GOVERNANÇA DE DADOS EM *STARTUPS*: UMA ANÁLISE DE *FRAMEWORKS* PARA ESTAR EM COMPLIANCE COM A LGPD

Data Governance in Startups: An Analysis of Frameworks for LGPD Compliance

Natacia Regina Fidelis Marinho Ferraz[1]
Universidade Federal do Paraná

Jose Simão de De Paula Pinto[2]
Universidade Federal do Paraná

DOI: https://doi.org//10.62140/NFJP2172024

Sumário: 1. Introdução; 2. Revisão de Literatura; 2.1. Evolução da Proteção de Dados Pessoais e o Surgimento das Leis de Privacidade; 2.2. Governança de Dados 2.3. *Frameworks* de Governança de Dados; 3. *Startups* e os Desafios da Conformidade; 4. Discussão dos Resultados; 5. Conclusão; Referências Bibliográficas.

Resumo: O presente artigo apresenta os desafios enfrentados pelas *startups* brasileiras na conformidade com a Lei Geral de Proteção de Dados (LGPD) e propõe a análise de diferentes *frameworks* de governança de dados para identificar soluções adaptadas a essas empresas. A revisão de literatura destaca a importância da governança de dados na proteção da privacidade e na eficiência operacional. A pesquisa analisou *frameworks* consolidados, como DAMA-DMBOK, COBIT, GDPR, e o *Data Governance Institute Framework* (DGI), identificando suas forças, lacunas e adaptabilidade ao contexto das *startups*. A análise revelou que nenhum *framework* é suficiente por si só para atender às necessidades específicas dessas empresas, exigindo a integração de diferentes elementos para uma governança eficaz. O estudo propõe um modelo flexível de governança de dados que permita a conformidade com a LGPD sem comprometer a agilidade e inovação características das *startups*. Os resultados ressaltam a necessidade de adaptar os *frameworks* às particularidades das *startups*, incluindo práticas de conscientização, treinamento contínuo e automação de processos. Espera-se que esta pesquisa contribua para o debate acadêmico e prático, oferecendo orientações que auxiliem as *startups* a alcançar a conformidade com a LGPD e fortalecer sua proteção de dados pessoais.
Palavras-chave: Governança de Dados; Startups; LGPD; Framework; Compliance..

Abstract: The present article presents the challenges faced by Brazilian startups in complying with the General Data Protection Law (LGPD) and proposes an analysis of different data governance frameworks to identify solutions tailored to these companies. The literature review highlights the importance of data governance in privacy protection and operational

[1] Advogada. Mestranda no Programa de Pós-Graduação em Gestão da Informação da Universidade Federal do Paraná. E-mail: nataciaferraz@ufpr.br
[2] Doutor em Medicina, com foco em Informática Aplicada ao ensino e Pesquisa em Cirurgia e professor no Departamento de Ciências Sociais Aplicadas da Universidade Federal de Paraná. E-mail: simao@ufpr.br

efficiency. The research analyzed consolidated frameworks such as DAMA-DMBOK, COBIT, GDPR, and the Data Governance Institute Framework (DGI), identifying their strengths, gaps, and adaptability to the startup context. The analysis revealed that no single framework is sufficient to meet the specific needs of these companies, requiring the integration of different elements for effective governance. The study proposes a flexible data governance model that allows for LGPD compliance without compromising the agility and innovation characteristic of startups. The results emphasize the need to adapt the frameworks to the unique characteristics of startups, including awareness practices, continuous training, and process automation. It is hoped that this research will contribute to both academic and practical debates, offering guidelines that help startups achieve LGPD compliance and strengthen their data protection practices.
Keywords: Data Governance; Startups; LGPD; Framework; Compliance.

1. INTRODUÇÃO

A Lei Geral de Proteção de Dados (LGPD), em vigor desde 2018, impõe a todas as empresas, independentemente do seu porte, a obrigatoriedade de estar em conformidade com suas normas de privacidade. As sanções para o descumprimento variam desde advertências e multas calculadas sobre o faturamento da empresa até a eliminação e perda de todos os dados de terceiros em sua posse. Um dos requisitos essenciais para a conformidade é a nomeação de um Encarregado de Dados (*Data Protection Officer* - DPO), responsável por monitorar a implementação das regras e políticas de privacidade de dados dentro da organização. Contudo, *startups* e pequenas empresas enfrentam desafios significativos para cumprir essas exigências, devido ao seu limitado número de colaboradores e aos elevados custos associados à adequação à LGPD, que frequentemente requer a contratação de uma equipe multidisciplinar com conhecimentos específicos, como advogados e especialistas em tecnologia da informação (Mello Filho *et al.*,, 2023). As *startups*, em particular, enfrentam desafios únicos na adequação à LGPD, uma vez que requerem uma mudança cultural significativa para adotar práticas éticas e seguras no tratamento de dados (Aragão *et al.*,, 2020). Portanto, a adoção de *frameworks* e metodologias adequadas pode ajudar a promover uma cultura organizacional mais focada na conformidade e na proteção dos dados pessoais, viabilizando uma implementação eficiente da governança de dados.

No que concerne a governança de dados, a literatura atual, tanto nacional quanto internacional, destaca a importância da gestão de dados e da conformidade com as regulamentações de privacidade para garantir a proteção dos dados pessoais, assim sugerem a utilização de *frameworks* para que as empresas possam gerir seus dados. Os *frameworks* de governança de dados são fundamentais para alinhar a tecnologia da informação com as estratégias de negócios, além de apoiar processos de tomada de decisão nas empresas (Faria *et al.*,, 2018). Esses modelos oferecem diretrizes para estruturar atividades de gerenciamento de dados, mas é comum que precisem ser ajustados para atender às complexidades específicas

de cada instituição. No Brasil, há um interesse crescente das organizações em implementar processos de governança de dados para melhorar a qualidade das informações e embasar decisões estratégicas (Castro *et al.*, 2022). No entanto, pequenas empresas e *startups* costumam enfrentar obstáculos significativos, como recursos financeiros limitados e falta de profissionais especializados, tornando a implementação de um programa robusto de governança e segurança de dados um grande desafio (De Paula *et al.*, 2024).

A implementação da Lei Geral de Proteção de Dados no Brasil traz ainda mais desafios para as *startups* e outras organizações na gestão e proteção de dados pessoais. Diversos *frameworks* têm sido propostos para facilitar a conformidade com a LGPD e apoiar as organizações nesse processo. Um dos *frameworks* baseados na metodologia BEST, por exemplo, foi desenvolvido para orientar profissionais de tecnologia da informação e comunicação (TIC) na adaptação aos requisitos legais impostos pela LGPD (Castro *et al.*, 2022). Além disso, há modelos conceituais inspirados no COBIT, que fornecem diretrizes para áreas tecnológicas, destacando a importância da governança de dados em ambientes de desenvolvimento ágil (Teodoro *et al.*, 2023). O padrão ISO 27701 também foi analisado como uma possível estrutura para apoiar a conformidade com a LGPD, embora apresente algumas limitações em termos de aplicabilidade em organizações menores (De Paula *et al.*, 2024). Outras abordagens incluem a aplicação dos princípios de privacidade por design durante o desenvolvimento de software, enfatizando a importância de incorporar práticas de proteção de dados desde a concepção do produto (De Paula *et al.*, 2024). Adicionalmente, métodos ágeis, como a metodologia Scrum, têm sido sugeridos para facilitar a implementação da LGPD em empresas que trabalham com ciclos de desenvolvimento mais curtos (Melo Filho *et al.*, 2023).

O problema central desta pesquisa é a falta de *frameworks* de governança de dados adaptados às particularidades de *startups*, pois embora existam modelos consolidados, eles muitas vezes não consideram as restrições de recursos e a necessidade de flexibilidade que caracterizam essas empresas, logo, foi identificada uma lacuna significativa na literatura acerca da utilização, adaptabilidade ou modificação desses *frameworks* para atender às necessidades específicas das *startups*, mantendo-se em conformidade com a LGPD, visto que, visando a proteção dos dados, a legislação requer a implantação de inúmeras medidas para serem cumpridas, no entanto, não há um modelo que possibilite que estas empresas atendam as referidas medidas sem que isso represente um custo expressivo para a regularização, e assim um desafio muitas vezes insuperável.

O objetivo principal da presente pesquisa é identificar e descrever os *frameworks* de governança de dados existentes a fim de adaptá-los às necessidades de *startups*, fornecendo um panorama geral dos modelos atuais, relacionando suas principais características, vantagens e limitações quando aplicados ao contexto de *startups*. Além disso, o estudo também tem como objetivo investigar as implicações legais e operacionais da implementação da LGPD em ambientes empresariais dinâmicos e em constante evolução, como o das *startups*

Como método científico, a presente pesquisa adota a metodológica qualitativa, baseada na revisão de literatura sobre *frameworks* de governança de dados, com um enfoque específico em artigos científicos que abordam a conformidade com a Lei Geral de Proteção de Dados, dirigindo a pesquisa em duas fases, sendo a primeira fase, uma revisão da literatura sobre governança de dados, legislação de proteção de dados e os desafios enfrentados por *startups*.

Com base na análise da literatura, foram elaboradas proposições práticas para auxiliar as *startups* na implementação eficaz de uma governança de dados em conformidade com a regulamentação de privacidade de dados, em especial a possibilidade de proposição de um *framework* flexível e adaptável para simplificar a conformidade com a legislação de proteção de dados, levando em consideração as particularidades e limitações de recursos das *startups*. O estudo busca compreender os desafios dessas empresas e adaptar os frameworks disponíveis às suas necessidades específicas. As conclusões incluem identificar os frameworks mais adequados para o contexto das startups e analisar as limitações e desafios na adaptação desses modelos, ressaltando as dificuldades práticas e a complexidade de implementar um programa de proteção de dados.

Portanto, verifica-se que estas modalidades de empresas encontrarão desafios para estruturar e aplicar a governança de dados e consequentemente implementas normas e diretrizes para estar em *compliance* com a LGPD, e, portanto, seguir as diretrizes de um programa de governança para a gestão dos dados.

2. REVISÃO DA LITERATURA

A governança de dados tornou-se um pilar essencial para as empresas que desejam não apenas estar em conformidade com regulamentações como a Lei Geral de Proteção de Dados, mas também otimizar o uso de informações para tomadas de decisões estratégicas. Nesse contexto, as *startups*, com suas características de flexibilidade e inovação, enfrentam desafios específicos ao tentar implementar práticas robustas de governança de dados,

especialmente quando comparadas a empresas mais consolidadas e com maior disponibilidade de recursos.

2.1. EVOLUÇÃO DA PROTEÇÃO DE DADOS PESSOAIS E O SURGIMENTO DAS LEIS DE PRIVACIDADE

De acordo com Mendes (2014), a proteção à privacidade teve início com uma visão individualista, porém, com as transformações tecnológicas ocorridas ao longo do século XX, o papel do Estado mudou, ampliando o significado e o alcance do direito à privacidade. Na era atual, a privacidade é marcada pela rápida evolução tecnológica e pela intensa troca de informações, os dados pessoais se tornaram um ativo valioso. Blank (2013) destaca que, nesse cenário, a informação assume uma natureza comercial, podendo ser utilizada para negociações e decisões estratégicas, logo, devido a essa nova dinâmica diretamente relacionada à coleta, gerenciamento e aplicação de dados pessoais, tornou a privacidade uma preocupação crescente dentro da sociedade.

Para regulamentar o tratamento desses dados, o Brasil sancionou, em 2018, a Lei Geral de Proteção de Dados (LGPD), estabelecendo os princípios e as finalidades da coleta, além de prever sanções em caso de violações, exige maior proteção, uma vez que seu uso inadequado pode resultar em discriminação e violação de direitos individuais, e, para proteger os direitos dos titulares de dados pessoais, definidos em seu artigo 5º, inciso I, como qualquer informação relacionada a uma pessoa natural identificada ou identificável, incluindo nome, endereço, telefone, e-mail, CPF, RG e dados bancários (Brasil, 2018), já os dados pessoais sensíveis, especificados no artigo 5º, inciso II, abrangem informações como origem racial, convicções religiosas, opiniões políticas, dados sobre saúde ou vida sexual e dados genéticos ou biométricos.

A importância do direito à privacidade é reforçada pela Constituição Federal, em seu artigo 5º, incisos X e XII, que asseguram a inviolabilidade da intimidade e o sigilo de dados, e ressalta-se que com a Emenda Constitucional nº 115, de 2022, o direito à proteção de dados pessoais, inclusive nos meios digitais, foi formalizado, reafirmando que todas as empresas – independentemente de seu porte ou setor de atuação – estão obrigadas a cumprir a LGPD, incluindo micro e pequenas empresas, que também precisam adotar medidas para proteger os dados pessoais de seus clientes e parceiros (Brasil, 2018).

Na prática, os agentes de tratamento de dados – controladores e operadores – têm a responsabilidade de garantir que os dados sejam tratados de acordo com os limites legais da LGP, com a devida implementação de políticas rigorosas que definem quem pode acessar os

dados, para que fins específicos, e por quanto tempo eles serão mantidos. Além disso, é necessário assegurar que medidas de segurança adequadas estejam em vigor para proteger as informações sensíveis. (Aragão *et al.*,, 2020). Diante desse contexto, a adequação à LGPD é um processo fundamental que deve ser incorporado por todas as empresas, independentemente de sua estrutura, para proteger os direitos dos indivíduos e assegurar a conformidade com as diretrizes da lei.

2.2. GOVERNANÇA DE DADOS

O conceito de governança de dados surge da necessidade de gerenciar grandes volumes de dados gerados diariamente, com o intuito de promover uma utilização segura e estratégica desses ativos dentro das organizações e refere-se à definição de políticas e procedimentos que assegurem o gerenciamento proativo e eficaz dos dados de uma organização, englobando aspectos como a qualidade, segurança e privacidade dos dados (Barbieri, 2020; Faria *et al.*,, 2021). Ela abrange desde a definição de papéis e responsabilidades dentro da organização até a implementação de tecnologias que garantam a proteção e o acesso controlado às informações, inter-relacionando-se com áreas como a gestão da informação, segurança cibernética, privacidade de dados e compliance, formando um arcabouço amplo de controle e boas práticas. (Aragão *et al.*,, 2020; Silva *et al.*,, 2023)

De acordo com a DAMA (2017), a governança de dados é definida como *"o exercício da autoridade, controle e tomada de decisão compartilhada (planejamento, monitoramento e execução) sobre o gerenciamento de ativos de dados"*. Segundo Khatri *et al.,* (2010), a governança de dados exige que as decisões fundamentais sobre os dados sejam tomadas com clareza, garantindo a responsabilidade dos diferentes atores no processo de tomada de decisão e gestão dos ativos de dados, ela envolve a criação de um ambiente controlado para a gestão de informações, assegurando que os dados sejam coletados, armazenados, usados e compartilhados de maneira eficiente e em conformidade com regulamentações legais, como a Lei Geral de Proteção de Dados (LGPD).

Na prática, a governança de dados busca resolver problemas comuns de desorganização e falta de controle sobre as informações, como a ausência de padrões claros para a coleta e armazenamento de dados, a duplicidade de registros, o acesso não autorizado e a falta de mecanismos de auditoria, fatores estes que afetam a qualidade da informação, e isso significa que os dados devem ser eficazes e adequados para a finalidade a que se destinam, no entanto, quando não apresentam uma qualidade satisfatória, a solução geralmente envolve ajustes nos processos e comportamentos. (Silva *et al.*,, 2023)

No campo das *startups*, a implementação de um programa de governança de dados é particularmente desafiadora, uma vez que essas empresas operam com menos recursos e em ambientes altamente dinâmicos, logo, é vital que as *startups* adotem *frameworks* flexíveis que permitam uma adaptação escalável à medida que a empresa cresce, mantendo-se em conformidade com regulamentações como a LGPD, que exige um controle rigoroso sobre o ciclo de vida dos dados pessoais (Aragão *et al.*,, 2020; Agustinho *et al.*,, 2024). Portanto, a adoção de uma governança eficaz contribui diretamente para a sustentabilidade e o crescimento de longo prazo das *startups*, ao mesmo tempo que as protege de sanções legais e prejuízos reputacionais.

2.3. *FRAMEWORKS* DE GOVERNANÇA DE DADOS

Os *frameworks* de governança de dados são estruturas conceituais que fornecem diretrizes e melhores práticas para a gestão de dados dentro de uma organização e são necessários para auxiliar as empresas para adequação aos processos internos, definir responsabilidades e implementar controles que garantam o uso adequado e seguro dos dados, ou seja, servem como ferramentas que organizam a governança de dados de forma estruturada, promovendo a conformidade com regulamentações como a LGPD e a melhoria da eficiência organizacional (Barbieri, 2020). Um dos principais *frameworks* amplamente utilizados é o proposto pelo *Data Governance Institute* (DGI), que divide a governança de dados em cinco domínios principais: princípios de dados, qualidade de dados, metadados, acesso a dados e ciclo de vida dos dados (Khatri *et al.*,, 2010). Esse modelo, ao ser aplicado em *startups*, permite um controle eficaz do fluxo de dados, essencial para garantir a conformidade com a LGPD, que exige que o tratamento de dados siga finalidades específicas e com base legal adequada.

Outro *framework* relevante é o DAMA-DMBOK *(Data Management Body of Knowledge*), que aborda dez áreas de conhecimento essenciais para a governança de dados, incluindo a segurança e privacidade de dados, além de estabelecer padrões de qualidade e gerenciamento de metadados (Dasgupta et. al., 2019), sendo um conjunto de boas práticas que cobre princípios e orientações para o gerenciamento eficaz de dados, destacando sua importância para manter a coerência e o equilíbrio entre as diversas funções de gerenciamento de dados, e, ao seu redor, estão 11 áreas de conhecimento, como Arquitetura de Dados, Modelagem e Design de Dados, Qualidade de Dados, Metadados, Segurança da Informação, entre outras, sendo que, cada uma dessas áreas é um pilar importante para a gestão de dados e pode ser

implementada em diferentes momentos, conforme as necessidades da organização (Benck, 2023).

Dentre os *frameworks* mais reconhecidos no campo da Tecnologia da Informação (TI) e a gestão de dados, destaca-se o *Control Objectives for Information and Related Technologies* (COBIT), desenvolvido pela ISACA, ele fornece um conjunto estruturado de processos, objetivos de controle e métricas que auxiliam as organizações a alinhar suas operações de TI aos objetivos estratégicos de negócios, podendo ser adaptado para organizar a coleta, o processamento e o armazenamento de dados, garantindo a conformidade com regulamentações de privacidade, como a LGPD (Barbieri, 2020; Teodoro *et al.,*, 2023).

Outro *framework* que tem sido utilizado para garantir a conformidade com a LGPD é ISO/IEC 27001:2022 é um padrão internacional que estabelece diretrizes essenciais para a criação de um Sistema de Gestão de Segurança da Informação (SGSI) e oferece um conjunto de práticas para proteger os ativos digitais de uma organização, concentrando-se na confidencialidade, integridade e disponibilidade das informações, identificando e mitigando riscos relacionados à segurança dos dados (de De Paula *et al.,*, 2024). Importante destacar que a ISO 27001:2022 (ABNT, 2022) abrange diversas áreas-chave, tais como a Política de Segurança da Informação (A5) que define diretrizes claras para a proteção das informações, enquanto a Organização da Segurança da Informação (A6) estabelece responsabilidades e papéis na segurança dos dados e a Segurança de Recursos Humanos (A7), além da Gestão da Continuidade do Negócio (A17) estabelece planos para manter as operações mesmo em caso de falhas de segurança, enquanto a Conformidade (A18) assegura o alinhamento das operações de segurança da informação com as obrigações legais e regulatórias, entre outras. Com esses componentes interligados, a ISO/IEC 27001:2022 cria um sistema completo e eficaz para a gestão da segurança da informação, abordando todas as áreas necessárias para a proteção adequada dos dados (de De Paula, 2024).

Além dos *frameworks* mencionados anteriormente, é importante destacar a influência do Regulamento Geral de Proteção de Dados (GDPR) da União Europeia na elaboração da Lei Geral de Proteção de Dados brasileira, sancionada em 2018, e embora a GDPR tenha sido criado especificamente para a conformidade com a legislação europeia, muitas diretrizes do GDPR são aplicáveis à LGPD, servindo como uma base para empresas que desejam gerenciar dados de forma responsável, pois ambas as leis compartilham princípios fundamentais de proteção de dados, protegendo a privacidade dos indivíduos. Mas, em que pese as leis se assemelhem, a GDPR é mais detalhado e abrangente em suas disposições, e por esse motivo, uma empresa em conformidade com a GDPR estará, na maioria dos casos,

em conformidade com a LGPD, entretanto, o contrário nem sempre é verdadeiro (Okano *et al.*, 2024; Castro *et al.*, 2022).

E para que as organizações alcancem essa conformidade com a GDPR, é fundamental a definição de cargos e responsabilidades, como titular, controlador e operador de dados, além de estabelecer políticas de acesso que definam claramente quem pode acessar os dados e com quais finalidades, além disso, assegurar transparência e conformidade que a documentação de todas as operações envolvendo dados pessoais é essencial para implementar medidas técnicas e organizacionais que protejam os dados pessoais, bem como realizar auditorias regulares para verificar a aderência às disposições da LGPD e do GDPR no intuito de garantir que o tratamento de dados esteja em conformidade com as legislações de proteção de dados (Okano *et al.*, 2024; Castro *et al.*, 2022; Aragão *et al.*, 2020). Cada um desses *frameworks* possui características que os tornam adequados para diferentes cenários e tamanhos de empresas, no entanto, *startups* enfrentam o desafio de adaptar esses modelos às suas realidades específicas, dado o seu tamanho, agilidade e limitação de recursos (Agustinho *et al.*, 2024).

Portanto, *startups* necessitam de *frameworks* que possibilitem escalabilidade e adaptação gradual, sem comprometer sua conformidade com a LGPD. A escolha de um *framework*, ou a combinação de elementos de diferentes modelos, deve levar em consideração a capacidade da empresa de alocar recursos e gerenciar os dados de forma eficiente, sem perder sua competitividade e agilidade no mercado. Este estudo visa explorar como esses *frameworks* podem ser ajustados para atender às necessidades particulares de *startups*, de modo que estas possam estar em conformidade com a LGPD sem comprometer sua inovação e crescimento.

2.4. *STARTUPS* E OS DESAFIOS DA CONFORMIDADE

Startups, por sua própria natureza, operam em ambientes de extrema incerteza e alta volatilidade, sendo geralmente caracterizadas por equipes enxutas, recursos financeiros limitados e uma forte pressão por crescimento rápido (Ries, 2011). Nesse contexto, a conformidade com regulamentações complexas, como a Lei Geral de Proteção de Dados, pode se apresentar como um desafio significativo, pois ela exige que todas as empresas adotem medidas rigorosas para a proteção de dados pessoais, o que implica na criação de políticas de privacidade, nomeação de um encarregado de dados (*Data Protection Officer* - DPO), implementação de controles de segurança e a gestão eficaz do ciclo de vida dos dados. Para *startups*, esses requisitos muitas vezes geram obstáculos, dado o custo e a complexidade associados à conformidade (Agustinho *et al.*, 2024; Aragão *et al.*, 2020).

Startups enfrentam inúmeros desafios ao implementar medidas de segurança da informação, principalmente devido à escassez de recursos, pois a adequação à Lei Geral de Proteção de Dados (LGPD) é particularmente complexa para essas empresas, dadas suas características estruturais, como equipes enxutas, recursos financeiros limitados e a necessidade constante de inovar rapidamente (Ries, 2011) e mesmo com investimentos do governo ou do setor privado, *startups* frequentemente enfrentam obstáculos que dificultam seu crescimento e a implementação de uma governança de dados eficaz. A falta de recursos se mostra como um problema fundamental, já que essas empresas precisam alocar pessoal e financiamento para iniciativas de conformidade, enquanto lidam com múltiplas atividades simultâneas, como aquisição de clientes e melhoria de produtos (Agustinho *et al.*,, 2024). Essa multiplicidade de tarefas acaba sobrecarregando os recursos limitados das *startups*, dificultando ainda mais a implementação de práticas sólidas de governança de dados.

Além disso, um dos principais desafios apontados por Agustinho *et al.,* (2024) é a implementação de ferramentas e estruturas eficazes de governança de dados, que requerem investimentos significativos, tendo em vista que as *startups* também precisam adaptar sua cultura interna, promovendo a conscientização entre os colaboradores sobre a importância desses aspectos, logo, não se trata apenas de estabelecer mecanismos para a proteção e privacidade de dados pessoais, mas sim de capacitação da equipe sobre a importância de proteção de dados. Outro obstáculo significativo está na gestão do portfólio de atividades, pois conforme destaca Ries (2011, p. 24), *startups* precisam equilibrar o suporte aos clientes existentes com a necessidade de inovar, sob a pressão de atender demandas imediatas, essas empresas muitas vezes acabam negligenciando as medidas de governança de dados, com o o intuito de acelerar seu crescimento. Além disso, a integração dos princípios da LGPD nas práticas de negócios pode ser um processo complexo e demorado, especialmente para aquelas sem expertise interna (Aragão *et al.*,, 2020).

A complexidade da LGPD agrava ainda mais esses desafios. A legislação é aplicada independentemente do porte da empresa, o que representa uma barreira adicional para *startups* que operam com equipes multifuncionais e colaboradores que acumulam diversas funções (Aragão *et al.,* 2020). A contratação de profissionais especializados, como o Data Protection Officer (DPO), é muitas vezes inviável devido aos altos custos, levando a falhas na implementação de políticas de conformidade e na gestão de riscos de dados (Chaves *et al.*,, 2023). Além disso, a exigência de consentimento explícito, a necessidade de segurança da informação e a manutenção de registros detalhados das operações tornam a adequação ainda mais complexa (Melo Filho *et al.*,, 2023). Por fim, o crescimento acelerado das *startups*

pode complicar ainda mais o processo de conformidade a medida que a empresa expande suas operações, tanto em termos de volume de dados quanto de alcance geográfico, pois aumenta a necessidade de uma governança de dados mais robusta aumenta.

Assim, entender os desafios específicos enfrentados por *startups* no que diz respeito à governança de dados e à conformidade com a LGPD é fundamental para o desenvolvimento de soluções que possam tornar o processo mais acessível, eficiente e alinhado às suas necessidades dinâmicas.

3. DISCUSSÃO DOS RESULTADOS

Os resultados preliminares da pesquisa indicam que, embora as *startups* enfrentem diversos obstáculos para alcançar a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), é possível desenvolver *frameworks* de governança de dados adaptados às suas necessidades específicas. A análise dos principais *frameworks* consolidados revela que cada um possui características e forças que, quando combinadas ou adaptadas, podem oferecer soluções viáveis para o contexto dinâmico e limitado em recursos das *startups*.

Ao analisar os *frameworks* DAMA-DMBOK, COBIT, GDPR (como o OneTrust), e o Data Governance Institute *Framework* (DGI), é possível perceber que cada modelo possui pontos fortes, lacunas e diferentes níveis de adaptabilidade, conforme resta demonstrado no quadro 1.

QUADRO 1 - COMPARATIVO DE FRAMEWORKS

Framework	**Áreas de Conhecimento**	**Forças**	**Lacunas/ Limitações**	**Adaptabilidade**	**Referências**
DAMA-DMBOK	Governança, Qualidade de Dados, Segurança, Metadados, Big Data	Abrangente; cobre múltiplas áreas de gestão de dados, fornecendo uma visão holística para implementação	Falta foco específico em leis de privacidade, como LGPD e GDPR; não adaptado para gestão de dados em nuvem	Altamente adaptável; pode integrar *frameworks* de privacidade faltantes para cumprir exigências legais	Barbieri (2020)
COBIT	Governança de TI, Segurança de Dados, Conformidade, Gestão de Riscos	Forte na governança de TI e gestão de riscos; alinha operações de TI aos objetivos do negócio e	Menor foco na qualidade de dados e gestão de metadados, críticos para uma	Flexível; pode ser integrado com *frameworks* que priorizam qualidade e privacidade de dados	Teodoro *et al.,* (2023)

		conformidade regulatória	governança completa		
***Frameworks* GDPR**	Privacidade, Segurança de Dados, Conformidade	Centrado em atender regulamentações como GDPR e LGPD; fornece diretrizes específicas para privacidade e segurança	Foco limitado nos processos de gestão de dados abrangentes; lacuna em práticas de qualidade e governança holística	Pode ser complementado por outros *frameworks* de governança para formar uma abordagem completa	Castro *et al.,* (2022)
Data Governance Institute *Framework* (DGI)	Políticas de Governança, Estruturas de Decisão, Qualidade de Dados	Abordagem holística com foco em políticas e processos consistentes de governança de dados	Menos prescritivo na governança de TI, limitando sua aplicação na integração com TI	Altamente compatível com *frameworks* focados em TI, como COBIT	Faria *et al.,* (2018)

Fonte: A Autora (2024)

A análise comparativa destes *frameworks*, conforme resumida no quadro apresentado, destaca que nenhum deles, isoladamente, é capaz de atender a todas as necessidades de governança de dados dessas organizações, o que demonstra que a aplicação combinada e adaptada pode oferecer uma solução prática e eficiente.

O DAMA-DMBOK, conforme Barbieri (2020), se destaca por sua abordagem abrangente, cobrindo áreas como governança, qualidade de dados, segurança, metadados e *big data* e sua principal vantagem é fornecer uma visão holística da governança de dados, mas observa-se uma limitação quanto a falta de foco específico em regulamentações de privacidade, como a LGPD e o GDPR, além de não ser originalmente adaptado para a gestão de dados em ambientes de nuvem, uma característica vital para *startups* que geralmente utilizam tecnologias *cloud* devido a seus recursos limitados, o DAMA-DMBOK pode ser complementado com *frameworks* de privacidade para preencher essas deficiências.

Quando analisado o COBIT, discutido por Teodoro *et al.,* (2023), tem-se que seu ponto forte é na governança de TI, segurança de dados, conformidade e gestão de riscos,

especialmente para organizações que precisam alinhar as operações de TI aos objetivos do negócio e à conformidade regulatória, no entanto, sua ênfase em governança de TI resulta em um menor foco na qualidade de dados e na gestão de metadados, que são elementos críticos para uma governança de dados abrangente, mas observa-se uma flexibilidade que permite que ele seja integrado a outros *frameworks* que priorizam qualidade e privacidade de dados, tornando-o uma ferramenta complementar útil, especialmente para *startups* em busca de conformidade com a LGPD.

Os *frameworks* centrados no GDPR, concentram-se fortemente na privacidade, segurança de dados e conformidade com regulamentos, atendendo assim diretamente aos requisitos tanto do GDPR europeu quanto da LGPD brasileira e como observado por Castro *et al.* (2022), sua maior vantagem está em fornecer diretrizes específicas para proteger a privacidade e a segurança dos dados pessoais. Contudo, eles apresentam uma lacuna significativa quando se trata de processos abrangentes de gestão de dados, já que seu foco principal está na conformidade regulatória, e não em aspectos mais amplos de governança de dados, logo, esses *frameworks* podem ser mais eficazes quando usados em conjunto com outros modelos que abordam a governança de dados de maneira mais holística.

O DGI propõe uma abordagem holística centrada em políticas de governança, estruturas de decisão e qualidade de dados, e sua força está em fornecer uma visão estruturada das políticas e processos necessários para uma governança de dados eficaz. No entanto, uma de suas limitações é ser menos prescritivo na governança de TI, o que pode restringir sua aplicação em organizações que precisam integrar a governança de dados e TI (Faria *et al.,* 2018), mesmo assim, o DGI é altamente compatível com *frameworks* focados em TI, como o COBIT, permitindo a criação de um modelo abrangente de governança.

Com base nessa análise, fica claro que nenhuma dessas abordagens é capaz, por si só, de fornecer uma solução completa para *startups* que buscam conformidade com a LGPD. No entanto, a adaptabilidade dos *frameworks* como DAMA-DMBOK e DGI abre a possibilidade de integrá-los com elementos de outros modelos, como o COBIT, para abordar aspectos específicos como segurança e qualidade de dados. Por exemplo, a robustez do DAMA-DMBOK em gestão de dados pode ser complementada com o foco do COBIT em governança de TI e com as diretrizes de privacidade fornecidas pelos *frameworks* centrados no GDPR.

4. CONCLUSÃO

A pesquisa realizada revela que, apesar dos desafios enfrentados pelas startups brasileiras para alcançar a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), é possível desenvolver frameworks de governança de dados adaptados às suas necessidades. A análise dos frameworks, como DAMA-DMBOK, COBIT, frameworks centrados no GDPR, e o DGI, mostrou que cada um possui forças e limitações. No entanto, ao serem combinados estrategicamente, esses modelos podem preencher lacunas e criar uma solução eficiente que equilibra a necessidade de conformidade com a LGPD e a natureza dinâmica das startups.

Assim, sugere-se a criação de um *framework* de governança de dados ajustado ao contexto das *startups*, capaz de simplificar a conformidade com a LGPD sem comprometer a inovação e a agilidade inerentes a essas empresas. A proposta inclui a adoção de práticas de conscientização e treinamento contínuo dos colaboradores, além da utilização de ferramentas tecnológicas acessíveis para automação de processos. Dessa forma, espera-se que os resultados da pesquisa contribuam significativamente para o campo da governança de dados em *startups*, fornecendo orientações práticas que possibilitem a adequação à LGPD e a proteção dos dados pessoais no ambiente de negócios em constante transformação.

REFERÊNCIAS BIBLIOGÁFICAS:

ARAGÃO, Alexandra *et al., Startup e o desafio do Compliance.* Revista Brasileira de Políticas Públicas, v. 10, n. 3, 2020. Disponível em: https://www.publicacoesacademicas.uniceub.br/RBPP/article/view/7270. Acesso em: 17.01.2024.

AGUSTINHO, E. O.; *et al., Engajamento corporativo nos programas de privacidade das empresas da Nova Economia*. Contribuciones A Las Ciencias Sociales, *[S. l.]*, v. 17, n. 6, p. e6361 , 2024. DOI: 10.55905/revconv.17n.6-104. Disponível em: https://ojs.revistacontribuciones.com/ojs/index.php/clcs/article/view/6361. Acesso em: 5 out. 2024.

BARBIERI, Carlos. *Governança de dados: práticas, conceitos e novos caminhos.* Rio de Janeiro: Alta Books, 2020.

BENCK, Larissa Lourenço Nunes. *LGPD e seu desafio para as organizações: um estudo demonstrativo entre as estruturas de dados (frameworks) de adequação à lei.* — Dissertação: UFPR. Curitiba, 2023.

BRASIL. *Lei Geral de Proteção de Dados Pessoais - Lei nº 13.709, de 14 de agosto de 2018*. Brasília: DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 05.10.2024.

DE CASTRO, Marcos Maciel; *et al., Uma Arquitetura Baseada em Blockchain para Auditoria de Conformidade com Regulamentos de Proteção de Dados*. In: Simpósio Brasileiro De Segurança Da Informação E De Sistemas Computacionais (SBSEG), 22., 2022, Santa Maria. Anais [...].

Porto Alegre: Sociedade Brasileira de Computação, 2022. p. 390-395. DOI: https://doi.org/10.5753/sbseg.2022.225347.

CHAVES, Joel Ricardo Ribeiro de *et al.,*. *Proteção de dados pessoais e startups: uma visão do contexto brasileiro*. Prisma Juridico, [S. l.], v. 22, n. 2, p. 196–216, 2023. DOI: 10.5585/2023.22454. Disponível em: https://periodicos.uninove.br/prisma/article/view/22454. Acesso em: 5 out. 2024..

DASGUPTA, A.; *et al., A Conceptual Framework for Data Governance in IoT-enabled Digital IS Ecosystems*. Proceedings of the 8th International Conference on Data Science, Technology and Applications, 2019.

DAMA. *Data Management Body of Knowledge (DMBOK*). Chicago: DAMA International, 2017.

FARIA, M. R.; SILVA, M. L.; CORDEIRO, K. F. GovDadosMB: Um *framework* de Governança de Dados Corporativos para a Marinha do Brasil. *SBC Brazilian Symposium on Databases*, 2018.

DE DE PAULA, A. P. O. de, *et al., LGPD por design: privacidade e proteção de dados em projetos de software*. Observatório De La Economía Latinoamericana, *[S. l.]*, v. 22, n. 6, p. e5520, 2024. DOI: 10.55905/oelv22n6-258. Disponível em: https://ojs.observatoriolatinoamericano.com/ojs/index.php/olel/article/view/5520. Acesso em: 5 out. 2024.

DE JESUS, Ewerton David Brito; *et al., Requisitos de Segurança e Privacidade em Startups: Um Estudo Empírico em uma Aplicação de Governança de Dados*. Disponível em: http://wer.inf.puc-rio.br/WERpapers/artigos/artigos_WER24/WER2024_paper_22.pdf. Acesso em: 5 out. 2024.

DONEDA, D. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

KHATRI, Vijay. *et al., Projetando governança de dados*. Commun. ACM 53, 1 (janeiro de 2010), 148–152. https://doi.org/10.1145/1629175.1629210. Acesso em: 5 out. 2024.

MELO FILHO, D. R. de, *et al., Scrum Methodology: An ally in the implementation of LGPD*. Research, Society and Development, *[S. l.]*, v. 12, n. 4, p. e22712441189, 2023. DOI: 10.33448/rsd-v12i4.41189. Disponível em: https://rsdjournal.org/index.php/rsd/article/view/41189. Acesso em: 5 oct. 2024.

OKANO, Marcelo T; *et al., LGPD O Novo Desafio Para As Organizações: Exemplos De Frameworks Para Diagnosticar Este Novo Cenário*. South American Development Society Journal, *[S. l.]*, v. 7, n. 20, p. 380, 2021. DOI: 10.24325/issn.2446-5763.v7i20p380-396. Disponível em: https://www.sadsj.org/index.php/revista/article/view/444. Acesso em: 5 out. 2024.

RIES, E. *Startup Enxuta: Como os empreendedores atuais usam inovação contínua para criar empresas de sucesso*. São Paulo: Leya, 2011.

SILVA, C. de A.; *et al., Modelo de governança de dados em uma plataforma de pagamentos digitais: Data governance model on a digital payments platform*. Brazilian Journal of Business, *[S. l.]*, v. 4, n. 4, p. 2511–2527, 2022. DOI: 10.34140/bjbv4n4-060. Disponível em: https://ojs.brazilianjournals.com.br/ojs/index.php/BJB/article/view/55448. Acesso em: 5 out. 2024.

TEODORO, J.; *et al., Um modelo Canvas do processo de adaptação à Lei Geral de Proteção de Dados: o caso da Universidade do Estado de Santa Catarina (UDESC)*. Revista Brasileira de Biblioteconomia e Documentação, *[S. l.]*, v. 19, p. 1–28, 2023. Disponível em: https://rbbd.febab.org.br/rbbd/article/view/1869. Acesso em: 5 out. 2024.