhece a empresa e as leis que regulam o negócio, bem como, no contexto interno, são levantados dados para identificar riscos e de desenvolver a matriz de riscos, para saber quais elementos demandam maior atenção, com isso pronto, o monitoramento se torna uma constante.

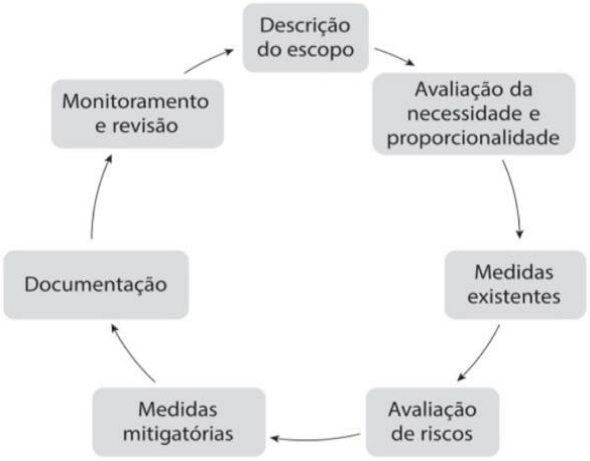
[124] Sua principal função é verificar quais dados são transportados entre vários sistemas, de modo a saber como esse são compartilhados, organizados e armazenados.

[125] É uma análise de riscos de privacidade e proteção de dados relativa às informações pessoais que serão processadas em um projeto, produto ou serviço novo.

[126] Descreve o processo designado para identificar riscos, que surgem do processamento de dados pessoais e para minimizar esses riscos o máximo e o mais rápido possível.

[127] SAAVEDRA, Giovani Agostini. Compliance de Dados. *In:* BIONI, Bruno. **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021. Edição Eletrônica. p.1112-1113

Figura 4: Ciclo de atividades do *Data Protection Impact Assessments* (DPIA).



Fonte: Tratado de proteção de dados pessoais[128].

O esquema acima denota que o *compliance* de dados engloba desde o entendimento dos dados que serão tratados, com a descrição do escopo do tratamento até o monitoramento constante, com vistas a garantir a integridade e segurança das informações tratadas.

Vale ressaltar que o *compliance* de dados congrega elementos essenciais para a sua execução, como o *Privacy by Design* (que garante a privacidade e a proteção de dados pessoais desde o início de um projeto de produto até a sua execução[129]), a implementação do código de ética e de conduta, além do encarregado de dados, já mencionado anteriormente nessa dissertação.

Dada a importância do *Privacy by Design*, este elemento possui princípios que, em última análise, contribuem sobremaneira para o *compliance* de dados desde a concepção de um projeto, são eles[130]:

> a) proatividade, não reatividade: previna e antecipe problemas de privacidade antes que eles ocorram, em vez de corrigi-los após o incidente;
> b) privacidade como configuração padrão: as configurações de privacidade devem ser as mais fortes por padrão, sem exigir que o usuário faça ações adicionais para proteger seus dados;

[128] SAAVEDRA, Giovani Agostini. Compliance de Dados. In: BIONI, Bruno. **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021. Edição Eletrônica. p.1113
[129] BRASIL. **Guia sobre Privacidade desde a Concepção e por Padrão.** Programa de Privacidade e Segurança da Informação (PPSI). Ministério da Gestão e da Inovação em Serviços Públicos: 2024. p.8.
[130] CAVOUKIAN, ANN. **Privacy and Security by Design.** Youtube. Data de Publicação: 29 de abriu de 2025. Disponível em: https://www.youtube.com/watch?v=I8FCCogzX28 Acesso em: 11 set. 2025.

> c) privacidade incorporada ao design: a privacidade deve ser parte integrante do projeto, não um recurso adicionado ou opcional;
> d) funcionalidade completa: congrega o equilíbrio entre privacidade e funcionalidade, garantindo que ambos os objetivos sejam alcançados sem sacrificar um pelo outro;
> e) segurança de ponta a ponta: a proteção dos dados deve ocorrer ao longo de todo o ciclo de vida, desde a coleta até o descarte;
> f) visibilidade e transparência: mantenha as políticas e os processos de tratamento de dados abertos e transparentes para os usuários, que devem saber como seus dados são usados;
> g) respeito pela privacidade do usuário: mantenha os interesses do usuário em primeiro lugar, oferecendo controles robustos para proteger seus dados e usando uma linguagem clara e amigável.

Conclusivamente, pode-se anotar que o instituto do *compliance* de dados é uma extensão do *compliance* empresarial, o qual contribui com as empresas que realizam tratamento de dados, de modo a propor que estas empresas possuam, em sua estrutura e dia a dia, ferramentas para realizar suas atividades de tratamento como forma de garantir que os dados pessoais de seus clientes que serão tratados não sejam objeto de algum incidente que possa causar prejuízos aos titulares e, consequentemente, às próprias empresas.

Isto posto, passemos a apresentar de forma estrita como o *compliance* de dados é abordado no bojo da Lei Geral de Proteção de Dados Pessoais - Lei 13.709/18.

4.4 *Compliance* e a Lei Geral de Proteção de Dados Pessoais

É notório que estamos em um período de elevado desenvolvimento tecnológico o qual, cada vez mais, viabiliza o acesso de um maior número de pessoas à internet, que por sua vez, passaram a realizar atividades da vida cotidiana (anteriormente feitas no ambiente físico) de modo digital, como por exemplo aquelas relacionadas a compras, comunicação, interação social, serviços bancários, dentre outras atividades, fazendo com que, a disponibilização de informações pessoais, de modo consciente ou não, ganhe proporções absurdamente grandes. Desta feita, é que nasce a preocupação regulatória do Estado com vistas, principalmente, à proteção da privacidade dos titulares desses dados.

De outra banda, estão as empresas querendo vender cada vez mais, e assim,

com o uso do tratamento de dados, conseguem traçar perfis de compradores e oferecer seus produtos através de publicidades bastante assertivas, inclusive pelo uso de itens de tecnologias como os *cookies* dos navegadores de internet. Nesse contexto, é necessário que essas empresas estejam em *compliance* com os ditames da LGPD, de modo a não sofrerem sanções, definidas no artigo 52[131] da Lei 13.709/18.

Além do mais, não só as empresas podem se comprometer com o mau tratamento de dados que porventura efetuem, mas também, os titulares podem suportar danos diversos. Nesta seara, estar em *compliance* torna-se, ao mesmo tempo, uma proteção e uma oportunidade para as companhias.

> É mister, essencial e necessário que se procure a conformidade através do trabalho deste instrumento no contexto do espaço cibernético ou digital. A cultura de *compliance* deve ser plenamente almejada, principalmente neste momento de transformação digital em que a sociedade se depara com novos instrumentos tecnológicos que, por imprudência, imperícia e/ou negligência, conseguem muitas vezes violar normativos de proteção de dados. Como consequência, são gerados danos severos em garantias, liberdades e direitos dos indivíduos, sendo que o principal instrumento para contrariar este cenário é o trabalho baseado numa gestão preventiva, em direitos fundamentais, bem como em mecanismos que promovem a cibersegurança[132].

A despeito do instituto do *compliance* ser, em sua origem, uma ferramenta de combate à corrupção, ele representa conformidade e coerência com as obrigações impostas por normas jurídicas, ao passo que, quando se trata de uma sociedade digital como se vê nos dias de hoje, ele deve ser aplicado de modo que a devida atenção aos normativos de proteção de dados seja dada pelas organizações, com o intuito de que seja alcançada, tecnicamente, a maximização da cibersegurança dos

---

[131] Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II; IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração; VII - (VETADO); VIII - (VETADO); IX - (VETADO). X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

[132] LÓSSIO. Claudio Joel Brito. **Proteção de dados e *compliance* digital.** 2.ed. São Paulo: Almedina, 2023.

dados tratados por estas empresas[133].

Sendo um dever das empresas se adequarem à LGPD, é um ônus que estas elaborem um programa de *compliance*, capaz de implementar políticas técnicas e administrativas que cumpram com a tutela dos dados pessoais dos seus clientes, minando a possibilidade de que riscos da própria atividade empresarial aconteçam, ao mesmo tempo que, se beneficiem da nova legislação, caso sofram sanções[134].

No que converge o tema do *compliance*, podemos encontrar na Lei Geral de Proteção de Dados Pessoais[135] artigos os quais determinam que o tratamento de dados deva ser realizado com técnica e segurança, sendo essencial para que se possa garantir o resultado esperado e, de outro lado, mantendo em segurança os dados dos titulares.

As medidas apontadas no artigo 46 abrangem recursos tecnológicos, como por exemplo, criptografia, autenticação de acesso, *backups* e ferramentas aptas a prevenir invasões, e recursos administrativos e jurídicos, incluindo políticas corporativas, contratos de confidencialidade e capacitação de colaboradores. Para isso, a LGPD demonstra que a proteção de dados exige atuação multidisciplinar, com base em governança, gestão de riscos e implementação de controles internos capazes de assegurar a confidencialidade, integridade e disponibilidade das informações. Dessa forma, a privacidade deixa de ser elemento complementar e passa a integrar a estrutura de *compliance* empresarial[136].

Relativo ao artigo 47, este apresenta que, de acordo com o princípio da segurança apresentado na LGPD, tanto o agente de tratamento como outra pessoa

---

[133] LÓSSIO. Claudio Joel Brito. **Proteção de dados e *compliance* digital.** 2.ed. São Paulo: Almedina, 2023.

[134] TEIXEIRA, Tarcísio. KASEMIRSKI, André Pedroso. Capítulo 1 - *Compliance* (conformidade) de dados pessoais para microempresas: autorregulação regulada e requisitos para efetividade. *In:* **Empresas e implementação da LGPD – Lei Geral de Proteção de Dados Pessoais.** 2. ed. rev., ampl. e atual. São Paulo: Editora Juspodivm, 2022, p.34.

[135] Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término. Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

[136] JIMENE, Camila do Valle. Capítulo VII – Da segurança e das boas práticas. *In*: MALDONADO, Viviane Nobre; BLUM, Renato Opice. **LGPD:** Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2019. p.265-271. E-book.

que, de algum modo, possa intervir em alguma das fases do tratamento de dados, ficam obrigados a garantir a segurança em relação a eles, mesmo quando o tratamento tenha finalizado. Isto posto, empresas preocupadas com sua reputação perante seus clientes, passaram a adotar tecnologias de segurança para os dados que são tratados, considerando, inclusive, o período após o término do tratamento, pois, em caso de incidentes, será necessário comprovar que foram utilizadas medidas técnicas que tornem os dados vazados inúteis para terceiros[137].

No que tange o artigo 48, este aponta a obrigação de comunicação à ANPD em casos de incidentes que possam gerar risco ou danos relevantes aos titulares, de modo que, essa comunicação deve conter informações detalhadas dos dados afetados, bem como, dos titulares envolvidos, além de apresentar as medidas de segurança adotadas para mitigar ao máximo os efeitos do incidente. Nesse contexto, a LGPD aponta a necessidade de integração entre direito e tecnologia nos mecanismos técnicos necessários à preservação da segurança dos dados que estão sendo tratados[138].

Sobre o artigo 49, tem-se que os agentes responsáveis pelo tratamento de dados deverão ter um grande cuidado na escolha dos sistemas que serão utilizados para a coleta, tratamento ou armazenamento de dados dos seus clientes, de modo que, os requisitos da lei no que toca a segurança e as boas práticas sejam atendidos[139].

Assim, no contexto da proteção de dados destacam-se três figuras profissionais responsáveis pelo tratamento, são elas: o controlador de dados, o operador de dados e a figura essencial do encarregado de dados, os quais são definidos no artigo quinto, incisos VI, VII e VIII da LGPD da seguinte maneira:

Tabela 4 – Definição de operador, controlador e encarregado de dados na LGPD.

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

[137] TEIXEIRA, Tarcisio. GUERREIRO, Ruth Maria. **Lei Geral de Proteção de Dados Pessoais:** comentada artigo por artigo. 4.ed. São Paulo: SaraivaJur, 2022. p.168-170.
[138] JIMENE, Camila do Valle. Capítulo VII – Da segurança e das boas práticas. *In*: MALDONADO, Viviane Nobre; BLUM, Renato Opice. **LGPD:** Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2019. p.277-282. E-book.
[139]TEIXEIRA, Tarcisio. GUERREIRO, Ruth Maria. **Lei Geral de Proteção de Dados Pessoais:** comentada artigo por artigo. 4.ed. São Paulo: SaraivaJur, 2022. p.172-174.

Controlador	Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais
Encarregado	Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Agência Nacional de Proteção de Dados – ANPD

Fonte: Lei Geral de Proteção de Dados Pessoais – Lei 13.709/18.

Em um contexto exemplificativo, o controlador dos dados são as empresas que vão se beneficiar de algum modo do tratamento de dados efetuado. O operador é quem faz o tratamento de dados para o controlador, trazendo informações relevantes dos titulares que, se fossem analisadas de forma isolada, não teriam valor efetivo para o controlador. E, por fim, o encarregado é quem faz a interface entre o controlador, os titulares dos dados (que são os clientes das empresas) e a Agência Nacional de Proteção de Dados - ANPD, sempre que necessário, sendo o DPO (como também é chamado o encarregado de dados) o elo principal da atividade de tratamento de dados no contexto brasileiro.

Assim, denota-se que para que o *compliance* seja alcançado no campo do tratamento de dados pessoais, é essencial que as empresas tenham esses responsáveis indicados, pois cada um exerce uma função no tratamento. Desta feita, é muito importante que estes personagens do tratamento de dados estejam totalmente em *compliance* com vistas a mitigar o máximo possível a possibilidade de que aconteçam vazamentos que possam causar prejuízos aos titulares de dados e consequentemente, às empresas.

O próximo capítulo aborda os temas apresentados nesta dissertação, que determinam a geração de valor real alcançada por aquelas organizações que se adequem aos ditames da Lei Geral de Proteção de Dados Pessoais – Lei 13.709/18, senão vejamos.

5 A ADEQUAÇÃO À LGPD COMO ESTRATÉGIA DE GOVERNANÇA E *COMPLIANCE* NA GERAÇÃO DE VANTAGEM COMPETITIVA EMPRESARIAL

A análise integrada dos temas abordados até aqui nos permite entender que as vantagens que decorrem da adequação à Lei Geral de Proteção de Dados Pessoais não se limitam à mera observância formal de comandos normativos. Trata-se, antes, de um processo inserido em um contexto maior de evolução institucional, amadurecimento organizacional e consolidação de novos institutos jurídicos empresariais aos quais as organizações estão submetidas.

Ao se demonstrar o contexto histórico e conceitual da proteção de dados, partindo do estudo relativo à privacidade pura e simplesmente, até que se chegue ao contexto da LGPD com seus fundamentos, princípios e, entendendo como o instituto da responsabilidade civil se aplica a ela, pode-se notar que, principalmente, em razão da evolução tecnológica, o tema da proteção de dados passou a fazer parte dos direitos fundamentais, mas também passou a ter grande enfoque mercadológico (que é o recorte dessa dissertação), no ponto em que passou a ser objeto de atenção pelas empresas que tratam dados dos seus clientes.

É amplamente reconhecido que a lei de proteção de dados brasileira sofreu influência da *General Data Protection Regulation* – GDPR, vigente no âmbito da União Europeia onde, naquele ordenamento, no artigo 24[140], é demonstrada a responsabilidade proativa do controlador de dados, mas, além disso, denota a importância que o tratamento de dados possui frente aos riscos que oferece, assim, essa proatividade também é esperada das empresas que tratam dados em solo nacional[141].

No que toca o tema da governança corporativa, a implementação de boas práticas alicerçadas nos princípios da equidade, transparência, integridade, responsabilização e sustentabilidade, são de suma importância para que conflitos de

---

[140] Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos de probabilidade e gravidade variáveis para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento deve implementar medidas técnicas e organizativas adequadas para garantir e poder demonstrar que o tratamento é realizado em conformidade com o presente regulamento.

[141] UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas físicas 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 – GDPR).** Jornal Oficial da União Europeia, L119, 4 maio 2016.

interesses sejam minimizados ou, preferencialmente, eliminados, de modo que assim as organizações sejam visualizadas de modo positivo por todos os seus *stakeholders*, fato este que contribui com o incremento do valor das empresas no que tange aos aspectos econômicos e reputacionais.

Relacionado ao *compliance* e ao *compliance* de dados, tem-se que a conformidade às leis, além de mitigar possíveis problemas jurídicos de ordem regulatória, financeira, reputacional e operacional, faz com que cresçam, no seio organizacional, comportamentos atrelados à integridade, prevenção de riscos, e eficiência operacional. Cabe anotar que esses comportamentos se unem aos elementos da governança corporativa e da Lei 13.709/18.

Desta feita, podem-se inferir algumas vantagens diretas da adequação à LGPD, com base principalmente, nos elementos do *compliance* e do *compliance* de dados, as quais serão apresentadas com maiores detalhes na sequência. São elas[142]:

> a) identificação, prevenção, mitigação e correção de riscos;
> b) oportunidade de negócios e vantagem competitiva;
> c) valorização da marca, da reputação e da imagem empresarial;
> d) atração de investimentos;
> e) eficiência operacional;
> f) segurança jurídica e limitação de responsabilidade, que serão analisadas, individualmente, a seguir.

5.1 Identificação, Prevenção, Mitigação e Correção de Riscos

A identificação e mitigação de riscos relacionados ao tratamento de dados pessoais depende diretamente da adoção de mecanismos internos de governança corporativa e *compliance,* apresentados anteriormente, exercendo papel fundamental na construção de estruturas organizacionais aptas a prevenir irregularidades, monitorar procedimentos internos e estabelecer padrões seguros de tratamento de dados.

Nesta esteira, os programas de *compliance* e *compliance* de dados assumem função estratégica, pois englobam o desenvolvimento de controles internos, políticas institucionais, protocolos e mecanismos de fiscalização ao passo que reduzem a probabilidade de vazamentos de dados e responsabilizações decorrentes do descumprimento da legislação.

Ademais, a antecipação aos possíveis problemas relacionados ao tratamento

---

[142] BLOK, Marcela. ***Compliance* e Governança Corporativa.** 4. ed. Rio de Janeiro: Freitas Bastos, 2023. Versão eletrônica.

de dados pessoais permite que soluções sejam apresentadas antes da ocorrência de incidentes, reduzindo a probabilidade de responsabilização por danos eventualmente causados aos titulares[143].

Além disso, como já visto, a adoção desses mecanismos de governança em privacidade, tem o viés de fortalecer a credibilidade institucional perante clientes, parceiros e investidores, ao demonstrar que a organização atua de maneira diligente na proteção dos dados que estão em sua responsabilidade, o que, num cenário econômico cada vez mais digitalizado, passa a representar importante ativo competitivo.

Considerando que a Lei 13.709/18 traz em seu bojo orientações relativas à governança e ao *compliance* (artigos 46 a 49), do ponto de vista das organizações, estar adequado a estas recomendações, faz com que sejam mitigadas as possibilidades de vazamento de dados (ou reduzidos os impactos financeiros advindos desses vazamentos), uma vez que os responsáveis pelo tratamento de dados são orientados pela lei a estabelecer regras de boas práticas no âmbito dos tratamentos de dados que serão realizados, nos termos do artigo 50, §1º da referida lei[144].

Deste fato, depreende-se que a implementação de políticas internas de proteção de dados, controles de acesso, medidas de segurança, dentre outras, contribuem, para além da conformidade legal, com o fortalecimento da imagem corporativa.

Nesse prisma, a implementação ao que a LGPD propõe, no que concerne à governança em privacidade, não apenas reduz a probabilidade de que incidentes ocorram, mas também, demonstra proatividade por parte das empresas, o que é bem visto, também, pela ANPD. Em complemento, empresas que realizam treinamento, mapeiam riscos e fazem relatórios de impacto, fazem com que a preocupação com o tratamento de dados seja inserida na cultura da empresa.

5.2 Oportunidade de Negócios e Vantagem Competitiva

Antes de mais nada, para seguir no entendimento sobre como a adequação à

---

[143] BLOK, Marcela. ***Compliance* e Governança Corporativa.** 4. ed. Rio de Janeiro: Freitas Bastos, 2023. Versão eletrônica.

[144] BRASIL. **Lei nº 13.709. Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília, DF, 14 de agosto de 2018.

LGPD resulta em vantagem competitiva, é importante entender o que esta significa. Assim, vantagem competitiva é adquirida por uma organização que, em relação aos seus concorrentes, obtém melhor desempenho resultando em menor custo de produção, ou ainda, na possibilidade de entregar para seus clientes produtos ou serviços com maiores níveis de percepção de valor[145].

Assim, a implementação de práticas de governança corporativa e *compliance* relacionadas à proteção de dados pessoais não produz apenas efeitos voltados à conformidade normativa, mas também repercute diretamente na posição competitiva das organizações no mercado. Isso porque, em um ambiente empresarial cada vez mais orientado pela confiança, pela transparência e pela segurança da informação, empresas que demonstram comprometimento com a proteção de dados tendem a transmitir maior credibilidade a consumidores, investidores e parceiros comerciais.

Em adendo, no contexto da proteção de dados pessoais, coletar grandes quantidades de dados, e realizar o tratamento correto de acordo com as legislações vigentes, importa que as organizações detentoras desses dados obtenham vantagens competitivas perante seus concorrentes, como ocorre com o Google e Facebook, por exemplo, no que se refere à publicidade digital que disponibilizam, e que é efetiva para os anunciantes, dada a quantidade de dados coletados que possuem, senão vejamos[146]:

> O controle do Facebook e do Google sobre a publicidade digital é possível graças à sua capacidade de coletar e agregar enormes quantidades de dados de usuários finais, mais do que qualquer outra empresa. Quanto mais dados o Facebook e o Google conseguem coletar, melhores são seus algoritmos preditivos, mais poderosa é sua capacidade de influenciar os usuários finais e maior é sua capacidade de monopolizar o mercado de publicidade digital. É por isso que é lucrativo para o Facebook e o Google comprar tantos tipos diferentes de empresas e aplicativos, cada um dos quais coleta dados de maneiras diferentes. Mais dados significam mais poder[147].

---

[145]PORTER, Michael. **Vantagem competitiva: criando e sustentando um desempenho superior.** 27. ed. Rio de Janeiro: Elsevier, 1989.

[146] PORTER, Michael. **Vantagem competitiva: criando e sustentando um desempenho superior.** 27. ed. Rio de Janeiro: Elsevier, 1989.

[147] Texto original: Facebook's and Google's control over digital advertising is made possible by their ability to collect and aggregate enormous amounts of end user data, more than any other company. The more data Facebook and Google are able to collect, the better their predictive algorithms, the more powerful their ability to nudge and influence end users, and the better their ability to corner the market on digital advertising. That is why it is profitable for Facebook and Google to buy up so many different kinds of companies and applications, each of which collects data in different ways. More data means more power.

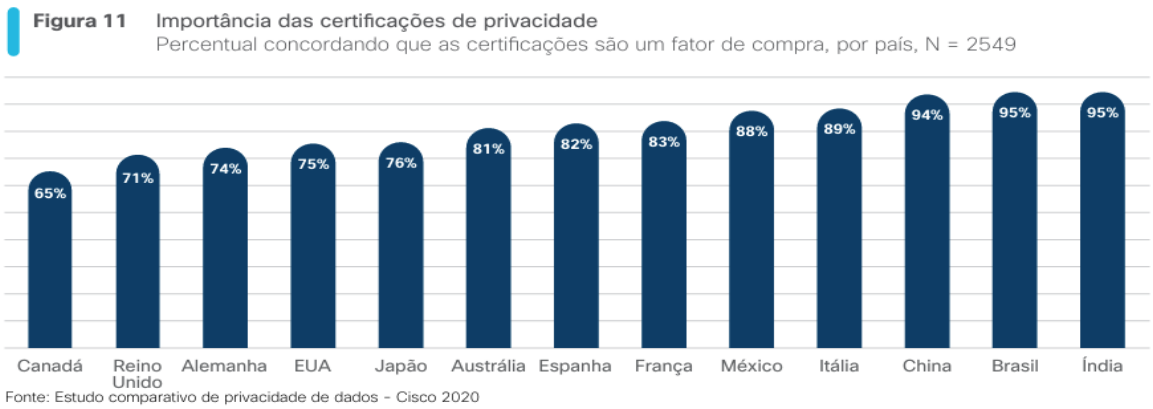
Isto posto, a despeito do exemplo citado ser de grandes empresas de tecnologia, a vantagem competitiva alcançada através da coleta de dados é a mesma para empresas menores, haja vista que, tendo essas informações em mãos, terão a possibilidade de entregar seus produtos ou serviços de modo cada vez mais personalizado aos seus clientes, obtendo maiores lucros.

De outro lado, é natural que, empresas que tenham programas de *compliance* robustos, e estejam estritamente cumprindo com os deveres legais, façam negócios, preferencialmente, com parceiros que também possuem essa ferramenta implementada em sua empresa, fazendo com que a vantagem surja no ponto em que uma empresa poderá ser contratada por outra justamente por ter uma boa política de coleta e proteção de dados[148].

Nesse contexto, a adequação à LGPD, quando associada a mecanismos efetivos de governança e *compliance*, passa a representar diferencial estratégico relevante, permitindo às organizações fortalecer relações negociais, ampliar oportunidades comerciais e consolidar vantagens competitivas em setores marcados pela intensa circulação de informações e dados pessoais.

Um estudo realizado pela CISCO no ano de 2020 denominado “Da privacidade ao lucro: como obter retornos positivos sobre investimentos em privacidade” demonstrou que, cada vez mais, as empresas veem nas certificações relacionadas a privacidade um fator de compra decisivo para realizar negócios com outras empresas como se demonstra no gráfico a seguir:

Figura 5 - Percentual de empresas que consideram certificações em privacidade um fator de compra



Fonte: Da privacidade ao lucro: como obter retornos positivos sobre investimento em privacidade[149].

[148] BLOK, Marcela. ***Compliance* e Governança Corporativa.** 4. ed. Rio de Janeiro: Freitas Bastos, 2023. Versão eletrônica.
[149] CISCO. **Da privacidade ao lucro:** como obter retornos positivos sobe investimento em privacidade.

Ademais, os clientes de uma determinada organização perceberão valor no modo como esta empresa possibilita que eles façam a gestão dos dados que a ela são disponibilizados durante as transações, seja no ambiente físico ou virtual, o que aumentará a percepção de valor no quesito segurança, de modo a fazer com que esse cliente volte a transacionar com essa empresa mais vezes pela segurança experimentada.

5.3 Valorização da Marca, da Reputação e da Imagem Empresarial

Como parte do valor que é gerado às empresas que têm em seus contextos a governança e o *compliance* sobre o tratamento de dados pessoais que realizam, estão a valorização da própria marca, da reputação e da imagem empresarial, pois ao se adequarem à LGPD, as organizações acabam por implementar práticas pautadas na ética, na transparência, na responsabilidade e no respeito aos direitos dos titulares dos dados, que refletem diretamente, nessa valorização.

Um estudo da Deloitte realizado em 2023, aponta que os consumidores estão, mais do que nunca, preocupados com a possibilidade de serem hackeados/rastreados durante suas interações no ambiente virtual. Quase 6 em cada 10 participantes temem que seus dispositivos sejam vulneráveis a violações de segurança. Fato novo está ligado à preocupação de 52% de usuários de casas inteligentes, terem receio com a privacidade relativa a seus dispositivos inteligentes[150].

> Para ajudar a reconquistar a confiança, os fabricantes de dispositivos e provedores de serviços devem responder às crescentes preocupações dos consumidores em relação a invasões e rastreamento, bem como ao seu desejo por mais transparência e controle sobre seus dados. As organizações devem considerar priorizar medidas robustas de segurança de dados e comunicar suas práticas de tratamento de dados de forma mais eficaz. Simplificar para os consumidores a compreensão de quais dados são coletados e como são usados, juntamente com o fornecimento de maneiras mais fáceis de controlar esse uso, pode criar uma vantagem competitiva. As empresas poderiam incentivar os usuários, em momentos apropriados, a fazer escolhas informadas sobre o uso de seus dados. A falha em ajudar as pessoas a reforçar a segurança e a privacidade de seus dados pode deixar as empresas vulneráveis à concorrência de empresas que têm como missão

2020. Disponível em: https://www.cisco.com/c/dam/global/pt_br/solutions/pdfs/2020-data-privacy-report-ptbr.pdf. Acesso em: 22 fev. 2026.

[150] ARBANAS, Jana; SILVERGLATE, Paulo; HUPFER, Susanne; LOUCKS, Jeff; RAMAN, Prashant; STEINHART, Michael. **As preocupações com a privacidade e a segurança dos dados estão aumentando, enquanto a confiança está em queda.** Deloitte: 2023. Disponível em: https://www.deloitte.com/us/en/insights/industry/telecommunications/connectivity-mobile-trends-survey/2023/data-privacy-and-security.html. Acesso em: 03 nov. 2025.

> proteger os dados do consumidor. Além de desejarem que as empresas ajudem, os consumidores também gostariam de ver mais regulamentações que imponham essa questão, e estas parecem inevitáveis[151].

Empresas que se mantêm cumprindo as legislações relativas ao negócio, tratando todos os envolvidos, mas, principalmente os clientes, de acordo com o que os ordenamentos jurídicos de proteção de dados preconizam, tem um ganho na percepção que esses interessados têm do negócio pelo cuidado que a empresa toma na relação entre eles. Esse aspecto é muito aparente no tratamento de dados pessoais, no qual os clientes, ao acessarem os ambientes, físicos e virtuais, das empresas conseguem perceber o cuidado que tais empresas têm com os dados que estão compartilhando.

O Relatório Cisco 2024 *Data Privacy Benchmark Study*, apresenta informações importantes que corroboram que a valorização da marca, da reputação e imagem empresarial são incrementadas através dos cuidados com privacidade, senão vejamos[152]:

> A privacidade tornou-se um elemento crítico e um facilitador da confiança do cliente, com 94% das organizações afirmando que seus clientes não comprariam delas se os dados não fossem protegidos adequadamente. 2. As organizações apoiam fortemente as leis de privacidade em todo o mundo, com 80% indicando que a legislação teve um impacto positivo sobre elas. 3. A economia da privacidade continua atrativa, com 95% afirmando que os benefícios superam os custos e a organização média obtendo um retorno de 1,6x sobre seu investimento em privacidade[153].

Em complemento, os clientes buscam cada vez mais evidências de que as empresas com as quais realizam negócios jurídicos sejam confiáveis em relação à privacidade, sendo que 98% das empresas entrevistadas no estudo realizado pela CISCO disseram que certificações de privacidade se tornaram determinantes para o

---

[151] ARBANAS, Jana; SILVERGLATE, Paulo; HUPFER, Susanne; LOUCKS, Jeff; RAMAN, Prashant; STEINHART, Michael. **As preocupações com a privacidade e a segurança dos dados estão aumentando, enquanto a confiança está em queda.** Deloitte: 2023. Disponível em: https://www.deloitte.com/us/en/insights/industry/telecommunications/connectivity-mobile-trends-survey/2023/data-privacy-and-security.html. Acesso em: 03 nov. 2025

[152] CISCO. **Privacy as na Enabler of Customer Trust. Cisco 2024 Data Privacy Benchmark Study**. p.3. Disponível em: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2024.pdf. Acesso em 05 nov. 2025.

[153] Texto original: *Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly. 2. Organizations strongly support privacy laws around the world, with 80% indicating legislation has had a positive impact on them. 3. The economics of privacy remain attractive, with 95% saying benefits exceed costs and the average organization realizing a 1.6x return on their privacy investment.*

processo de compra[154].

Em síntese, aquelas empresas que conseguem fazer com que seus clientes percebam seu comprometimento com a proteção de dados, ganham em sua reputação e valor de marca.

5.4 Eficiência Operacional e Atração de Investimentos

A implementação de estruturas de governança corporativa e programas de *compliance* voltados à proteção de dados também produz impactos relevantes na eficiência operacional das organizações. Isso ocorre porque a adequação à LGPD exige mapeamento de processos internos, definição de responsabilidades, padronização de procedimentos e criação de mecanismos de monitoramento contínuo, fatores que contribuem para maior organização administrativa e redução de falhas operacionais.

Quando uma empresa atende às legislações relativas ao tratamento de dados é pouco provável que tenha que gastar recursos (humanos, financeiros, tempo) com a resolução de problemas advindos de incidentes relacionados aos dados dos clientes que ali são tratados, de modo que, assim, consegue ser mais eficiente em outros aspectos mais importantes do seu dia a dia[155].

Sob a ótica dos investidores, é mais interessante para a realização de um investimento que este seja feito em empresas sólidas, com chances remotas de se envolverem em problemas jurídicos de grande monta, e também, onde é possível visualizar que o tratamento de dados está em conformidade com as leis vigentes[156].

A proteção que os investidores têm quando uma empresa está em *compliance* com os regulamentos normativos que sobre ela incidem, bem como, quando esta organização possui governança corporativa em sua gestão, aumentam a segurança que estes investidores têm sobre o investimento que é feito em empresas, contribuindo também, com a diminuição dos custos de capital dessa empresa[157].

---

[154] CISCO. **Privacy as an Enabler of Customer Trust. Cisco 2024 Data Privacy Benchmark Study**. p.4. Disponível em: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2024.pdf. Acesso em 05 nov. 2025.

[155] BLOK, Marcela. ***Compliance* e Governança Corporativa.** 4. ed. Rio de Janeiro: Freitas Bastos, 2023. Versão eletrônica.

[156] BLOK, Marcela. ***Compliance* e Governança Corporativa.** 4. ed. Rio de Janeiro: Freitas Bastos, 2023. Versão eletrônica.

[157] MACHADO, Luiz Kennedy Cruz; PRADO, José Willer do; RAUBER, Laurí Luis; CARVALHO, Eduardo Gomes; SANTOS, Antônio Carlos dos. **A influência da governança corporativa no desempenho financeiro, na oportunidade de crescimento e no valor de mercado das firmas:** uma

5.5 Limitação de Responsabilidade e Mitigação de Gastos com Vazamentos de Dados

A existência de mecanismos efetivos de governança corporativa e *compliance* relacionados à proteção de dados pessoais mostra-se relevante no contexto da responsabilização decorrente de incidentes de segurança da informação. Conforme abordado anteriormente, a adoção de políticas internas, medidas técnicas e administrativas, protocolos de resposta a incidentes e práticas de monitoramento contínuo demonstra maior diligência organizacional no tratamento de dados pessoais.

No que concerne à limitação de responsabilidade em virtude de um vazamento de dados ocasionado, o artigo 52 inciso VIII da LGPD demonstra que a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, podem diminuir as sanções recebidas em decorrência de vazamentos de dados por ela ocasionados[158].

Nesse contexto, estar em conformidade com a Lei Geral de Proteção de Dados Pessoais possibilita que os controladores de dados, que em virtude de incidentes de tratamento que possam acontecer, sejam beneficiados com a diminuição das sanções que a eles seriam impostas caso consigam provar que mantêm em sua estrutura mecanismos e procedimentos de trabalho capazes de diminuir as consequências desses vazamentos.

Ademais, estar em conformidade pode trazer economia de recursos financeiros que são gastos em virtude de acontecimentos relacionados aos próprios vazamentos de dados. Um estudo da IBM demonstra que o custo médio global de uma violação de dados é de 4,4 milhões de dólares, fora os relacionados às sanções propriamente ditas[159].

Para denotar ainda mais a importância de as organizações estarem em conformidade com os ditames da LGPD, apresenta-se, na sequência, uma listagem com sanções impostas a empresas nacionais e estrangeiras em virtude de

---

análise com modelagem de equações estruturais. Enfoque: Reflexão Contábil, Maringá/Pr, volume 39, número 2, p.31. Disponível em: https://periodicos.uem.br/ojs/index.php/Enfoque/article/view/45852 Acesso em 10 set 2025.

[158] BRASIL. **Lei nº 13.709. Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília, DF, 14 de agosto de 2018.

[159] IBM. **Relatório do custo das violações de dados 2025.** Disponível em: https://www.ibm.com/br-pt/reports/data-breach. Acesso em 12 nov. 2025.

vazamentos de dados.

O Painel LGPD, disponibilizado pela ANPD aponta que entre 2022 e 2025 tramitaram doze processos sancionadores de empresas privadas e entes públicos que de algum modo fizeram má utilização de dados que coletaram, trazendo (ou podendo trazer) de fato, prejuízos aos titulares[160].

Dentre esses doze processos sancionadores, oito já constam como concluídos, sendo que sete são de empresas públicas, e somente um de empresa privada, que por coincidência, foi o primeiro caso brasileiro de aplicação de multa à empresa *Telekall Infoservice*, cujo valor da multa foi de 2% do faturamento bruto, resultando em um valor de R$14.400,00 (quatorze mil e quatrocentos reais)[161].

Cabe anotar que, dos quatro processos que estão em andamento, dois são de empresas públicas e dois são de empresas privadas, quais sejam, a RaiaDrogasil S.A.[162] e a *Bytedance* Brasil *Tecnologia* Ltda (*TikTok*)[163] podendo ser autuadas em grandes valores pecuniários, com limite de 50 milhões de reais, disposto na Lei 13.709/18, dada a grande magnitude de dados que são tratados.

A despeito do número de processos sancionadores ainda ser pequeno, o que em certa medida demonstra uma certa ineficiência na fiscalização por parte do Estado, ou um certo desconhecimento dos direitos que os titulares de dados têm, vale ressaltar que o aspecto jurídico, no que toca a responsabilidade civil é um ponto de preocupação inerente à possíveis vazamentos de dados.

Entretanto, no âmbito internacional, grandes empresas já foram autuadas, conforme se demonstra na tabela abaixo:

Tabela 5 – Empresas que já receberam multas relativas à proteção de dados

EMPRESA	SANÇÕES
Amazon	Multada em 746 milhões de Euros pela Luxembourg *National*

[160] ANPD. **Painel ANPD. Estatísticas dos Processos.** Disponível em: https://app.powerbi.com/view?r=eyJrIjoiYmZlMmM5YzItMzQ1MS00N2E2LThhYTctMTYwZTliOGJmZWM0IiwidCI6IjVhYmEwNGExLWY4NjMtNGI1Ni04MTdkLTQ0MjkxYzkwZDFiOCJ9. Acesso em: 8 fev. 2026.

[161] ANPD. **ANPD aplica a primeira multa por descumprimento à LGPD.** Brasília, 07 de julho de 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd. Acesso em: 8 fev. 2026.

[162] O processo está integralmente disponível através do site: https://www.gov.br/anpd/pt-br/assuntos/noticias/SEI_ANPD0168027NotaTcnica62025Pub.pdf.

[163] O processo está integralmente disponível através do site: https://www.gov.br/anpd/pt-br/assuntos/noticias/nota-tecnica-50_pub_0153891.pdf.

	Commission for Data Protection[164]
British Airways	Multada em 20 milhões de libras pelo Gabinete do Comissário de Informação do Reino Unido (ICO)[165]
Marriot (hotéis)	Multada em 18,4 milhões de libras pelo *The Information Commissioner's Office* (ICO)[166]
Google LLC	Multada em 50 milhões de euros pela *National Data Protection* Commission (CNIL)[167]
H&M (moda)	Multada em 35.3 milhões de euros pelo *Hamburg Commissioner for Data Protection and Freedom of Information* (HmbBfDI)[168]
TIM (*Telecom* Italia)	Multada em 27.8 milhões de euros pela autoridade italiana de proteção de dados[169]

Fonte: elaborado pelo autor.

Para não estender com muitos exemplos, esses foram trazidos apenas para ilustrar o quão gravoso pode ser para uma empresa receber uma multa advinda de problemas com proteção de dados que são por ela tratados, corroborando a ideia de que, manter ou investir em governança corporativa e no *compliance* de dados, traz, de acordo com o nível de maturidade das empresas nestes aspectos, mais ou menos vantagens.

[164] DATA PRIVACY MANAGER. **Luxembourg DPA issues €746 million GDPR Fine to Amazon.** Disponível em: https://dataprivacymanager.net/luxembourg-dpa-issues-e746-million-gdpr-fine-to-amazon/. Acesso em 8 fev. 2026.

[165] BBC. **British Airways fined £20M over data breach.** Disponível em: https://www.bbc.com/news/technology-54568784. Acesso em 8 fev. 2026.

[166] REUTERS. **UK's ICO fines Marriott 18.4 mln pounds for failing to secure customer data.** Disponível em: https://www.reuters.com/business/uks-ico-fines-marriott-184-mln-pounds-failing-secure-customer-data-2020-10-30/. Acesso em: 8 fev. 2026.

[167] EUROPEAN DATA PROTECTION BOARD - EDPB. **The CNIL's restricted committee imposes a financial penalty of 50 Milion euros Against GOOGLE LLC.** Disponível em: https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en. Acesso em: 9 fev. 2026.

[168] EUROPEAN DATA PROTECTION BOARD - EDPB. **Hamburg Commissioner Fines H&M 35.3 Million Euro for Data Protection Violations in Service Centre.** Disponível em: https://www.edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_en. Acesso em: 9 fev. 2026.

[169] EUROPEAN DATA PROTECTION BOARD - EDPB. **Marketing: The Italian AS fines TIM EUR 27.8 million.** Disponível em: https://www.edpb.europa.eu/news/national-news/2020/marketing-italian-sa-fines-tim-eur-278-million_en. Acesso em: 9 fev. 2026.

CONCLUSÃO

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18) foi concebida, antes de tudo, como instrumento de proteção de um direito fundamental, qual seja, a privacidade dos titulares de dados. Todavia, sua aplicação no ambiente empresarial revela uma dimensão que vai além da tutela individual, alcançando de forma concreta o direito negocial e a organização das atividades econômicas, no ponto em que, sob a ótica negocial, adequar-se à LGPD pode agregar vantagens ao negócio.

O que se verificou ao longo desta dissertação é que a adequação à LGPD, embora podendo ser vista como um ônus regulatório, não se resume a isso. Quando inserida em um contexto de governança corporativa bem estruturada e associada a programas sérios de *compliance*, especialmente no campo do *compliance* de dados, a conformidade normativa pode ganhar caráter estratégico, contribuindo para a mitigação de riscos, o fortalecimento da reputação e a melhoria das relações negociais.

Por isso, a LGPD não deve ser lida apenas como mecanismo de controle imposto às empresas. Ela carrega também um potencial real de geração de valor, contudo esse potencial depende diretamente da forma como a lei é incorporada à estrutura empresarial. A adequação meramente formal, desacompanhada de uma cultura de governança e de práticas efetivas de *compliance*, tende a não lograr todos os benefícios que a adequação à lei pode trazer, ficando restrita ao cumprimento mínimo do que a lei exige.

Por outro lado, empresas que de fato internalizam os princípios da proteção de dados e os integram às suas estratégias e estruturas de governança e *compliance,* têm condições de transformar a conformidade em vantagem competitiva, diferenciando-se no mercado e fortalecendo sua posição perante todos os *stakeholders* da empresa.

Ainda, programas de *compliance* relacionados à proteção de dados influenciam diretamente a cultura organizacional e os padrões de comportamento dos colaboradores, haja vista que estes pressupõem práticas éticas, transparentes, responsáveis de modo a promover mudanças institucionais.

Conclui-se, portanto, que a LGPD, embora fundada na proteção de direitos fundamentais, apresenta uma dimensão mercadológica relevante no contexto empresarial contemporâneo, podendo atuar como instrumento de geração de valor,

quando articulada de forma consistente com práticas de governança corporativa e compliance.

A resposta ao problema de pesquisa, assim, não é única e direta, haja vista que a LGPD pode tanto ser vista como somente um mecanismo de controle regulatório, quanto se configurar como instrumento estratégico, e o que define essa diferença é a maturidade organizacional das empresas e a efetividade das estruturas de governança e *compliance* que estas adotam.

REFERÊNCIAS

A AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **ANPD aplica a primeira multa por descumprimento à LGPD.** Brasília, 7 jul. 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd. Acesso em: 8 fev. 2026.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Painel ANPD: estatísticas dos processos**. Disponível em: https://app.powerbi.com/view?r=eyJrIjoiYmZlMmM5YzItMzQ1MS00N2E2LThhYTctMTYwZTliOGJmZWM0IiwidCI6IjVhYmEwNGExLWY4NjMtNGI1Ni04MTdkLTQ0MjkxYzkwZDFiOCJ9. Acesso em: 8 fev. 2026.

AMARAL, Francisco. **Direito civil:** introdução. 10. ed. São Paulo: Saraiva Educação, 2018.

ANDRADE, Renato Campos. **Compliance como realizador do ESG:** construção dos pilares com foco no ambiental. São Paulo: Editora Dialética, 2024. ePUB.

ARBANAS, Jana et al. As preocupações com a privacidade e a segurança dos dados estão aumentando, enquanto a confiança está em queda. **Deloitte**, 2023. Disponível em: https://www.deloitte.com/us/en/insights/industry/telecommunications/connectivity-mobile-trends-survey/2023/data-privacy-and-security.html. Acesso em: 3 nov. 2025.

ASSI, Marcos. **Governança, riscos e compliance**: mudando a conduta nos negócios. São Paulo: Saint Paul Editora, 2017.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27701:**2019: técnicas de segurança — extensão para a ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — requisitos e diretrizes. Rio de Janeiro: ABNT, 2019.

BALKIN, Jack. How to regulate (and not regulate) social media. **Journal of Free Speech Law**, v. 1, n. 71, p. 84, 2021. Tradução livre. Disponível em: https://www.journaloffreespeechlaw.org/balkin.pdf. Acesso em: 14 fev. 2026.

BARBIERI, Carlos. **Uma visão sintética e comentada do Data Management Body of Knowledge (DMBOK).** Belo Horizonte: Funsoft, 2013.

BARBIERI, Carlos; FARINELLI, Fernanda. Uma visão sintética e comentada do Data Management Body of Knowledge (DMBOK). **FUMSOFT**, 16 abr. 2024. Disponível em: https://www.researchgate.net/publication/297699158_Uma_visao_sintetica_e_comentada_do_Data_Management_Body_of_Knowledge_DMBOK. Acesso em: 13 abr. 2026.

BBC. **British Airways fined £20M over data breach.** Disponível em: https://www.bbc.com/news/technology-54568784. Acesso em: 8 fev. 2026.

BITTENCOURT, Carlos Magno Andrioli. **Governança corporativa e compliance:** planejamento e gestão estratégica. Curitiba: Contentus, 2020. E-book. p. 16.

BLOK, Marcela. **Compliance e governança corporativa**. 4. ed. Rio de Janeiro: Freitas Bastos, 2023. E-book.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988.

BRASIL. Projeto de Lei nº 4.060, de 2012. **Dispõe sobre o tratamento de dados pessoais**, **e dá outras providências.** Brasília, DF: Câmara dos Deputados, 2012.

BRASIL. Projeto de Lei do Senado nº 330, de 2013. **Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais**, **e dá outras providências.** Brasília, DF: Senado Federal, 2013.

BRASIL. Instituto Nacional de Tecnologia da Informação (ITI). **Programa de Integridade e Compliance.** Brasília, DF: ITI, 2018. Disponível em: https://www.gov.br/iti/pt-br/acesso-a-informacao/institucional/Programa_de_Integridade_e_Compliance___Assinado_1.pdf. Acesso em: 22 abr. 2026.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 9 maio 2025.

BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. Secretaria de Tecnologia da Informação. Portaria nº 58, de 23 de dezembro de 2016. **Dispõe sobre os procedimentos complementares referentes às diretrizes de gestão de documentos arquivísticos digitais.** Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/portarias-federais/portaria-no-58-de-23-de-dezembro-de-2016. Acesso em: 19 abr. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014.** Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 9 maio 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Programa de Privacidade e Segurança da Informação (PPSI). **Guia sobre privacidade desde a concepção e por padrão**. Brasília, DF: MGI, 2024.

BRASIL. Superior Tribunal de Justiça. **Agravo em Recurso Especial nº 2.130.619/SP**. Brasília, DF, 7 mar. 2023.

BRUNO, Marcos Gomes da Silva. Dos agentes de tratamento de dados pessoais. In: MALDONADO, Viviane Nobre; BLUM, Renato Opice (org.). **LGPD: lei geral de proteção de dados comentada.** São Paulo: Thomson Reuters Brasil, 2019. E-book.

cap. 6.

CAVALIERI FILHO, Sergio. **Programa de responsabilidade civil**. 10. ed. São Paulo: Atlas, 2012.

CAVOUKIAN, Ann. Privacy and security by design. [S.l.]: **YouTube**, 29 abr. 2025. 1 vídeo. Disponível em: https://www.youtube.com/watch?v=I8FCCogzX28. Acesso em: 11 set. 2025.

CISCO. Da privacidade ao lucro: como obter retornos positivos sobre investimento em privacidade. [S.l.]: **Cisco**, 2020. Disponível em: https://www.cisco.com/c/dam/global/pt_br/solutions/pdfs/2020-data-privacy-report-ptbr.pdf. Acesso em: 22 fev. 2026.

CISCO. Privacy as an Enabler of Customer Trust: Cisco 2024 Data Privacy Benchmark Study. [S.l.]: **Cisco**, 2024. p. 3. Disponível em: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2024.pdf. Acesso em: 5 nov. 2025.

COMPARATO, Fábio Konder. **Rumo à justiça**. São Paulo: Saraiva, 2010. p. 41.

DATA PRIVACY MANAGER. **Luxembourg DPA issues €746 million GDPR fine to Amazon.** Disponível em: https://dataprivacymanager.net/luxembourg-dpa-issues-e746-million-gdpr-fine-to-amazon/. Acesso em: 8 fev. 2026.

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: BIONI, Bruno (org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 30-37.

EUROPEAN DATA PROTECTION BOARD (EDPB). **Hamburg Commissioner fines H&M 35.3 million euro for data protection violations in service centre**. Disponível em: https://www.edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_en. Acesso em: 9 fev. 2026.

EUROPEAN DATA PROTECTION BOARD (EDPB). **The CNIL's restricted committee imposes a financial penalty of 50 million euros against Google LLC**. Disponível em: https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en. Acesso em: 9 fev. 2026.

EUROPEAN DATA PROTECTION BOARD (EDPB). **Marketing:** the Italian SA fines TIM EUR 27.8 million. Disponível em: https://www.edpb.europa.eu/news/national-news/2020/marketing-italian-sa-fines-tim-eur-278-million_en. Acesso em: 9 fev. 2026.

FEDERAÇÃO BRASILEIRA DE BANCOS (FEBRABAN). **Função de compliance. Coleção Instituto Febraban de Educação.** p. 11. Disponível em: https://www.febraban.org.br/7rof7swg6qmyvwjwf7i0asdf9jyv/sitefebraban/funcoescompliance.pdf. Acesso em: 12 out. 2025.

FRAZÃO, Ana; PINTO, Mariana. Compliance de Dados e Incidentes de Segurança. *In:* PINHEIRO, Caroline da Rosa. **Compliance entre a teoria e a prática.** Indaiatuba, SP: Editora Foco, 2022.

FRAZÃO, Ana; CARVALHO, Angelo Prata de. **A LGPD e a necessidade de adequação emergencial das estruturas empresariais. Passos preliminares e fundamentais para a conformidade.** Disponível em: https://www.professoraanafrazao.com.br/files/publicacoes/2021-03-04-A_LGPD_e_a_necessidade_de_adequacao_emergencial_das_estruturas_empresariais_Passos_preliminares_e_fundamentais_para_a_conformidade.pdf. Acesso em 24 abr. 2026.

FREITAS, Daniel Paulo Paiva. **Proteção e governança de dados.** Curitiba: Contentus, 2020. p.46.

GOMES, Orlando. **Contratos**. Atualização de Antonio Junqueira de Azevedo e Francisco Paulo de Crescenzo Marino. 26. ed. Rio de Janeiro: Forense, 2009.

GONÇALVES, Carlos Roberto. **Responsabilidade civil**. 21. ed. São Paulo: SaraivaJur, 2022.

IBM. **Relatório do custo das violações de dados 2025**. Disponível em: https://www.ibm.com/br-pt/reports/data-breach. Acesso em: 12 nov. 2025.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). **Código das melhores práticas de governança corporativa**. 6. ed. São Paulo: IBGC, 2023. Disponível em: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=24640. Acesso em: 12 ago. 2025.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC**). Portal do conhecimento**. Disponível em: https://www.ibgc.org.br/conhecimento/governanca-corporativa. Acesso em: 1 set. 2025.

JIMENE, Camila do Valle. Da segurança e das boas práticas. In: MALDONADO, Viviane Nobre; BLUM, Renato Opice (org.). **LGPD**: lei geral de proteção de dados comentada. São Paulo: Thomson Reuters Brasil, 2019. E-book. cap. 7.

KPMG BOARD LEADERSHIP CENTER. **Conselho de administração:** prioridades para a agenda de 2024. Disponível em: https://kpmg.com/br/pt/insights/2024/02/conselho-de-administracao-2024.html. Acesso em: 10 abr. 2026.

LIMA, André Gustavo Bastos; FAGUNDES, Vladimir. Implementação da governança em privacidade e proteção de dados. In: BARRETO, Gileno Gurjão; ANTONIO, André Luiz Sucupira; LIMA, André Gustavo Bastos (org.). **Governança em privacidade e proteção de dados: uma visão integrada aos negócios empresariais**. 1. ed. Curitiba: Editorial Casa, 2022.

LOBO, Jorge. Princípios de governança corporativa. **Revista do Ministério Público**,

Rio de Janeiro, n. 31, jan./mar. 2009. Disponível em: https://www.mprj.mp.br/documents/20184/2716675/Jorge_Lobo.pdf. Acesso em: 28 ago. 2025.

LÓSSIO, Claudio Joel Brito. **Proteção de dados e compliance digital**. 2. ed. São Paulo: Almedina, 2023. E-book.

MACHADO, Luiz Kennedy Cruz et al. A influência da governança corporativa no desempenho financeiro, na oportunidade de crescimento e no valor de mercado das firmas: uma análise com modelagem de equações estruturais. **Enfoque**: Reflexão Contábil, Maringá, v. 39, n. 2, p. 29. Disponível em: https://periodicos.uem.br/ojs/index.php/Enfoque/article/view/45852. Acesso em: 10 set. 2025.

MAIER, Jerry Antonio Raitz; FERREIRA, Hugo Silva. A governança corporativa e suas contribuições para as finanças empresariais: a importância da governança corporativa e do Chief Financial Officer (CFO) para as finanças empresariais. **Revista Científica Multidisciplinar O Saber**, v. 7, ed. especial. Disponível em: https://submissoesrevistarcmos.com.br/rcmos/article/view/664/1427. Acesso em: 2 out. 2025.

MAZZIONI, Sady et al. Reflexos das práticas ESG e da adesão aos ODS na reputação corporativa e no valor de mercado. **Revista Gestão Organizacional**, v. 16, n. 3, p. 61-62, 2023. Disponível em: https://bell.unochapeco.edu.br/revistas/index.php/rgo/article/view/7394. Acesso em: 2 out. 2025.

MELLO, Celso Antônio Bandeira de. **Curso de direito administrativo**. 17. ed. São Paulo: Malheiros, 2004.

NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos.** 1948. Disponível em: https://www.un.org/en/about-us/universal-declaration-of-human-rights. Acesso em: 8 ago. 2025.

NATIONAL ARCHIVES. **A declaração de direitos: uma transcrição**. Revisado em: 28 abr. 2025. Disponível em: https://www.archives.gov/founding-docs/bill-of-rights-transcript. Acesso em: 30 jun. 2025.

NEVES, Edmo Colnaghi. **Fundamentos de governança corporativa**: riscos, direito e compliance. Curitiba: InterSaberes, 2021. E-book.

OFFICE OF PRIVACY AND CIVIL LIBERTIES. **Overview of the Privacy Act:** 2020 edition. Atualizado em: 4 out. 2022. Disponível em: https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/introduction. Acesso em: 30 jun. 2025.

ORGANIZAÇÃO PARA A COOPERAÇÃO E O DESENVOLVIMENTO ECONÔMICO (OCDE). **Princípios de governação corporativa do G20/OCDE**. Paris: OCDE, 2024. p. 7. Disponível em: https://www.oecd.org/content/dam/oecd/pt/publications/reports/2023/09/g20-oecd-

principles-of-corporate-governance-2023_60836fcb/58478f0f-pt.pdf. Acesso em: 1 set. 2025.

PEREIRA, Caio Mário da Silva. **Responsabilidade civil**. Atualização de Gustavo Tepedino. 13. ed. Rio de Janeiro: Forense, 2022.

PORTER, Michael E. **Vantagem competitiva:** criando e sustentando um desempenho superior. 27. ed. Rio de Janeiro: Elsevier, 1989.

PRADO, Roberta Nioac. **Manual prático e teórico da empresa familiar:** organização patrimonial, planejamento sucessório, governança familiar e corporativa e estratégias societárias e sucessórias. São Paulo: SaraivaJur, 2023. E-book.

PRIVACY & BUSINESS COMPLIANCE. **Dia internacional da proteção de dados e a cronologia da LGPD.** Disponível em: https://pbcompliance.com.br/noticias/dia-internacional-da-protecao-de-dados-e-a-cronologia-da-lgpd/. Acesso em: 1 ago. 2025.

QUEIROZ, Renata Capriolli Zocatelli. A proteção de dados pessoais: a LGPD e a disciplina jurídica do encarregado de proteção de dados pessoais. Orientador: Álvaro Villaça Azevedo. 2021. 137 f. **Tese (Doutorado em Direito**) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021.

REALE, Miguel. **Lições preliminares de direito**. 25. ed., 21. tir. São Paulo: Saraiva, 2001.

REUTERS. **UK's ICO fines Marriott 18.4 mln pounds for failing to secure customer data.** Disponível em: https://www.reuters.com/business/uks-ico-fines-marriott-184-mln-pounds-failing-secure-customer-data-2020-10-30/. Acesso em: 8 fev. 2026.

ROCHA, Claudia da. Boas práticas e governança corporativa na ótica da Lei Geral de Proteção de Dados. In: TEIXEIRA, Tarcisio (org.). **Empresas e implementação da LGPD:** lei geral de proteção de dados pessoais. 2. ed. rev., ampl. e atual. São Paulo: Editora Juspodivm, 2022. cap. 3.

ROSA, Glaucio Monteiro. **Privacidade e proteção de dados: uma abordagem histórica e evolucionista.** In: BARRETO, Gileno Gurjão; ANTONIO, André Luiz Sucupira; LIMA, André Gustavo Bastos (org.). Governança em privacidade e proteção de dados: uma visão integrada aos negócios empresariais. 1. ed. Curitiba: Editorial Casa, 2022.

ROSENVALD, Nelson. **As funções da responsabilidade civil:** a reparação e a pena civil. São Paulo: Atlas, 2013.

SAAVEDRA, Giovani Agostini. **Compliance de dados**. In: BIONI, Bruno (org.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021. E-book.

TEIXEIRA, Tarcisio. **Direito empresarial sistematizado**. 12. ed. São Paulo: SaraivaJur, 2024.

TEIXEIRA, Tarcisio; GUERREIRO, Ruth Maria. **Lei geral de proteção de dados pessoais (LGPD):** comentada artigo por artigo. 4. ed. São Paulo: SaraivaJur, 2022.

TEIXEIRA, Tarcisio; KASEMIRSKI, André Pedroso. Compliance (conformidade) de dados pessoais para microempresas: autorregulação regulada e requisitos para efetividade. In: TEIXEIRA, Tarcisio (org.). **Empresas e implementação da LGPD:** lei geral de proteção de dados pessoais. 2. ed. rev., ampl. e atual. São Paulo: Editora Juspodivm, 2022. cap. 1.

TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. **Fundamentos do direito civil:** responsabilidade civil. 2. ed. Rio de Janeiro: Forense, 2021. E-book.

TOMASEVICIUS FILHO, Eduardo. **O princípio da boa-fé no direito civil.** São Paulo: Almedina, 2020.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, 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 — GDPR). **Jornal Oficial da União Europeia**, L 119, 4 maio 2016.

UNIVERSITY OF MICHIGAN. Information and Technology Services. **Safe Computing. History of privacy timeline.** Disponível em: https://safecomputing.umich.edu/protect-privacy/history-of-privacy-timeline. Acesso em: 7 jun. 2025.

VAINZOF, Rony. Disposições preliminares. In: MALDONADO, Viviane Nobre; BLUM, Renato Opice (org.). **LGPD**: lei geral de proteção de dados comentada. São Paulo: Thomson Reuters Brasil, 2019. E-book. cap. 1.

VIEIRA, Lucas Pacheco. **Compliance de dados pessoais**. Revista de Direito e as Novas Tecnologias, v. 22, p. 3, 2024. Disponível em: https://www.researchgate.net/profile/Lucas-Vieira-12/publication/382217030_COMPLIANCE_DE_DADOS_PESSOAIS/links/6691f503af9e615a15e309c0/COMPLIANCE-DE-DADOS-PESSOAIS.pdf. Acesso em: 15 out. 2025.