

A GOVERNANÇA DE DADOS COMO INSTRUMENTO DE GARANTIA DO DIREITO À PRIVACIDADE: uma abordagem jurídica à luz da Lei Geral de Proteção de Dados (Lei n. 13.709/2018)

DATA GOVERNANCE AS AN INSTRUMENT TO GUARANTEE THE RIGHT TO PRIVACY: A Legal Approach in Light of the General Data Protection Law (Law No. 13.709/2018)

Raiane Castro de Moura¹

Alana Taise Castro Sartori²

Recebido/Received: 20.01.2026/Jan 20th, 2026

Aprovado/Approved: 25.02.2026/Feb 25th, 2026

RESUMO: A governança de dados configura-se como um instrumento essencial para a garantia do direito fundamental à privacidade na era digital, à luz da Lei Geral de Proteção de Dados, conhecida popularmente como LGPD (Lei n. 13.709/2018). Embora a LGPD tenha surgido como marco regulatório essencial, sua eficácia depende da adoção de práticas internas, especialmente no âmbito privado. Neste contexto, a governança de dados assume um papel jurídico-organizacional ao implementar políticas, processos e uma cultura de proteção de dados que reforçam os princípios estabelecidos pela LGPD. Partindo dessa premissa, a pesquisa busca responder a seguinte questão: de que forma a governança de dados contribui para efetiva proteção do direito à privacidade dos titulares dos dados, conforme previsto na LGPD? O objetivo geral é investigar de que forma a governança de dados, fundamentada na Lei Geral de Proteção de Dados, assegura a proteção do direito à privacidade no âmbito das empresas privadas. Como objetivos específicos, pretende-se: explicar o conceito de direito à privacidade, com base na Constituição Federal (CRFB/1988) de 1988 e na Lei Geral de Proteção de Dados, destacando a relevância da sua proteção na atualidade; analisar o que é a governança de dados e qual o seu papel nas empresas privadas, para garantir a proteção do direito à privacidade; e examinar as disposições da Lei Geral de Proteção de Dados e suas implicações na segurança das informações pessoais, abordando a necessidade de adotar práticas de governança de dados para garantir o cumprimento desta legislação. A pesquisa utiliza o método de abordagem dedutivo, pois origina-se de premissas gerais, como a análise do direito à privacidade e a governança de dados. Quanto ao método de procedimento, elegeu-se o método monográfico, visto que o estudo envolve a pesquisa sobre uma temática sob diferentes aspectos de abordagem, baseando-se no levantamento bibliográfico e legislativo quanto à

¹ Bacharela em Direito pela Universidade Regional Integrada do Uruguai e das Missões (URI São Luiz Gonzaga/RS). E-mail: 099190@saoluiz.uri.edu.br.

² Doutoranda e Mestre em Direito pela Universidade Regional Integrada do Uruguai e das Missões (URI/RS). Docente do curso de graduação em Direito da URI. E-mail: alanas@san.uri.br. Currículo Lattes: <http://lattes.cnpq.br/3072936815192617>. ORCID: <https://orcid.org/0000-0002-6015-7371>.

temática. Espera-se que esta pesquisa contribua significativamente para a compreensão do papel estratégico da governança de dados como instrumento efetivo de proteção do direito à privacidade no ambiente corporativo. Revelou-se, enfim, que, a implementação da governança de dados representa uma mudança cultural: sem ela, a LGPD permanece apenas formal; com ela, integra-se à prática institucional, visando a proteção do direito à privacidade na era da informação.

PALAVRAS-CHAVE: direito à privacidade; governança de dados; Lei Geral de Proteção de Dados; Lei n. 13.709/2018.

ABSTRACT: Data governance is an essential instrument for guaranteeing the fundamental right to privacy in the digital age, in light of the General Data Protection Law, popularly known as LGPD (Law No. 13.709/2018). Although the LGPD has emerged as an essential regulatory framework, its effectiveness depends on the adoption of internal practices, especially in the private sector. In this context, data governance assumes a legal-organizational role by implementing policies, processes, and a data protection culture that reinforce the principles established by the LGPD. Based on this premise, this research seeks to answer the following question: how does data governance contribute to the effective protection of the right to privacy of data subjects, as provided for in the LGPD? The overall objective is to investigate how data governance, based on the General Data Protection Law, ensures the protection of the right to privacy within private companies. The specific objectives of this study are: to explain the concept of the right to privacy, based on the 1988 Federal Constitution (CRFB/1988) and the General Data Protection Law, highlighting the relevance of its protection today; to analyze what data governance is and its role in private companies to guarantee the protection of the right to privacy; and to examine the provisions of the General Data Protection Law and their implications for the security of personal information, addressing the need to adopt data governance practices to ensure compliance with this legislation. The research uses a deductive approach, as it originates from general premises, such as the analysis of the right to privacy and data governance. Regarding the procedural method, the monographic method was chosen, since the study involves research on a topic from different perspectives, based on bibliographic and legislative research on the subject. It is expected that this research will contribute significantly to the understanding of the strategic role of data governance as an effective instrument for protecting the right to privacy in the corporate environment. It has finally become clear that the implementation of data governance represents a cultural shift: without it, the LGPD (Brazilian General Data Protection Law) remains merely formal; with it, it integrates into institutional practice, aiming to protect the right to privacy in the information age.

KEYWORDS: right to privacy; data governance; General Data Protection Law; Law No. 13.709/2018.

INTRODUÇÃO

Esse trabalho versa sobre as contribuições da governança de dados na proteção do direito à privacidade à luz da Lei Geral de Proteção de Dados, conhecida popularmente como LGPD (Lei n. 13.709/2018) em empresas privadas no Brasil. Com o avanço da tecnologia, a internet tornou-se um instrumento de exploração indiscriminada de dados pessoais. Tal prática ocorre através de uma dinâmica comercial, em que os usuários precisam fornecer informações pessoais, em troca de acesso a bens ou serviços, o que enfraquece o direito fundamental à privacidade. Diante desse cenário, a LGPD (Lei n. 13.709/2018) surge como resposta à vulnerabilidade dos usuários e de sua privacidade, impondo a governança de dados como um freio à atuação das empresas.

Embora a legislação alcance igualmente os dados tratados em suportes físicos, o presente trabalho concentrou sua análise predominantemente na proteção da privacidade dos usuários no ambiente digital. Nesse sentido, a pesquisa visa responder a seguinte questão: de que forma a governança de dados contribui para efetiva proteção do direito à privacidade dos titulares dos dados, conforme previsto na LGPD? O objetivo central da pesquisa, é, portanto, investigar de que forma a governança de dados, fundamentada na Lei Geral de Proteção de Dados, assegura a proteção do direito à privacidade no âmbito das empresas privadas.

De forma complementar, apresentam-se os seguintes objetivos específicos: a) explicar o conceito de direito à privacidade, com base na Constituição Federal de 1988 (CRFB/1988) e na Lei Geral de Proteção de Dados, destacando a relevância da sua proteção na atualidade; b) analisar o que é a governança de dados e qual o seu papel nas empresas privadas, para garantir a proteção do direito à privacidade; c) examinar as disposições da Lei Geral de Proteção de Dados e suas implicações na segurança das informações pessoais, abordando a necessidade de adotar práticas de governança de dados para garantir o cumprimento desta legislação.

A motivação para esse estudo decorre da trajetória profissional da acadêmica, que, em seu exercício profissional com tecnologias que envolvem o processamento informacional, desenvolveu um interesse em relação à implementação da governança de dados sob a perspectiva jurídica, nas empresas privadas. Esta, por sua vez, apresenta-se como um instrumento de auxílio na efetiva aplicação da Lei

Geral de Proteção de Dados, preservando, assim, o direito à privacidade dos titulares dos dados.

Frente à nova realidade digital, os dados demonstram-se como ativos valiosos para a sociedade, fazendo-se necessária, uma análise da preocupante lacuna informacional existente no tratamento de dados pessoais. Isto ocorre, devido a relevância social que essas informações possuem, especialmente no contexto empresarial. Tem-se, portanto, a governança de dados como uma exigência normativa, a qual representa um alicerce indispensável para a preservação do direito à privacidade.

Aqui, instala-se a importância desta temática na atualidade, tanto no âmbito universitário quanto para a sociedade como um todo. De modo que, para as universidades, tal estudo está intrinsecamente ligado à formação dos profissionais de direito, sobretudo quanto à compreensão do papel da governança de dados para as empresas privadas. Bem como, no desenvolvimento da aptidão para auxiliá-las no cumprimento das normativas, perante a crescente demanda pela implementação da LGPD.

No que se refere à metodologia utilizada no trabalho, a pesquisa delineou-se através do método de abordagem dedutivo, originando-se de premissas gerais, como a análise do direito à privacidade e a governança de dados. De modo que se possa analisar, em específico, como a implementação da governança de dados contribui para o direito à privacidade no setor privado. Quanto ao método de procedimento, elegeu-se o método monográfico, pois o estudo envolve a pesquisa sobre uma temática sob diferentes aspectos de abordagem.

Tal método, por sua vez, baseou-se no levantamento bibliográfico e legislativo quanto à temática. Por fim, classifica-se, ainda, como uma pesquisa exploratória e bibliográfica. É exploratória por buscar o aprofundamento do conhecimento sobre o tema da governança de dados e sua relação com a proteção do direito à privacidade, e bibliográfica por se apoiar em fontes já publicadas, como livros, artigos acadêmicos e legislações.

Quanto à organização do texto do artigo, este subdivide-se em três momentos. No primeiro, desenvolve-se a conceituação do direito à privacidade, com base na Constituição Federal de 1988 e na Lei Geral de Proteção de Dados. O segundo momento dedica-se à análise da governança de dados, suas definições, princípios e relevância para as empresas privadas. Por fim, o terceiro aborda as

contribuições das práticas de governança de dados para a efetivação do direito à privacidade, especialmente no processo de implementação da LGPD no âmbito corporativo.

1 O DIREITO À PRIVACIDADE NA CONSTITUIÇÃO FEDERAL DE 1988 (CRFB/1988) E NA LEI GERAL DE PROTEÇÃO DE DADOS (LEI N. 13.709/2018)

A privacidade, em seu contexto geral, é o direito inerente à pessoa humana de controlar suas informações, sejam elas de cunho pessoal, comercial ou profissional, permitindo-lhes a decisão de mantê-las em sigilo ou compartilhá-las em sociedade. Esta, correlaciona-se com um pilar fundamental na vida humana: o livre desenvolvimento da personalidade, o qual representa um equilíbrio emocional para sociedade como um todo, especialmente diante da constante exposição de informações (Branco; Mendes, 2024).

Aqui, pondera-se a importância da privacidade, sobretudo, quanto à possibilidade de identificar a pessoa humana através de seus dados¹, sejam eles fornecidos voluntariamente a empresas e órgãos públicos, ou mesmo coletados de forma externa, sem o conhecimento direto do usuário. Neste ponto, observa-se os dados, como manifestações concretas da personalidade de cada indivíduo, de modo que demandam proteção jurídica em razão da sua ligação com a dignidade humana. Dito isso, a privacidade é uma garantia essencial para proteção de informações pessoais, ou seja, quaisquer dados referentes a uma pessoa (Doneda, 2019).

A priori, faz-se necessário um olhar atento, ao art. 5º, X, da Constituição Federal Brasileira de 1988 (CRFB/1988), que consagra a privacidade como um direito constitucional:

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:
(...)

1 Considera-se *dado* o estado primitivo da informação. Dados são simplesmente fatos brutos que, quando processados e organizados, se convertem em algo inteligível, podendo ser deles extraída uma informação (BIONI, 2019). Por outro lado, de acordo com o art. 5º, I, da Lei nº 13.709/2018 (LGPD), dado pessoal é a “informação relacionada a pessoa natural identificada ou identificável”. Ou seja, o dado pessoal é a informação que permite que uma pessoa seja identificada.

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (Brasil, 1988, s.p.).

Isto significa que o direito à privacidade representa uma limitação jurídica à ingerência da coletividade no que tange à esfera íntima e pessoal de cada indivíduo. Observa-se que a Constituição Brasileira optou pela alusão ao princípio da privacidade, em sua máxima abrangência, resguardando todas as prerrogativas que o integram, tais como a proteção da intimidade, dos aspectos relacionados à vida pessoal e da personalidade humana, reforçando, assim, a autonomia do titular sobre suas informações pessoais privadas. Aqui, compreende-se a ideia de esfera privada não apenas nas relações familiares, domésticas ou particulares, como também nas ações, padrões comportamentais, pensamentos, projetos existenciais e informações que o indivíduo mantém em sigilo (Tavares, 2024).

Surge então, a partir dessa perspectiva, a privacidade como exercício de liberdade, revestindo-se de uma nova concepção jurídica e filosófica. Isto porque, há uma relação intrínseca entre privacidade e liberdade, a qual desdobra-se de múltiplas formas. Entende-se que ao resguardar sua intimidade, o indivíduo não apenas protege um direito fundamental, mas afirma sua própria liberdade. Liberdade esta, que se manifesta à medida que este determina a soberania de seu corpo, bem como garante segurança em suas comunicações e autodetermina suas escolhas pessoais, o que confere ao ser humano o poder de decidir o que será partilhado ao mundo (Gazolla, 2021).

A respeito disso, destaca-se que a CRFB/1988 estabelece em seu art. 1º, III, a soberania do princípio da dignidade da pessoa humana como um dos fundamentos do Estado Democrático de Direito¹. Esse princípio estrutura o ordenamento jurídico brasileiro, orientando a interpretação das normas e impondo limites ao exercício do poder do Estado e também das entidades privadas, exigindo que todas as relações jurídicas se pautem pelo respeito à pessoa humana. A dignidade atua, assim, como parâmetro normativo de conduta, impondo que a pessoa humana seja valorizada em sua integralidade, e não reduzida a objeto de manipulação ou instrumento para fins alheios (Blum, 2022).

1 "Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos: (...) III - a dignidade da pessoa humana" (Brasil, 1988, s.p.).

Frisa-se que, o referido princípio representa uma cláusula geral de tutela da personalidade, conferindo ao ser humano centralidade e protagonismo no ordenamento jurídico. Dentro dessa lógica, o direito à privacidade revela-se como um desdobramento da dignidade da pessoa humana, o qual supera a conceituação de segredo tornando-se mais próximo do controle que a pessoa possui sobre suas informações (Blum, 2022). Em outras palavras, visualiza-se a privacidade como uma chave mestra para autonomia individual. De modo que, sem ela, a sociedade possui acesso à camada mais íntima de cada indivíduo (Véliz, 2021).

Partindo dessa linha de pensamento, o direito à privacidade fomenta a existência de uma dualidade de fronteiras, a qual delimita o âmbito privado e o público. Sob este viés, as liberdades individuais, enquanto direitos inerentes da condição humana, consagram-se como a possibilidade de florescer em um ambiente que não há interferências externas. Destarte, tal direito consagra o exercício da autonomia, em que cada pessoa delimita seu espaço íntimo e, por consequência, alcança seu pleno desenvolvimento como ser humano (Tamer, 2024).

Por sua vez, esse equilíbrio social vê-se pressionado pelo crescimento exponencial dos avanços tecnológicos relacionados à internet, em que os dados informacionais ganham protagonismo no trânsito de informações virtuais. Se, por um lado, tais avanços acarretam incontáveis benefícios à humanidade, por outro, há um mar de desafios significativos a serem enfrentados. Nesse sentido, a privacidade é posta em constante risco, à medida que as pessoas se encontram à mercê de exposições constantes de suas informações (Vigliar, 2022).

É neste ambiente tecnológico que se percebe a existência de uma “bolha de imprivacidade”, termo este utilizado para referir-se à exposição diária e indevida dos usuários em ambiente virtual. Isto porque, denota-se uma imersão da privacidade na sociedade da informação, ao passo que é feito o gerenciamento e o uso de dados pessoais, o que evidencia a necessidade de adotar-se práticas institucionais eficazes para proteção dos titulares dos dados (Alves; Peixoto; Rosa, 2021). Blum (2022, p. 34) reforça essa necessidade ao observar que, acerca dos dados:

[...] o consumidor já está habituado a fornecê-los para realizar compras ou contratar serviços. Além disso, muitos têm “perfis” em sites de relacionamento na internet, como o Facebook, que já conta com cerca de 99 milhões de usuários no Brasil. Nestes “perfis”, as pessoas divulgam seus dados pessoais para efetivar o cadastro, além de compartilharem publicamente, no ambiente virtual, diversas informações privadas sobre o

seu modo de vida, como por exemplo, o status de relacionamento afetivo (casado, solteiro, etc.), dentre outras.

Isto se agrava na medida em que a permanência dos usuários nesse ecossistema digital, exige uma conexão contínua, eficiente e ininterrupta à internet, que, por sua vez, possibilita o tráfego de informações pessoais entre dispositivos, muitas vezes, sem que haja consentimento ou conhecimento prévio do usuário a respeito de quais informações serão coletadas ou compartilhadas (Alves; Peixoto; Rosa, 2022). Como resultado, abre-se espaço para a manipulação de informações em detrimento de terceiros, o que torna o detentor das informações possuidor de poder sob outras pessoas - tal como, ocorre, em instituições privadas que utilizam os dados não só como fonte de renda, mas sim, como forma de alavancar a venda de seus produtos ou serviços (Véliz, 2021).

A problemática central que se revela no horizonte de tais reflexões refere-se à possibilidade de exploração financeira das informações privadas coletadas de forma irregular em ambiente virtual. Essa prática consiste na coleta, armazenamento, análise e comercialização de informações individuais com fins lucrativos. As informações, obtidas muitas vezes por meio de cadastros, navegação na internet ou uso de aplicativos, são utilizadas para direcionar publicidade, criar perfis de consumo e influenciar decisões de compra. Embora tal prática impulse modelos de negócios baseados em personalização, cumpre ressaltar que ela suscita preocupações quanto à privacidade, à proteção de informações sensíveis, ao consentimento real dos titulares da informação e à sua destinação final. Como exemplo de caso envolvendo a comercialização de informações pessoais, cita-se os escândalos envolvendo a empresa Cambridge Analytica. O caso envolveu a coleta de dados de milhões de usuários do Facebook, sem consentimento prévio, que posteriormente foram comercializados para influenciar campanhas políticas, como o pleito presidencial dos Estados Unidos de 2016 e o referendo do Brexit (Fornasier; Beck, 2020).

Ademais, observa-se que as informações pessoais de usuários do ambiente virtual são usadas de maneira frequente com base em dois fatores principais: a eficiência e o controle. Isto é, a coleta e o processamento das informações relacionando-se com a otimização de serviços, bem como ao monitoramento destes, devido à necessidade de segurança. Explica-se que, ante ao desenvolvimento das tecnologias da informação, em especial o avanço da informática, esses fatores eram

comumente utilizados pelo Poder Público, no entanto, atualmente envolvem ambos, tanto os entes privados quanto o Estado (Doneda, 2019).

Contudo, diante do caso envolvendo a empresa Cambridge Analytica, emergiu, no contexto jurídico global, a preocupação a respeito da possível utilização das informações pessoais com a finalidade de manipulação dos indivíduos, seja para fins de consumo, seja para finalidades políticas. No intuito de evitar práticas abusivas da exploração econômica de informações pessoais compartilhadas em ambientes virtuais ou físicos, houve a publicação, em 2018, da Lei n. 13.709/18, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD) - instrumento normativo fundamental à defesa dos dados pessoais e à salvaguarda dos direitos personalíssimos, como a intimidade, a imagem e a honra (Tamer, 2024).

Para uma compreensão mais clara, de acordo com o artigo 5º, I da referida legislação, considera-se “dado pessoal: informação relacionada à pessoa natural identificada ou identificável” (Brasil, 2018, s.p.). Portanto, ela se aplica a toda e qualquer situação envolvendo o trânsito de informações pessoais, que recebem a denominação técnica de dados pessoais. Nota-se, que esses dados pertencem juridicamente a figura do titular de dados, razão pela qual a norma os transforma em “monarcas de seus próprios dados” - ou seja, detentores de pleno controle sobre o compartilhamento, armazenamento e tratamento de seus dados pessoais (VIGLIAR, 2022).

Constrói-se, assim, uma perspectiva em que os dados pessoais, carregam consigo uma conotação íntima, que engloba aspectos da existência de seu titular. Por esse motivo, a proteção jurídica conferida pela LGPD alcança qualquer forma de tratamento, tanto em ambientes digitais, quanto informações eventualmente preservadas em meios tradicionais. Aqui, evidencia-se que o legislador reconhece o valor humano subjacente a cada dado, reafirmando que, quando estes são transformados em informações, esta não se dissocia do direito à privacidade, especialmente diante dos desafios impostos pelo avanço da tecnologia (Lima, 2020).

Posto isto, a LGPD ergue-se como um alicerce no ordenamento jurídico brasileiro, na medida em que consagra soberania à privacidade na era da informação, garantindo, assim, a proteção dos dados pessoais dos respectivos titulares. Ilustrativamente, cita-se que o seu art. 1º determina como objetivo da legislação o amparo aos direitos fundamentais e o livre desenvolvimento da personalidade, consoante aos preceitos elencados na CRFB/1988.

Complementando este arcabouço protetivo, o artigo 2º, I, estabelece como fundamento basilar da lei o respeito à privacidade, configurando-o como verdadeiro escudo jurídico contra intromissões na esfera íntima dos titulares de dados pessoais (Brasil, 2018).

A privacidade, embora solidamente ancorada na legislação supramencionada, manifesta-se, no âmbito da LGPD, por meio de uma de suas facetas contemporâneas: a proteção de dados pessoais¹. Tal perspectiva, é decorrente da correlação entre os dados e o direito à privacidade, uma vez que os dados pessoais representam a essência existencial que cada indivíduo possui em si. Por essa razão, quando os dados identificam ou possibilitam a identificação de um indivíduo, nos termos do art. 1º da LGPD, a violação de sua integridade configura uma afronta direta à esfera privada (Tamer, 2024).

Diante desse cenário, torna-se, portanto, imprescindível reconhecer que, por meio da LGPD, o direito à privacidade passa a contar com proteção reforçada, especialmente com a definição e o reconhecimento da figura do titular de dados, conforme mencionado anteriormente. Nos termos do art. 17 da referida lei, considera-se o titular como toda pessoa natural a quem se referem os dados pessoais, já que tais informações podem pertencer a qualquer indivíduo. Assim, garante-se ao titular o controle sobre seus próprios dados, impondo-se limites claros à sua utilização, os quais devem sempre observar o regime legal vigente e respeitar os direitos fundamentais de liberdade, intimidade e, sobretudo, privacidade (Brasil, 2018).

No que tange aos direitos desses titulares de dados, mencionar-se-á que existem prerrogativas elencadas no art. 18, as quais conferem ao titular um poder acerca do tratamento de seus dados. Dentre os direitos previstos, estão a confirmação da existência de tratamento, o acesso, a correção de dados incompletos, a anonimização, a portabilidade e a revogação do consentimento. Tais prerrogativas, materializam um conceito maior: o princípio da autodeterminação informativa. Sob esta ótica, permitindo ao indivíduo não apenas ter conhecimento sobre o uso de seus dados, mas também decidir sobre sua permanência, alteração ou exclusão. Isso representa, na prática, a efetivação do direito à privacidade constitucionalmente assegurado (Brasil, 2018).

¹ Ressalta-se que a proteção de dados pessoais foi incluída, por meio da Emenda Constitucional nº 115, de 10 de fevereiro de 2022, no rol de direitos e garantias fundamentais.

Contudo, entende-se que não basta apenas a declaração formal dos direitos dos titulares dos dados pessoais para garantir, de fato, o efetivo direito à privacidade. Torna-se necessária a adoção de práticas de gerenciamento de dados pessoais no âmbito organizacional. Neste contexto, insere-se a importância da governança de dados (GD). A governança de dados é entendida como um conjunto de práticas, políticas e processos que asseguram a qualidade, a segurança, a privacidade e o uso adequado das informações dentro de uma organização. Em outras palavras, trata-se de uma prática que deve ser adotada em todos os ambientes corporativos diante das exigências da Lei Geral de Proteção de Dados, a fim de garantir os direitos assegurados aos titulares dos dados pessoais.

2 APONTAMENTOS SOBRE A GOVERNANÇA DE DADOS (GD) NO ÂMBITO DAS EMPRESAS PRIVADAS BRASILEIRAS

Diante da crescente vulnerabilidade do direito à privacidade, torna-se necessária uma análise aprofundada quanto ao papel da governança de dados (GD), além do seu viés empresarial. A GD é fruto da convergência de duas estruturas complementares: a governança corporativa e a governança de tecnologia da informação. Embora o termo “governança”, em seu sentido primordial, remeta à ideia de estratégia e controle, a sua aplicação concentra-se em princípios organizacionais, bem como na gestão de insumos essenciais à produção de informação e conhecimento nas empresas: os dados (Barbieri, 2020).

A Governança de Dados (GD) passou a ocupar uma posição de eixo central no âmbito da implementação da LGPD. Para ilustrar essa evolução Filipe Souza (2024, p. 148) esclarece através de seu entendimento que:

Com a expansão das regulamentações de privacidade, como a LGPD no Brasil e o GDPR na Europa, as empresas terão que investir ainda mais em governança de dados. A proteção da privacidade dos usuários e a integridade das informações serão prioridades estratégicas. Além disso, a convergência entre compliance e segurança cibernética se tornará uma realidade inevitável, com as organizações implementando medidas avançadas para proteger seus sistemas contra ciberataques.

Tradicionalmente, a GD era vista apenas como um conjunto de diretrizes e políticas voltadas à gestão interna do setor privado. Esse entendimento, porém, foi superado pelo contexto corporativo atual, no qual os direitos fundamentais estão constantemente expostos a riscos. Hoje, a GD é reconhecida como um programa

voltado à conformidade normativa das empresas, atuando especialmente sobre dados estratégicos e garantindo o tratamento adequado de dados pessoais, o que, por consequência, protege o direito à privacidade a partir da aplicação da LGPD (Rêgo, 2020).

Acerca desta temática, é primordial, estabelecer uma distinção entre governança e gestão de dados, embora sejam conceitos complementares. Tal premissa se explica pelo fato de que a GD é uma espécie de gestão, porém com poderes específicos voltados ao alinhamento de políticas, diretrizes e parâmetros que regulam o tratamento da informação dentro das organizações (Rêgo, 2020). Metaforicamente, a relação entre as duas sistemáticas assemelha-se à arquitetura dos poderes do Estado. A governança corresponde às funções legislativa e judiciária, à primeira função compete a edição de políticas, normas e diretrizes estruturantes; já à segunda, a fiscalização e garantia de sua estrita observância (Barbieri, 2020).

Por outro lado, a gestão corresponde ao Executivo, incumbindo-lhe a responsabilidade de realizar tais diretrizes, como coleta, processamento e armazenamento de dados. Esta corresponsabilidade entre a governança e a gerência dos dados, entre quem define as regras e quem as coloca em prática, por meio de seus gestores, como da TI, segurança, evidencia um conceito abrangente de gestão de dados. Destarte, a existência de uma pluralidade de perspectivas técnicas na tomada de decisões permite descentralizar o poder de um único setor, promovendo, por fim, maior equilíbrio e efetividade no tratamento das informações (Barbieri, 2020).

Em que pese os benefícios incontáveis trazidos pela tecnologia, ainda persistem notórias lacunas na efetiva proteção ao direito à privacidade. Nesse ínterim, importa mencionar que ao perceber o aumento de lucros e eficiência por meio da coleta de dados, o mercado organizacional passou a adotar tal prática de forma irrestrita. Como resultado, ignorando o caráter potencialmente prejudicial desses dados à privacidade e até mesmo à própria individualidade. Ante esse quadro, chega-se à conclusão de que a restrição absoluta da coleta de informações na sociedade contemporânea, representaria um verdadeiro marco para o regresso digital. No entanto, é precisamente neste dilema que a governança de dados e a LGPD emergem como faróis de equilíbrio, conciliando inovação e proteção (Tomasevicius Filho, 2021).

Vale dizer que, em sua expressão contemporânea, a GD é um conjunto de processos, políticas, padrões e princípios, cujo objetivo reside em garantir a qualidade, segurança e confiabilidade dos dados de uma organização. Além de proteger informações sensíveis, em conformidade com as leis e regulamentos aplicáveis. Paralelamente a isso, a materialização desse conceito se dá através da arquitetura de dados, definição de modelos, criação de padrões para nomeá-los, definição de processos de gerenciamento de dados, entre outros. Esses mecanismos, em sua totalidade, têm como escopo assegurar que os dados sejam consistentes e possuam uma elevada qualidade (Costa, 2023).

A posteriori, cabe destacar, que ao falar em “dados” em contexto corporativo - base estrutural da inteligência organizacional - faz-se referência à base da matéria prima, cujo valor está diretamente relacionado à sua conversão em informação. Condição esta, que confere utilidade prática aos dados, tornando-os fundamentais para a aplicação estratégica nas empresas. Isso porque, isoladamente, elementos como números e textos descontextualizados não possuem, por si só, relevância significativa. Assim, quando devidamente interpretados, os dados representam o primeiro passo para a construção da chamada sabedoria empresarial (Rêgo, 2013).

A partir desse pressuposto, a LGPD, em seu art. 50, impõe expressamente aos agentes de tratamento de dados a adoção de boas práticas e governança na efetiva aplicação da legislação (BRASIL, 2018). Tal exigência, aliada à atuação da Autoridade Nacional de Proteção de Dados (ANPD), órgão fiscalizador e regulador instituído pela própria legislação, tornam-se pilares fundamentais para o tratamento de dados pessoais. Conforme a publicação da Resolução CD/ANPD nº 20/2024, a ANPD deixa de tratar a governança de dados como mera formalidade, elevando-a à condição de elemento estrutural da atividade empresarial, para que haja consonância com os preceitos elencados na legislação (Brasil, 2024).

A ANPD é uma autarquia de natureza especial vinculada ao Ministério da Justiça e Segurança Pública, responsável por assegurar a proteção de dados pessoais no Brasil. Sua atuação é orientada pela Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018) e também pela Estatuto Digital da Criança e do Adolescente (Lei n. 15.211/2025). A organização e a composição institucional da ANPD estão disciplinadas pelo Decreto nº 10.474. Ressalta-se, ainda, que a ANPD passou a ter natureza de Agência Reguladora por força da Medida Provisória nº 1.137, que a incluiu no rol das agências previsto na Lei nº 13.848.

É imperioso expor que a ANPD se revela de suma importância para o cumprimento da LGPD, uma vez que há uma carência de órgão com poderes específicos para fiscalizar e sancionar as violações. Com efeito, a referida autoridade foi instaurada por meio de uma Medida Provisória nº 869/2018, posteriormente convertida na Lei nº 13.853/2019, a qual dispõe sobre a proteção de dados pessoais (Lima, 2021). A partir disso, a ANPD, passou a integrar, conforme disposto no art. 55-A, a administração pública federal direta, vinculada à Presidência da República. Tendo assim, competências com caráter preventivo e repressivo, que permitem a interferência quanto ao tratamento de dados pessoais, nos termos do art. 55-J da referida legislação (Brasil, 2018).

A Autoridade Nacional de Proteção de Dados (ANPD) possui, ao todo, 24 competências. Entre as principais, destacam-se o zelo pela proteção dos dados pessoais, a promoção do conhecimento sobre o tema e sobre medidas de segurança, além da elaboração de diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade. Compete-lhe, também, realizar estudos alinhados a padrões internacionais e fiscalizar o cumprimento da legislação. Em casos de descumprimento, cabe à ANPD aplicar sanções, comunicar irregularidades às autoridades competentes e analisar reclamações apresentadas por titulares de dados. Quando necessário, pode celebrar termos de compromisso para corrigir irregularidades e criar mecanismos acessíveis para que os cidadãos registrem suas reclamações (Brasil, 2018).

O contexto altamente tecnológico da sociedade atual, no qual há um grande fluxo de informações (dados) entre pessoas físicas e empresas, principalmente no ambiente virtual, cria uma realidade na qual possíveis vazamentos de informações ou utilização para finalidades diversas gera uma fragilidade na reputação das empresas. A ausência de práticas eficazes de governança expõe as empresas a riscos consideráveis, como inconsistências, fraudes e vulnerabilidades de segurança, repercutindo diretamente na proteção do direito à privacidade dos titulares de dados. No que se refere à governança de dados, ela assume papel estratégico, tanto para as empresas privadas quanto para o próprio sistema jurídico, ao assegurar a confiabilidade das informações, favorecendo decisões ágeis e compatíveis com as diretrizes institucionais. Uma gestão eficaz de dados, contribui diretamente para uma imagem sólida da empresa perante o mercado, como também

garante dados íntegros e transparentes, aos olhos da sociedade, isto é, auxiliando na efetivação das disposições normativas constantes na LGPD (Rêgo, 2013).

É importante destacar que, conforme a Lei Geral de Proteção de Dados, os dados pessoais devem estar restritos apenas a pessoas autorizadas, o que demanda a adoção de mecanismos claros de proteção (Rêgo, 2013). Entre eles, destacam-se um leque de iniciativas que as instituições empresariais devem promover para garantia de uma GD eficaz, tais como, o desenvolvimento de políticas claras de classificação entre dados pessoais ou dados sensíveis¹. Além de controle de acessos e permissões que garantem o direito à privacidade, especialmente dos dados. Incluem-se, ainda, medidas voltadas à segurança destinadas a disseminar riscos que ferem a proteção de dados pessoais, bem como uma possível reeducação dos colaboradores na conscientização da valorização da segurança dos dados (Pinto, 2024).

Sob este prisma, constata-se que a constituição de uma equipe multidisciplinar, dotada de expertise técnica e comprometida com a redução das vulnerabilidades relacionadas ao tratamento de dados pessoais, é essencial para o fortalecimento da governança de dados. Para tanto, impõe-se a necessidade de conformidade com a legislação vigente, em especial a LGPD, a qual demanda de uma atuação profissional pautada em critérios técnicos, éticos e jurídicos compatíveis com a complexidade da sociedade da informação (Pinto, 2024).

Se por um lado, a GD busca reduzir riscos relacionados à privacidade, por outro, ela torna-se essencial para o apoio dos profissionais capacitados para garantir a efetividade de suas práticas. Tal perspectiva se evidencia especialmente em situações de uso indevido de dados por pessoas não autorizadas, o que resulta em uso malicioso de informações e exposições desnecessárias dos indivíduos. Por isso há necessidade de uma união entre as áreas técnicas, compartilhando a responsabilidade com a equipe de segurança da informação ou administração de sistemas, que são responsáveis por configurar e operar as tecnologias necessárias (Rêgo, 2013).

1 A lei estabelece o dado pessoal como toda aquela “informação relacionada à pessoa natural identificada ou identificável” (BRASIL, 2018, s.p.), ou seja, dados como nome, endereço, sexo, RG e CPF. Já o dado pessoal sensível é definida pelo “dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (BRASIL, 2018, s.p.).

Na era da hiperconectividade, o ordenamento jurídico parece marchar a passos lentos, de modo que há uma morosidade no processo legislativo. Com isso, os princípios tornam-se fundamentais, pois conferem à legislação uma maleabilidade quanto à extensão de sua aplicabilidade, abarcando situações imprevistas pela proteção legislativa e jurídica (Carvalho; Pedrini, 2019). Uma vez que, na atual conjuntura, os dados extrapolam o campo da tecnologia e assumem a função de ativos organizacionais, cuja vulnerabilidade digital expõe de forma exponencial o direito à privacidade (Barbieri, 2020).

Em razão disso, a governança, traz em sua essência, a transparência e a conformidade regulatória. Com efeito, ao coletar informações de clientes, cabe à empresa não apenas garantir o armazenamento adequado, como também assegurar que haja consentimento para o uso, a fim de que os dados estejam registrados corretamente. Ademais, ela também pode auditar automaticamente as práticas de armazenamento de dados para garantir conformidade. À medida que a tecnologia avança, podemos esperar que a governança de dados se torne ainda mais inteligente e autônoma, permitindo às empresas gerenciar dados de forma eficaz, bem como extrair deles conhecimento estratégicos, em consonância com a função final do direito: harmonizar a inovação e proteger os direitos fundamentais (Aguiar; Silva, 2025).

À luz dessa realidade, propõe-se que a GD seja estruturada a partir de pilares centrais que orientem sua aplicação no contexto empresarial. O primeiro pilar é a gestão estratégica da informação, que compreende os dados como insumo indispensável para a formulação e execução de decisões organizacionais. O segundo refere-se ao patrocínio institucional, que consiste no comprometimento da administração em assegurar recursos e alinhamento com objetivos corporativos. Já o terceiro, destaca que a governança é um governo, composta por normas, papéis, responsabilidade e prestação de contas. Por este prisma, a governança não se limita a uma estrutura estática, mas sim a um processo dinâmico e adaptativo, essencial para a gestão eficiente de organizações e instituições (Rêgo, 2013).

Em meio a todos os benefícios, a implementação da GD enfrenta, por vezes, resistência interna, notadamente por parte dos funcionários, que receiam as mudanças, uma vez que não compreendem os benefícios que a governança possui. Tal dificuldade se intensifica pela carência de profissionais preparados para aplicar, de modo efetivo, as normas de proteção de dados e privacidade, decorrente da

rápida transformação digital. Essa realidade exige uma mudança cultural e institucional, orientada à valorização da privacidade como direito fundamental, além da necessidade de adotar uma autorregulamentação, tanto por parte das empresas, quanto pelo poder público, em que haja transparência quanto à finalidade e ao tempo de uso dos dados (Pinheiro, 2021).

É diante deste contexto de desafios que a GD transcende seus conhecimentos convencionais, demandando a incorporação de uma reflexão ética como pilar fundamental nas relações empresariais e os titulares de dados. Uma vez que, consoante à tradição filosófica, vê-se a definição de ética como um conjunto de princípios informais, isto é, internalizado por meio da cultura, educação ou criação, os quais constituem uma métrica quanto à conduta humana do que é certo ou errado. Dito isso, explica-se que mesmo com a presença da GD, o uso impróprio dos dados, em última análise, não decorre de um desconhecimento da legislação, mas sim de uma ausência de ética no ambiente corporativo (Barbieri, 2020).

Evidentemente, a adoção de práticas de GD contribuem para a efetivação da proteção do direito à privacidade no Brasil no âmbito das empresas privadas. Isso porque ela oferece os instrumentos para a aplicação prática da Lei Geral de Proteção de Dados no ambiente corporativo, de forma a resguardar a segurança dos dados pessoais e a privacidade das pessoas. As contribuições das práticas de Governança de Dados (GD) para garantir o direito à privacidade e a implementação da Lei Geral de Proteção de Dados no âmbito das empresas privadas brasileiras é tema abordado no próximo tópico da pesquisa.

3 AS CONTRIBUIÇÕES DAS PRÁTICAS DE GOVERNANÇA DE DADOS (GD) PARA GARANTIR O DIREITO À PRIVACIDADE E A IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NO ÂMBITO DAS EMPRESAS PRIVADAS BRASILEIRAS

A LGPD representa um marco regulatório para defesa do direito à privacidade e à proteção de dados pessoais no Brasil. A criação desta legislação advém com intuito de reforçar os objetivos e princípios a proteção de diversos direitos fundamentais já longamente consagrados como tais pela ordem jurídica brasileira, tais como a liberdade, a privacidade e o livre desenvolvimento da personalidade da pessoa natural (Vigliar, 2022).

Para tanto, menciona-se que ela se espelhou no Regulamento Geral sobre a Proteção de Dados (GDPR), da União Europeia. Isto se deve ao fato de que, devido à sua rigidez normativa deu-se ensejo a reforma legislativa no Brasil e a outros países, que mantinham um vínculo comercial com organizações ou cidadãos europeus (Gazolla, 2021). Em outras palavras, com o avanço da proteção de dados, atribuiu-se ao sistema normativo uma função de natureza dupla: proteger os titulares de dados e, simultaneamente, fomentar o livre fluxo de informações entre países. Tendo em vista que as legislações estrangeiras, impõem restrições à troca livre de informações e dados com outras nações que não tenham legislação específica e equivalente. Portanto, exigiu-se uma harmonização regulatória como condição para o intercâmbio seguro de dados (Dresch; Menke, 2021).

De maneira complementar, a herança europeia visualiza-se especialmente por meio do art. 6º da Lei Geral de Proteção de Dados, que consagra princípios basilares para o tratamento de dados pessoais no ordenamento jurídico brasileiro. Dentre eles, destacam-se a finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, não discriminação, bem como a responsabilização e a prestação de contas. Por último, ressalta-se, ainda, o princípio da boa-fé, que permeia todas as relações e negócios jurídicos que envolvam o tratamento de dados pessoais (Gazolla, 2021).

Dito isso, cumpre destacar também que, diante da historicidade da proteção de dados, tal legislação surge como um avanço em relação ao esboço da Lei nº 12.965/2014, reconhecida como Marco Civil da Internet. Essa legislação centrava-se, principalmente, no consentimento de dados manipuláveis, esclarecendo sua essência, no que diz respeito à autorização expressa dos usuários e às limitações dos provedores de serviço (Alves; Peixoto; Rosa, 2021). Entretanto, havia ainda, uma insuficiência quanto à definição de critérios que esclarecesse a questão de dados pessoais (Carvalho; Perini, 2019).

Para isto, Laura Mendes (2014, p. 32), conceitua a proteção de dados pessoais “[...] como uma possibilidade de tutelar a personalidade do indivíduo, contra os potenciais riscos a serem causados pelo tratamento de dados pessoais”. Frente a essa nova realidade, observa-se que, no contexto do Big Data, expressão que significa “grandes dados”, mas que, se refere também ao processamento e armazenamento de dados em grande escala. Denota-se uma urgência quanto à criação de uma lei que harmonize a proteção da individualidade e privacidade das

peças com a livre iniciativa comercial e de comunicação (Teixeira; Guerreiro, 2022).

Assim sendo, a LGPD se insere como uma resposta legislativa à crescente preocupação com a proteção de dados, uma das vertentes do direito à privacidade. Perante esse cenário normativo, a lei estabelece parâmetros claros quanto ao tratamento de dados pessoais, nas relações entre usuários e os setores públicos e/ou privados. Esta, assegura também, direitos aos titulares de dados, conferindo-lhe a necessidade de consentir a coleta e o uso dos dados pessoais, além da possibilidade de visualizar, corrigir e excluir tais informações, sempre que houver necessidade, consoante ao art. 18 da norma em questão (Brasil, 2018).

No que se refere às definições basilares de cada um dos princípios, observa-se que o princípio da finalidade delimita os objetivos do tratamento dos dados, enquanto a adequação assegura que sua utilização esteja compatível com tais finalidades. De igual modo, o princípio da necessidade impõe que sejam coletadas apenas as informações estritamente indispensáveis, em harmonia com o livre acesso, que garante ao titular a possibilidade de consultar integralmente seus dados. Assim, mantendo a transparência, a qual exige clareza, precisão e acessibilidade. Sobretudo, assegura-se a qualidade dos dados, para que permaneçam corretos e atualizados, conforme a finalidade e a necessidade do tratamento (Soler, 2022).

Adentrando na seara do princípio da segurança, destaca-se que ela desempenha papel central, a medida em que protege os dados contra condutas ilícitas e acessos não autorizados. Outrossim, cita-se a prevenção, atuando como elemento estratégico na adoção de medidas antecipatórias que reduzem significativamente a probabilidade de danos. Se, por um lado, essas práticas visam resguardar direitos, por outro, o princípio da não discriminação impõe que o tratamento de dados não seja utilizado para finalidades ilícitas ou discriminatórias, como a exclusão de candidatos por gênero ou orientação sexual. É neste aspecto que se insere os princípios de responsabilização e a prestação de contas, garantindo o cumprimento efetivo das obrigações legais e a proteção do direito à privacidade. É justamente na seara da responsabilização e da prestação de contas que a Governança de Dados se destaca como prática de implementação da LGPD (Soler, 2022).

Têm-se a GD nas empresas como forma de promover a prestação de contas aos titulares de dados, de acordo com Marcus Pinto (2024, p. 113) mediante:

[...] relatórios regulares que detalhem as práticas de gestão de dados, os progressos alcançados e os desafios enfrentados, demonstrando o compromisso da organização com a transparência e a prestação de contas.

Partindo dessa premissa, compreende-se que a GD não se limita a cumprir um papel meramente normativo, mas configura-se como vetor de uma transformação estrutural dentro das organizações. Para além da redução de riscos e da padronização de processos de coleta, armazenamento e gerenciamento, a GD projeta-se como um modelo de gestão inteligente que contribui com a implementação da LGPD, ao passo que, promove uma melhora na qualidade dos dados e reduz possíveis riscos de violações. Isso inclui a integração transversal entre setores, possibilitando o compartilhamento de informações dentro da organização de maneira segura e adequada. Ao adotar tais práticas, a organização fomenta a inovação e o desenvolvimento econômico, com efeito, reduzindo custos operacionais e evitando desperdícios (Pinto, 2024).

Em decorrência disso, emerge o princípio da autodeterminação informativa, que se consagra como a própria alma da privacidade. Esse princípio, conforme estipulado no art. 2, II, da LGPD, pressupõe que o direito atua como um guardião da pessoa humana, visto que proporciona instrumentos que capacitam o indivíduo a compreender, deliberar e agir de maneira consciente sobre o tratamento de seus dados. Em outras palavras, ao mesmo tempo em que busca resguardar o indivíduo, esse fundamento reconhece sua inserção em uma sociedade que se estimula também por meio da economia. Contudo, tal proteção não é absoluta, pois coexistem limites individuais e coletivos, o que propicia uma considerável margem interpretativa para situações análogas, sempre com o intuito de equilibrar os interesses de ambas as partes (Garcia, 2020).

De igual modo, ganha destaque na regulamentação brasileira a análise do consentimento, consoante ao disposto no art. 5º, XII da LGPD. Para ter validade, essa manifestação de vontade deve ser prévia, livre, informada e específica. Entende-se o requisito prévio, quando a pessoa deve ter pleno poder decisório, sem nenhuma interferência, isenta de qualquer sanção ou obrigação imposta pelos controladores de tratamento de dados. Ainda, esta é livre quando exige que a escolha não seja destituída de coação física ou moral capaz de influenciar a

declaração de vontade. Em um segundo plano, os atributos de específico e informado prescrevem que o titular deve possuir ciência clara de conhecimento acerca dos dados que são coletados, da finalidade do tratamento, bem como de seus riscos, consequências ou eventuais implicações. Permitindo assim, ao titular de dados uma precisa avaliação da dimensão de sua decisão acerca da disposição de seus dados pessoais (Gazzola, 2021).

Aliado a isto, revela-se indispensável a atuação dos agentes de tratamento de dados pessoais. Isso inclui o controlador, o operador e o encarregado, os quais possuem obrigações específicas e claramente definidas nos arts. 37 a 41 da referida legislação (BRASIL, 2018). Para isto, há de se considerar que, o encarregado para a LGPD, torna-se uma figura essencial, pois deve possuir um conjunto de habilidades multidisciplinares, abrangendo conhecimentos técnicos, como cibersegurança e, se possível, a governança de dados (Garrido, 2023). Ao nomear um encarregado de dados, sua função consiste em atuar como um elo entre a organização, a ANPD e os titulares de dados, tendo como escopo assegurar que as empresas executem medidas preventivas e correção rápida de eventuais falhas na gestão de dados (Souza, 2024).

Conforme estabelece a legislação, explicar-se-á qual o papel do controlador - pessoa natural ou jurídica, de direito público ou privado - o qual, é o centro das decisões. Cabe a ele, decidir o que será realizado com os dados, bem como qualquer decisão que tenha a ver com essa temática (Brasil, 2018). Em posição hierárquica distinta, surge o operador, atua de maneira subordinada, realizando o tratamento de dados pessoais em nome do controlador, geralmente mediante a confecção de um contrato de prestação de serviços, uma parceria ou sociedade por conta de participação que discipline essa relação (Dresch; Menke, 2021).

Para a GD, esses papéis revelam-se cruciais em prol da segurança e da integridade das informações. Ambos, têm como propósito preservar a saúde organizacional, mas sob perspectivas distintas. O encarregado dos dados, dedica-se à conformidade com os regulamentos aplicáveis, por meio do processamento correto dos dados. Já o diretor de segurança da informação, volta-se para a defesa da empresa, contra-ataques externos, identificando vulnerabilidades e mitigando tais riscos através da implementação de medidas. Em outras palavras, enquanto o encarregado protege os titulares de dados contra abusos da empresa, o diretor protege a empresa contra ameaças externas (Olesen-Bagneux, 2023).

É importante destacar que a governança de dados, em sua literalidade, caracteriza-se como um conjunto de práticas, políticas e normas que administram os dados, de forma eficaz, perpassando-se pela qualidade até a segurança dos dados (Aguilar; Silva, 2025). Nesse ínterim, Patricia Garrido (2023, p. 172), enfatiza que “a instituição de medidas e regras de boas práticas e de governança é essencial para que todos os requisitos necessários à proteção dos dados pessoais sejam efetivados.” Tal premissa, justifica a necessidade de adotar-se programas estruturados de governança de dados, com respaldo nos arts. 50 e 51 da LGPD.

A esse respeito, têm-se a emblemática das violações aos dados pessoais juridicamente protegidos, eventos que não transgridem apenas a esfera privada, mas que se revelam capazes de ocasionar danos sociais de uma imensurável magnitude. Diante desse panorama, convém sublinhar que o centro da questão reside no duplo valor atribuído aos dados, que por um lado, são ativos de utilidade e valor econômico de mercado, e por outro, são expressões de personalidade. Consequentemente, o uso inadequado dessas informações acarreta sérias consequências para as pessoas, especialmente considerando que, historicamente, a escassez de repercussões em casos de mau uso de dados gerou uma percepção de confiança que incentivou a coletividade a compartilhar suas informações de forma voluntária (Tomasevicius Filho, 2021).

Foi também dentro deste quadro que se deu relevância a necessidade de implementar a governança de dados, que se conceitua como uma prática que busca assegurar qualidade e segurança das informações dentro das empresas. Trata-se de um instrumento que deve ser utilizado de forma integrada a outras áreas de gestão, como a gestão de processos e a gestão de riscos. De modo que se possa atingir seus objetivos estratégicos e fortalecer sua competitividade no mercado. Nesse sentido, cita-se a gestão de processos - como uma prática que aprimora processos de atividades internas, abrangendo desde a identificação dos processos existentes até sua análise e melhoria contínua. Por sua vez, a gestão de riscos se destina à identificação, avaliação e tratamento dos riscos que permeiam os processos e operações empresariais, tais como, riscos financeiros, operacionais, regulatórios ou reputacionais (Costa, 2023).

A título ilustrativo, têm-se as organizações que atuam no comércio eletrônico, através de vendas on-line, nas quais o uso de dados revela-se um elemento indispensável para realização da venda. Dito isso, é imperiosa a delimitação das

informações necessárias - como o nome do consumidor, endereço de entrega e os dados de pagamento - evitando, assim, a coleta abusiva ou desnecessária. No entanto, para garantir a devida proteção de dados e eficiência, é necessária integração da governança de dados com a gestão de processos e riscos, bem como uma equipe qualificada e com o uso de ferramentas adequadas, que permitam a realização de análises precisas e a implementação de medidas efetivas (Costa, 2023).

À vista disso, revela-se inafastável admitir que o tratamento de dados seja conduzido de forma responsável e criteriosa. Consoante previsão da LGPD, o que resulta na extinção dos dados quando verificado o exaurimento da finalidade para a qual foram coletados ou, ainda, quando tais informações se revelarem desnecessárias ou desproporcionais ao fim legitimamente perseguido (Gazolla, 2021). Destarte, constata-se que a GD, incorporada pela LGPD à condição de parâmetro normativo, extrapola a esfera técnica e assume função jurídico-organizacional, vinculando assim, os controladores e operadores à responsabilidade de tutelar o direito à privacidade com as exigências legais inerentes ao tratamento de dados (Brasil, 2018).

Importa assinalar que a proteção dos dados deve estar intrinsecamente alinhada aos objetivos organizacionais, erguendo-se como um diferencial competitivo. Nesse sentido, as empresas que demonstram comprometimento com a privacidade e segurança conquistam maior confiança de clientes e parceiros, consolidando sua reputação e ampliando oportunidades de negócios (Souza, 2024). Depreende-se que a governança, especialmente a de dados, é um sinônimo de organização, podendo comparar-se ao objetivo de uma biblioteca, em que os livros são separados de forma eficiente, para que possam ser encontrados com facilidade. Isto é, ela permite que os dados estejam organizados, seguros e prontos para serem usados quando necessário (Aguiar; Silva, 2025).

Em suma, observa-se a importância de manter um processo contínuo de governança de dados nas empresas, sobretudo no que tange à confiabilidade e segurança dos dados, ao longo do tempo, ou seja, prevenindo acessos não autorizados, roubos e vazamentos. Ainda que a LGPD estabeleça diretrizes que resguardam os dados pessoais, a governança delineia-se de forma autônoma para garantir a segurança e privacidade das informações dentro das empresas (Aguiar; Silva, 2025).

Em um cenário no qual as informações se tornam tão valiosas no âmbito empresarial, é de suma importância que sejam adotadas práticas de Governança de Dados a fim de assegurar os direitos dos titulares dos dados pessoais nos termos da Lei Geral de Proteção de Dados no Brasil. Nesse sentido, percebe-se a imprescindibilidade do diálogo inter e multidisciplinar entre a área jurídica e áreas como a tecnologia de informação ou administração de empresas, a fim de que sejam viabilizadas práticas consistentes de GD, que atendam à legislação.

CONSIDERAÇÕES FINAIS

A governança de dados reafirma-se importante para sociedade contemporânea, especialmente, para a efetiva proteção do direito fundamental à privacidade no âmbito das empresas privadas. Isto se deve ao fato de que, na atualidade, os dados assumiram posição central e valor exponencial, sendo considerados ativos estratégicos capazes de gerar significativos ganhos econômicos. Ressalte-se, contudo, que a utilidade dos dados transcende a sua importância no mercado, uma vez que, é imperioso reconhecê-los como base fundamental para o desenvolvimento da pessoa humana, razão pela qual se exige adequada tutela jurídica. Com isso, tal prática torna-se uma violação não apenas à legislação específica, mas sobretudo aos direitos constitucionais inerentes à pessoa humana.

Aqui, faz-se necessária menção à Carta Magna de 1988, que estabelece em seu art. 5º, X, a inviolabilidade à intimidade, vida privada, honra e a imagem. Embora promulgada antes do advento da internet e da sociedade da informação, essa norma resguarda o direito à privacidade como uma extensão da dignidade humana conceituando-o através de suas facetas. Por sua vez, para garantir sua efetividade, é imprescindível complementar esse arcabouço jurídico com instrumentos organizacionais, dentre os quais se insere a governança de dados. A privacidade, consolida-se assim, um valor intrínseco à arquitetura das organizações, exigindo uma harmonização entre inovações tecnológicas e os direitos dos titulares de dados. Essa conciliação assegura que os avanços tecnológicos respeitem os limites éticos e legais, promovendo confiança e segurança no uso de dados pessoais.

Ao longo desta pesquisa evidencia-se que a simples existência de um marco regulatório robusto como a Lei Geral de Proteção de Dados (LGPD), embora seja um avanço expressivo no ordenamento jurídico brasileiro, mostra-se insuficiente por si só para garantir a efetiva proteção dos dados pessoais e, por consequência, da privacidade dos titulares. Compreende-se, hoje, os dados pessoais como uma manifestação concreta do direito à privacidade, sendo essenciais ao pleno desenvolvimento da personalidade humana, o que os torna, portanto, constantemente vulneráveis às práticas do ambiente corporativo. Diante deste cenário, têm-se aqui, a GD como uma limitação à atuação das empresas privadas, no que concerne ao uso dos dados pessoais, orientando-as de dentro para fora.

Acrescenta-se que a referida legislação, ao regulamentar o tratamento de dados pessoais, instituiu formalmente a figura do titular. Trata-se de toda pessoa natural a quem se referem os dados e que possa ser por eles identificada. A partir do reconhecimento desse agente, surgiram prerrogativas legais intrínsecas à sua condição de titular, como a garantia de acesso facilitado, retificação, portabilidade e eliminação de suas informações, fomentando, em última instância, o exercício da autodeterminação informativa. Este, consubstancia-se no poder de controlar a coleta, o uso, o armazenamento e o compartilhamento de seus dados pessoais, assegurando a observância dos princípios estruturantes que regem as atividades de tratamento. Não obstante, verifica-se que, na prática, diversas organizações ainda descumprem tais preceitos de forma integral, ocasionando violações reiteradas aos direitos dos titulares.

Para exemplificar a importância de sistemas de governança na prevenção dessas violações, abordou-se um caso com extrema significância, em que milhões de dados de usuários foram coletados sem o consentimento prévio. Em resposta à este panorama, visualiza-se o papel da GD como sistema de autogestão que constrói um ambiente corporativo mais ético no tratamento de dados pessoais. Noutros termos, configura-se como um pilar estratégico que concilia os interesses empresariais com a proteção do direito à privacidade, resguardando os preceitos elencados na LGPD e na CF/88. Com efeito, visualiza-se sua efetividade na prática ao estabelecer políticas claras, controle de acesso, medidas para mitigar violações, entre outras diretrizes.

Dito isso, cabe assinalar que a aplicação dos princípios basilares elencados na LGPD, tem por escopo assegurar uma implementação adequada de governança.

Citam-se eles, nomeadamente como a finalidade, necessidade, livre acesso, responsabilidade, segurança, transparência, entre outros. Estes princípios transcendem a mera normatividade, fazendo com que a GD se projete como uma prática institucional que atua em harmonia com a liberdade empresarial. Para além disso, a clara definição de papéis e responsabilidades compartilhadas de forma transversal, reduz a margem de equívocos e amplia a confiabilidade do sistema, visto que submete as decisões ao crivo plural de diferentes colaboradores.

Desse processo, instaura-se um círculo virtuoso de conscientização progressiva, no qual os indivíduos que atuam nas organizações, assimilam o tratamento adequado dos dados com uma cultura organizacional orientada pela ética, comprometida com o ordenamento jurídico brasileiro. Cumpre salientar, que a governança encarna em si, uma função preventiva, voltada à busca disseminar possíveis riscos de violações. Atuação esta, reforçada pela Autoridade Nacional de Proteção de Dados (ANPD), a qual torna-se determinante na fiscalização, regulamentação e orientação das práticas corporativas. Conforme estabelece a Resolução CD/ANPD nº 20/2024, que determina à ANPD o desenvolvimento de uma política interna de governança em proteção de dados e privacidade. Promovendo assim, não apenas a conformidade normativa, mas também uma gestão ativa e contínua de dados nas organizações.

Em síntese, a pesquisa demonstra que a efetiva proteção do direito à privacidade no âmbito corporativo está intrinsecamente ligada à adoção de práticas estruturadas de governança de dados. Essa estrutura possibilita o uso estratégico e responsável das informações evitando retrocessos históricos no manejo de dados pessoais, especialmente em uma sociedade em que tais informações possuem valor exponencial e permeiam todas as interações cotidianas. Neste sentido, a GD funciona, portanto, como um vetor de inovação responsável, equilibrando o aproveitamento econômico e estratégico dos dados com a proteção dos titulares, consolidando ambientes corporativos seguros, éticos e alinhados aos princípios constitucionais.

Por fim, conclui-se que é necessária uma conjugação entre um marco legal, como a LGPD, e a implementação contínua de práticas de governança de dados. Recomenda-se, portanto, que as empresas invistam em políticas, processos e tecnologias voltadas à gestão ética das informações, promovendo educação e conscientização de seus colaboradores e assegurando transparência e segurança

aos titulares de dados. A consolidação desses esforços não apenas fortalece a conformidade legal, mas também contribui para a construção de uma cultura corporativa responsável, capaz de sustentar o desenvolvimento sustentável da sociedade digital.

REFERÊNCIAS

AGUIAR, Nelson Augusto Oliveira de; SILVA, Elias Eduardo Bernardo da. **Governança de dados de forma inteligente e segura**. São Paulo: Ed. dos Autores, 2025.

ALVES, David; PEIXOTO, Mario; ROSA, Thiago. **Internet das Coisas (IoT): Segurança e privacidade de dados pessoais**. Rio de Janeiro: Editora Alta Books, 2021.

BARBIERI, Carlos. **Governança de dados**. Rio de Janeiro: Editora Alta Books, 2020.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

BLUM, Rita Peixoto Ferreira. **O Direito à Privacidade e a Proteção dos Dados do Consumidor**. 2 ed. São Paulo: Grupo Almedina, 2022.

BRANCO, Paulo Gustavo G.; MENDES, Gilmar. **Curso de Direito Constitucional (Série IDP)**. 19 ed. Rio de Janeiro: Saraiva Jur, 2024.

BRASIL. Autoridade Nacional de Proteção de Dados. **Resolução CD/ANPD nº 20, de 20 de fevereiro de 2024**. Institui a Política Interna de Proteção de Dados Pessoais da Autoridade Nacional de Proteção de Dados - ANPD. Diário Oficial da União: seção 1, Brasília, DF, 07 out. 2024. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-20-de-3-de-outubro-de-2024-588653756>. Acesso em: 01. mai. 2025.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso em: 26. mar. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 03 abr. 2025.

CARVALHO, Gisele Primo; PEDRINI, Tainá Fernanda. Direito à Privacidade na Lei Geral de Proteção de Dados Pessoais. **Revista da ESMESC**, v. 26, n.32, p- 363-

382. Disponível em: <https://revista.esmesc.org.br/re/article/view/217> Acesso em: 11 abr. 2025.

COSTA, André. Governança de Dados - **Como transformar a gestão de dados em um diferencial competitivo**. [S.l.]: André Costa, 2023.

DONEDA, Danilo. **Privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. São Paulo: Revista dos Tribunais. 2 ed. 2019.

DRESCH, Rafael de Freitas Valle; MENKE, Fabiano. **Lei geral de proteção de dados**: aspectos relevantes. São Paulo: Editora Foco, 2021.

TOMASEVICIUS FILHO, Eduardo. **A Lei Geral de Proteção de Dados Brasileira**. São Paulo: Grupo Almedina, 2021.

FORNASIER, Mateus de Oliveira. Cambridge Analytica: escândalo, legado e possíveis futuros para a democracia. **Revista do Departamento de Ciências Jurídicas e Sociais da Unijuí**. Editora Unijuí – Ano XXIX – n. 53 – jan./jun. 2020. Disponível em: https://www.researchgate.net/profile/Mateus-Fornasier/publication/341650745_CAMBRIDGE_ANALYTICA_Escandalo_Legado_e_Possiveis_Futuros_para_a_Democracia/links/5ecd26904585152945106119/CAMBRIDGE-ANALYTICA-Escandalo-Legado-e-Possiveis-Futuros-para-a-Democracia.pdf. Acesso em: 11 ago. 2025.

GARCIA, Lara Rocha. **Lei Geral de Proteção de Dados (LGPD)**: Guia de implantação. São Paulo: Editora Blucher, 2020.

GARRIDO, Patricia Peck. **Proteção de Dados Pessoais**: Comentários À Lei N 13709/2018 (Lgpd). 4 ed. Rio de Janeiro: Saraiva Jur, 2023.

GAZOLLA, Frederico. **Direito à privacidade na sociedade da informação e o pós-panoptismo**: uma análise sobre privacidade e regulação da proteção de dados pessoais. São Paulo: Editora Dialética, 2021.

MENDES, Laura. **Série IDP - Linha de pesquisa acadêmica - Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental, 1 ed. Rio de Janeiro: Saraiva, 2014.

OLESEN-BAGNEUX, Ole. **O Catálogo de Dados Corporativo**: Aprimore a descoberta de dados, garanta a governança de dados e impulse a inovação. São Paulo: Novatec Editora, 2023.

PINHEIRO, Patrícia Peck. **Direito Digital**. 7 ed. Rio de Janeiro: Saraiva Jur, 2021.
PINTO, Marcus Vinicius. **Fundamentos da Governança de Dados**. 1 ed. [S.l.]: Independently Published, 2024.

RÊGO, Bergson Lopes. **Gestão e Governança de Dados**: Promovendo dados como ativo de valor nas empresas. Rio de Janeiro: Brasport, 2013.

RÊGO, Bergson Lopes. **Simplificando a Governança de Dados**: governe os dados de forma objetiva e inovadora. Rio de Janeiro: Brasport, 2020.

SOLER, Fernanda Galera. **Proteção de Dados**: reflexões práticas e rápidas sobre a LGPD. Rio de Janeiro: Expressa, 2022.

SOUZA, Filipe Elienai Santos. **Aspectos Práticos de Compliance Empresarial – Como Implementar Boas Práticas de Governança**. 1. ed. [S.l.]: Filipe Elienai Santos Souza, 2024.

TAMER, Maurício. **Manual de Direito da Proteção de Dados Pessoais**. 1 ed. Rio de Janeiro: SRV, 2024.

TAVARES, André R. **Curso de Direito Constitucional**. 22. ed. Rio de Janeiro: Saraiva Jur, 2024.

TEIXEIRA, Tarcísio; GUERREIRO, Ruth M. **Lei Geral de Proteção de Dados Pessoais**: Comentada Artigo Por Artigo. 4. ed. Rio de Janeiro: Saraiva Jur, 2022.

VÉLIZ, Carissa. **Privacidade é poder**: por que e como você deveria retomar o controle de seus dados. 1 ed. São Paulo: Editora Contracorrente, 2021.