REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

ESTRATÉGIAS DE COOPERAÇÃO E GOVERNANÇA DIGITAL: O IMPACTO DAS JOINT VENTURES E DA INTELIGÊNCIA ARTIFICIAL NA VANTAGEM COMPETITIVA

COOPERATION STRATEGIES AND DIGITAL GOVERNANCE: THE IMPACT OF JOINT VENTURES AND ARTIFICIAL INTELLIGENCE ON COMPETITIVE ADVANTAGE

Ciências Sociais Aplicadas • 18/05/2026

REGISTRO DOI: 10.70773/revistatopicos/778988124

Vinicius Rodrigues de Oliveira[1]

Kamilla Prado Souza[2]

RESUMO

O presente artigo investiga a convergência entre redes de cooperação interorganizacional, *Joint Ventures* (JVs) e a Inteligência Artificial (IA) como vetores de vantagem competitiva sustentável. O objetivo central é analisar como modelos de governança digital e conformidade legal permitem que pequenas e médias empresas (PMEs) superem barreiras de entrada em mercados de alta tecnologia. A metodologia adotada consistiu em uma revisão bibliográfica sistemática, com análise qualitativa de marcos regulatórios e levantamento bibliométrico em bases como Scopus e Web of Science entre 2019 e 2026. Os resultados revelam que a viabilidade das alianças digitais depende da orquestração eficiente de ecossistemas e da garantia de transparência algorítmica. Identificou-se que a IA, integrada a contratos robustos de transferência tecnológica, mitiga riscos de passivos jurídicos e potenciais danos morais. Conclui-se que a vantagem competitiva na era digital decorre da capacidade de integrar recursos externos com segurança jurídica, transformando o *compliance* em um ativo estratégico de reputação e escalabilidade produtiva.

Palavras-chave: Cooperação Interorganizacional; Joint Venture; Inteligência Artificial; Governança Digital; LGPD.

ABSTRACT

This article investigates the convergence between inter-organizational cooperation networks, Joint Ventures (JVs), and Artificial Intelligence (AI) as drivers of sustainable competitive advantage. The main objective is to analyze how digital governance models and legal compliance enable small and medium-sized enterprises (SMEs) to overcome entry barriers in high-tech markets. The adopted methodology consists of a systematic literature review, featuring a qualitative analysis of regulatory frameworks and a

bibliometric survey in databases such as Scopus and Web of Science between 2019 and 2026. The results reveal that the viability of digital alliances depends on efficient ecosystem orchestration and the guarantee of algorithmic transparency. It identifies that AI, when integrated into robust technology transfer contracts, mitigates legal liability risks and potential moral damages. The study concludes that competitive advantage in the digital era stems from the ability to integrate external resources with legal certainty, transforming compliance into a strategic asset for reputation and productive scalability.
Keywords: Inter-organizational Cooperation; Joint Venture; Artificial Intelligence; Digital Governance; LGPD.

1. INTRODUÇÃO

A competitividade global na terceira década do século XXI deslocou o eixo da eficiência puramente individual para a orquestração estratégica de ecossistemas digitais. No cenário contemporâneo, a manutenção da vantagem competitiva transcende a posse física de ativos, exigindo que as organizações desenvolvam "capacidades ainda mais dinâmicas" para sentir, apreender e transformar suas bases de recursos frente a mudanças tecnológicas aceleradas (TEECE, 2020). Nesse prisma, a cooperação interorganizacional deixou de ser uma alternativa tática para consolidar-se como o novo lócus da inovação disruptiva, permitindo que empresas compartilhem riscos e acessem fluxos externos de conhecimento que seriam inacessíveis de forma isolada (Balestrin; Verschoore, 2008).

Analisando o ecossistema de interdependência, a Inteligência Artificial desponta como um dos principais catalisadores de

transformação, reformulando os pilares da produtividade e da escala empresarial. Segundo Nambisan et al. (2019), O surgimento de tecnologias computacionais inovadoras e poderosas, plataformas e infraestruturas digitais transformou a inovação e o empreendedorismo de maneiras significativas. A inserção de pequenas e médias empresas em ecossistemas de redes de cooperação e a formação de *Joint Ventures* tornam-se mecanismos imprescindíveis para mitigar a escassez de recursos técnicos e financeiros, possibilitando que lacunas de mercado sejam preenchidas por meio de soluções tecnológicas de ponta (RIALTI et al., 2020).

No entanto, as integrações aceleradas da Inteligência Artificial nas alianças estratégicas introduzem uma complexidade jurídica e ética sem precedentes. A problemática central reside no vácuo de segurança jurídica relacionado à autoria algorítmica, aos conflitos de propriedade intelectual e à proteção de ativos de *know-how* em ambientes compartilhados. Conforme aponta Floridi (2021), a eficácia das parcerias tecnológicas depende agora de um "compliance algorítmico" que assegure a transparência e a explicabilidade dos modelos utilizados. No ordenamento jurídico brasileiro, essa pressão é acentuada pelo rigor da Lei Geral de Proteção de Dados Pessoais (LGPD) e pela recente jurisprudência ocasionada pelo Superior Tribunal de Justiça (STJ, 2025), onde eleva o padrão de responsabilidade das empresas no tratamento de dados sensíveis.

A luz desse cenário de incerteza regulatória e dinamismo tecnológico, o presente artigo propõe-se a investigar: como estruturar modelos de governança digital em cooperações e *Joint Ventures* para que o uso da Inteligência Artificial resulte em

vantagem competitiva sustentável sem comprometer a integridade legal e os ativos intelectuais das organizações. O objetivo é analisar a convergência entre a Visão Baseada em Recursos Digitais (DRBV) e as diretrizes de conformidade algorítmica, oferecendo um *framework* de governança que permita ao pequeno empreendedor navegar na economia de dados com segurança jurídica e escalabilidade.

2. FUNDAMENTAÇÃO TEÓRICA

2.1. Visão Baseada em Recursos Digitais (DRBV)

A Visão Baseada em Recursos Digitais (DRBV) é a evolução da Visão Baseada em Recursos (RBV), ela postula que a vantagem competitiva não reside apenas nos ativos físicos, mas na capacidade de orquestrar dados, algoritmos e infraestrutura de nuvem. O uso de Machine Learning permite às empresas desenvolver ofertas mais inovadoras a partir do acesso a Big Data, potencializando a capacidade de inovação (NAMBISAN et al., 2019). Analisando o contexto das Pequenas e Médias empresas, a utilização da IA atua como um recurso de rede. Segundo Volberda et al. (2021), a agilidade estratégica na era digital depende da habilidade de integrar competências externas, dado que o ciclo de inovação da IA é acelerado.

As pequenas empresas enfrentam dificuldades para inovar, pois têm menor capacidade de captura de valor através dos dados dos seus clientes, segundo Nambisan et al. (2019) as empresas menores dependem predominantemente de proteções informais, como o controle de versões e a agilidade no prazo de entrega. A cooperação pode potencializar o Big Data destas organizações, tendo em vista o

acesso a dados de clientes conjuntos das organizações. Nesse prisma, as *Joint Ventures* permitem o compartilhamento de ativos complementares de dados. Conforme Rialti et al. (2020), a vantagem competitiva em ambientes de Big Data advém da ambidestria organizacional: explorar o negócio atual enquanto se co-cria o futuro em rede, diluindo custos de Pesquisa e Desenvolvimento (P&D).

A DRBV transcende a visão estática da posse de ativos, posicionando a orquestração de ecossistemas digitais como o cerne da vantagem competitiva contemporânea (TEECE, 2020). Conforme defendido por Nambisan et al. (2019) e Volberda et al. (2021), a raridade e a inimitabilidade no cenário digital não decorrem de recursos isolados, mas da capacidade dinâmica de integrar IA e dados em redes de cooperação, permitindo que PMEs alcancem escalabilidade e proteção jurídica outrora restritas a grandes corporações."

2.2. Governança de Dados e Orquestração de Ecossistemas

A governança em parcerias tecnológicas evoluiu para a Orquestração de Ecossistemas Digitais (LINGENS et al., 2021). A Inteligência artificial quando aplicada as Joint Ventures, requer que um esforço gerencial da governança para que faça o equilíbrio da tensão entre a abertura (compartilhamento de dados para treinamento) e o fechamento (proteção de segredos comerciais). Teece (2020) reforça que as Capacidades Dinâmicas sentir, apreender e transformar são essenciais para que as empresas reconfigurem suas bases de recursos frente às mudanças regulatórias, como a LGPD no Brasil e o *AI Act* na União Europeia (EUROPEAN UNION, 2024). A governança digital atua como uma salvaguarda contra o comportamento oportunista em ambientes de alta incerteza (JACOBIDES et al., 2019).

2.3. Inteligência Artificial Ética e Compliance Algorítmico

A integralização da IA exige o chamado Compliance Algorítmico (FLORIDI, 2023). As organizações devem ir além das exigências legais, para mitigar riscos e garantir a segurança jurídica dos usuários, frente a um cenário de rápidas mudanças tecnológicas (Pinheiro; Brega, 2021) A vantagem competitiva agora é também reputacional. Conforme Jobin et al. (2019), a transparência e a explicabilidade dos algoritmos (*XAI*) são requisitos de governança para evitar passivos jurídicos. O Brasil segundo Kfouri e Zambão (2025), carece de regulamentação especifica, como a Due Diligence Algorítmica e explicabilidade contratual para a realização de análises rigorosas antes da implementação dos sistemas para avaliar dados, arquitetura e potenciais impactos.

O recente crescimento exponencial de dados e os avanços dos cibercrimes reforçam a necessidade de legislações específicas para assegurar direitos fundamentais (Araújo, 2024). O marco regulatório existente em países como o Reino Unido (*Public Services AI Procurement Framework*) e a União europeia (AI Act) visam proteger os direitos fundamentais, os algoritmos das IAs são reflexos dos dados aos quais são alimentados, segundo Maracajá et al (2026) os sistemas de IA não são neutros: eles refletem os valores, preconceitos e limitações dos dados com os quais são treinados e dos objetivos que orientam sua construção. Em 2016 o caso do chatbot da Microsoft a robô Tay, que passou a emitir comentários homofóbicos, machistas e racistas após interações com usuários, ilustra como essa preocupação é válida.

2.4. Exigências Centrais da LGPD e a Gestão de Riscos no Setor de Pequeno Porte

A observância dos requisitos legais na economia de dados é imperativa para mitigar riscos de responsabilização civil e administrativa, especialmente em ambientes de cooperação onde o fluxo de informações é intenso. Conforme Pereira Filho e De Araújo Lima (2025), é necessário o desenvolvimento de políticas de governança algorítmica que assegurem que os princípios de transparência sejam sempre seguidos. O desenvolvimento constante e a inclusão de camadas adicionais de segurança são extremamente necessários, pois sua violação, conforme consolidado pelo STJ (2025), aciona o dano moral presumido devido à potencialidade discriminatória e à grave invasão da esfera íntima.

No âmbito da operabilidade, a eficácia do *compliance* em *JV* depende do enquadramento do tratamento em uma das bases legais previstas na LGPD. Ressalta-se a aplicação rigorosa do Art. 14 para dados de crianças e adolescentes, que impõe o consentimento específico e em destaque. Além disso, a gestão da transparência que é materializada nos Arts. 9º e 18 não são apenas um dever legal, mas uma estratégia de fidelização e confiança, garantindo ao titular direitos de acesso, portabilidade e exclusão (FLORIDI, 2021).

Por fim, a segurança e o descarte (Art. 16 e 46) e a Gestão de Operadores (Art. 39) representam os pontos críticos da responsabilidade compartilhada. Micro e pequenas empresas que terceirizam serviços de TI ou logística para viabilizar a operação de IA, devem formalizar contratos com cláusulas especificas sobre confidencialidade. Como o controlador permanece como o garantidor final perante a ANPD, a falha técnica de um operador terceirizado pode comprometer a solvência da pequena empresa devido à responsabilidade solidária em incidentes de segurança (SILVA, 2024). A responsabilidade compartilhada, pode oferecer

riscos a integridade moral da empresa se não houver transparência com os usuários e contratos

3. METODOLOGIA

A presente pesquisa caracteriza-se por uma abordagem qualitativa e exploratória, fundamentada no método de Revisão Bibliográfica Sistemática (RBS), que visa fornecer uma síntese rigorosa e replicável do estado da arte sobre a interseção entre *Joint Ventures*, Inteligência Artificial e Governança Digital (SNYDER, 2019). O desenho metodológico foi estruturado em três fases distintas e complementares:

Fase 1: Levantamento Bibliométrico e Heurística de Busca A coleta de dados primários ocorreu entre janeiro de 2025 e março de 2026, com consultas às bases de dados indexadas *Scopus (Elsevier)*, *Web of Science* e *Google Scholar*. Utilizou-se a técnica de busca booleana com os descritores combinados: ("Joint Venture" OR "Inter-organizational Cooperation") AND ("Artificial Intelligence" OR "Algorithmic Governance") AND ("Competitive Advantage" OR "VRIO"). Como critério de inclusão, estabeleceu-se o recorte temporal de 2019 a 2026, priorizando artigos de periódicos com revisão por pares (*peer-reviewed*) e marcos regulatórios vigentes.

Fase 2: Análise Documental e Jurídica Complementarmente, realizou-se uma análise documental exegética de dispositivos legais brasileiros, com foco na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18) e na Emenda Constitucional nº 115/2022. Para garantir a atualidade da discussão sobre responsabilidade civil em ambientes digitais, foram integrados acórdãos recentes do Superior Tribunal de Justiça (STJ, 2025), permitindo a conexão entre a teoria

administrativa e a realidade jurisprudencial brasileira (RIBEIRO; MOREIRA, 2026).

Fase 3: Tratamento de Dados e Síntese Qualitativa Os dados foram submetidos à Análise de Conteúdo, seguindo as etapas de pré-análise, exploração do material e tratamento dos resultados (BARDIN, 2016). Os achados foram confrontados com as premissas da Visão Baseada em Recursos Digitais (DRBV) e da Teoria da Orquestração de Ecossistemas, resultando na proposição do *framework* de governança apresentado na seção de discussão. A validação das inferências buscou a triangulação entre as exigências de *compliance* tecnológico e os objetivos de vantagem competitiva estratégica para PMEs.

4. RESULTADOS E DISCUSSÕES OU ANÁLISE DOS DADOS

4.1. Desafios Estruturais e Alianças Estratégicas

A análise dos dados bibliométricos e documentais aponta que a formação de *Joint Ventures* (JVs) configura-se como a estratégia de orquestração mais eficiente para que PMEs superem a "liability of smallness" no campo da Inteligência Artificial. Conforme a Visão Baseada em Recursos Digitais (DRBV), a JV permite a fusão de ativos de dados heterogêneos, criando uma vantagem competitiva inimitável. Contudo, essa estrutura híbrida de governança exige a gestão de tensões relacionais e operacionais, sintetizadas na Tabela 1.

Tabela 1: Dinâmica Estratégica e Conflitos em Joint Ventures (JVs)

Razões Estratégicas para JV	Potenciais Conflitos de Governança

Transferência de Tecnologia: Acesso simbiótico a inovações e know-how estratégico de parceiros.	Oportunismo Pós-Contratual: Uso individual de tecnologias desenvolvidas na rede para fins privados.
Divisão de Riscos: Compartilhamento de encargos financeiros e incertezas inerentes à P&D.	Assimetria de Informação: Desacordos sobre licenciamento e titularidade de descobertas comuns.
Economia de Escala: Otimização da produção e distribuição de ativos digitais em rede.	Choque de Cultura Organizacional: Conflito entre a necessidade de disseminação e o sigilo industrial

Fonte: Elaborado pelo autor (2026) com base em de Moro & Glitz (2013) e Teece (2020).

4.2. Impacto da LGPD e a Gestão de Riscos na Economia de Dados

A sustentabilidade das PMEs na economia digital brasileira está intrinsecamente ligada à sua capacidade de resposta normativa. No biênio 2025-2026, a conformidade deixou de ser meramente administrativa para tornar-se um requisito de viabilidade financeira. A Tabela 2 correlaciona as limitações estruturais das MPEs às estratégias de mitigação necessárias para a preservação do valor da rede.

Tabela 2: Desafios Estruturais para PMEs na Implementação da LGPD

Categoria do Desafio	Impacto Operacional na Organização	Estratégia de Mitigação Proposta
Recursos Financeiros	40% das MPEs possuem orçamento indefinido	Adoção de arquiteturas Cloud partilhadas e infraestruturas

	para TI.	escaláveis (SaaS).
Profissionais	28% carecem de equipes de TI ou DPOs dedicados (RIBEIRO, 2026).	Terceirização via Compliance-as-a-Service e convênios técnicos setoriais. (Ex: Sebraetec).
Risco Jurídico	Dano moral in re ipsa para dados sensíveis (STJ, 2025)	Implementação de Privacy by Design e Auditorias Algorítmicas de Viés

Fonte: Elaborado pelo autor (2026) com base em Dos Santos & Evangelista (2023) e STJ (2025).

4.3. Riscos, Sanções e Responsabilidade Civil

O descumprimento dos preceitos da LGPD fere Emenda Constitucional 115/2022, ela assegura o direito a proteção dos dados pessoais, inclusive nos meios digitais. A análise da jurisprudência do Superior Tribunal de Justiça, especificamente no REsp n° 2.121.904/SP (2025) que aborda a responsabilidade de seguradoras no tratamento de informações confidenciais, revela um endurecimento na interpretação do nexo causal em incidentes digitais, onde a principal consequência jurídica destacada nesta decisão foi a caracterização do dano moral presumido em que não há necessidade da vítima provar o sofrimento psicológico, o vazamento de dados sensíveis já é considerado suficiente para gerar o dever de indenizar.

Na tabela 3 podemos ainda identificar outros pontos considerados fundamentais nesta decisão, que demonstram o enrijecimento da legislação e a fundamentação da decisão com base na LGPD e Código de Defesa do Consumidor para aplicar a responsabilidade objetiva da empresa, sendo abordada em três principais pontos:

Tabela 3: Riscos, Responsabilidades, Sanções e Consequências do Vazamento de Dados

Riscos Associados ao Vazamento de Dados Sensíveis	Responsabilidade Civil	Sanções e Consequências (Dano Moral)
Honra e Imagem – Pois houve vazamento de dados como orientação sexual, origem racial, opinião política. Intimidade e Vida Privada – vazamento de dados como convicções religiosas, orientação sexual, vida sexual, opinião política. Patrimônio – Exposição de dados bancários e fiscais. Integridade física e segurança pessoal – pois houve vazamento de dados como endereço pessoal.	Dever de Proteção – O fornecedor tem a responsabilidade de comprovar a proteção dos dados pessoais, principalmente os sensíveis. Ineficiência na Prestação de Serviço – A falha em garantir a segurança desses dados estabelece o nexo causal necessário para a responsabilização da empresa. Inversão do Ônus de Prova – Cabe a organização comprovar que não houve falhas e que houve a adoção de todas as medidas de segurança exigidas na LGPD e pelo Código de Direito do Consumidor.	Dano Presumido – Não é necessário que a vítima prove o sofrimento psicológico. Indenização no valor de R$ 15.000,00 – compensação financeira por danos morais, mas reforçando que revisões dos valores em recursos especiais só ocorrem quando o montante for irrisório ou exorbitante.

Fonte: Elaborado pelo autor (2026) com base em Brasil (2025).

4.4. Flexibilizações da ANPD para Agentes de Tratamento de Pequeno Porte

Reconhecendo as assimetrias de poder econômico, a Autoridade Nacional de Proteção de Dados (ANPD), por meio da Resolução CD/ANPD nº 2/2022, estabeleceu um regime diferenciado para agentes de tratamento de pequeno porte. Tais flexibilizações incluem a dispensa da nomeação obrigatória do DPO (desde que mantido canal de comunicação acessível) e a concessão de prazos em dobro para o atendimento de requisições. Contudo, conforme Silva (2024), essa simplificação procedimental não isenta a organização da responsabilidade civil objetiva em caso de danos.

4.5. Framework de Melhoria Contínua em Governança

Para garantir que a governança digital acompanhe a evolução dos modelos de *Machine Learning*, propõe-se a integração do Ciclo PDCA ao *compliance* estratégico:

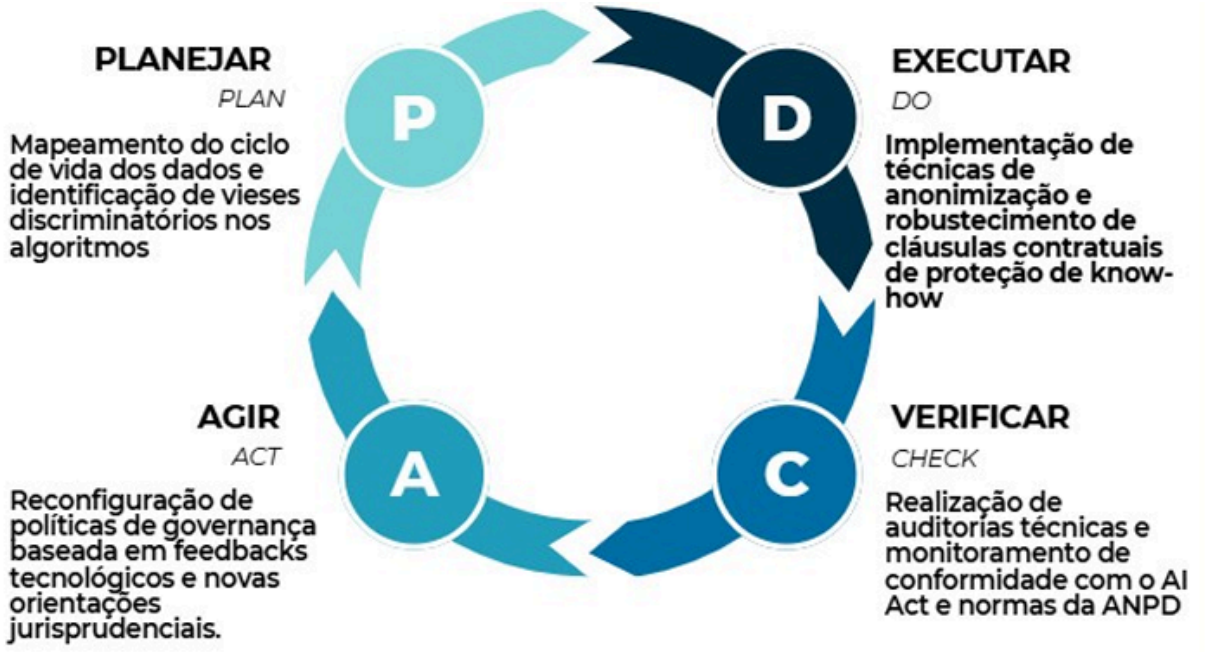
I. **Plan (Planejar):** Mapeamento do ciclo de vida dos dados e identificação de vieses discriminatórios nos algoritmos, esse planejamento deve incluir a Due Diligence Algorítmica para realizar uma investigação profunda.

II. **Do (Executar):** Implementação de técnicas de anonimização e robustecimento de cláusulas contratuais de proteção de *know-how*.

III. **Check (Verificar):** Realização de auditorias técnicas e monitoramento de conformidade com o *AI Act* e normas da ANPD, além do compliance jurídico essa fase vai monitorar a performance dos ativos digitais, avaliando os dados e algoritmos compartilhados na JV, gerando a heterogeneidade de recursos previstas pela DBRV.

IV. **Act (Ajustar):** Reconfiguração de políticas de governança baseada em *feedbacks* tecnológicos e novas orientações jurisprudenciais, permitindo a neutralização de ameaças e reforçando a exclusividade de seus ativos intelectuais. A capacitação dinâmica de orquestração transforma o compliance em uma barreira de entrada para concorrentes.

Figura 1: Integração do Ciclo PDCA ao *compliance* estratégico



Fonte: Elaborado pelo autor (2026)

As barreiras dessa implementação, contudo, variam conforme a natureza dos parceiros, as interrupções na continuidade afetam a credibilidade e legitimidade das ações do Governo, criando a visão no mercado que o governo não conclui as coisas (ZARPELON, 2016). Enquanto a iniciativa privada tem uma cultura de tempo mais escasso para retornos financeiros (SANTOS. 2016). Podemos observar algumas barreiras na tabela abaixo referentes aos entes públicos e privados.

Tabela 3: Comparativo de Barreiras na Cooperação Público-Privada

Dificuldades (Setor Público)	Dificuldades (Setor Privado)
Descontinuidade Política: Alterações de gestão que paralisam projetos de IA de longo prazo.	Miopia de Retorno: Pressão por lucros de curto prazo que compromete a P&D disruptiva.
Lentidão Administrativa: Burocracia legal que reduz a agilidade frente ao ciclo *tech*.	Assimetria de Sigilo: Dificuldade em conciliar a transparência pública com o segredo industrial.
Erosão da Memória Técnica: Alta rotatividade de servidores afetando a orquestração da rede.	Retirada de Capital: Desinvestimento imediato se a vantagem VRIO não for percebida.
A alternância de governo e a descontinuação de programas dificultam a evolução da cooperação com entes públicos	Descontinuação de programas com baixo retorno financeiro e perda de subsidio governamental e incentivos fiscais.

Fonte: Elaborado pelo autor (2026) com base em:Balestrin e Verschoore (2016), Silva (2024), Zarpelon (2016), Santos (2016).

5. CONCLUSÃO/CONSIDERAÇÕES FINAIS

A investigação empreendida permitiu concluir que a vantagem competitiva na era da Inteligência Artificial não advém estritamente da posse da tecnologia, mas da Capacidade Dinâmica de orquestrar parcerias seguras em ecossistemas digitais. A transição da Visão Baseada em Recursos para a Visão Baseada em Recursos Digitais (DRBV) demonstrou que, para PMEs, a formação de *Joint Ventures* não é apenas uma estratégia de ganho de escala, mas uma necessidade existencial para o compartilhamento de ativos de dados e riscos de Pesquisa e Desenvolvimento (P&D).

Os resultados evidenciam que a sustentabilidade dessas alianças está intrinsecamente ligada à robustez da governança digital e ao

compliance algorítmico. A evolução jurisprudencial brasileira, marcada pelo entendimento do STJ sobre o dano moral *in re ipsa* em vazamentos de dados, impõe um novo paradigma de responsabilidade civil objetiva. Nesse cenário, o *framework* proposto integrando o Ciclo PDCA à gestão da privacidade oferece uma trilha para que a conformidade com a LGPD deixe de ser um centro de custos e torne-se um ativo reputacional gerando confiança no mercado.

Do ponto de vista gerencial, as evidências sugerem que os gestores de PMEs devem priorizar a transparência algorítmica e a segregação contratual clara do *know-how* prévio em relação às inovações geradas na parceria. As flexibilizações concedidas pela ANPD para agentes de pequeno porte mitigam barreiras burocráticas, mas não isentam a organização da necessidade de auditorias constantes de viés e segurança. A tecnologia, portanto, atua como propulsora da eficiência desde que amparada por uma estrutura de governança que neutralize o oportunismo pós-contratual e assegure a ética no tratamento de dados.

Como limitações, este estudo pauta-se em uma revisão sistemática e análise documental, o que, embora ofereça rigor teórico, carece de validação empírica em setores específicos da indústria brasileira. Sugere-se, para pesquisas futuras, a realização de estudos de caso múltiplos que analisem a eficácia real das cláusulas de *Privacy by Design* em JVs de tecnologia no Brasil. Em suma, o horizonte da competitividade em rede dos próximos anos será pautado pela inovação e segurança jurídica, a governança digital forma bases solidas para a economia de dados sustentáveis.

REFERÊNCIAS BIBLIOGRÁFICAS

ARAÚJO, G. B. A Lei Geral de Proteção de Dados no comércio eletrônico: impactos e desafios para a proteção ao consumidor no Brasil. Goiânia: Pontifícia Universidade Católica de Goiás, 2024. Artigo científico (Graduação em Direito). Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/7618. Acesso em: 08 mar. 2026.

BALESTRIN, A.; VERSCHOORE, J. R. Ganhos competitivos das empresas em redes de cooperação. Revista de Administração Eletrônica, São Paulo, v. 1, n. 1, art. 2, 2008.

BALESTRIN, A.; VERSCHOORE, J. Redes de cooperação empresarial: estratégias de gestão na nova economia. 2. ed. Porto Alegre: Bookman, 2016.

BARDIN, L. Análise de conteúdo. Tradução de Luís Antero Reto e Augusto Pinheiro. São Paulo: Edições 70, 2016.

BRASIL. [Constituição (1988)]. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais. Brasília, DF: Presidência da República, 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018.

BRASIL. Superior Tribunal de Justiça (3. Turma). Recurso Especial nº 2.121.904 - SP (2024/0031292-7). Relatora: Ministra Nancy Andrighi. Brasília, DF, 11 de fevereiro de 2025. Diário da Justiça Eletrônico Nacional (DJEN), 17 fev. 2025.

BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 2.121.904/SP. Relator: Min. Nancy Andrighi, Terceira Turma, julgado em 11/02/2025, DJe 17/02/2025.

COOPER, H. M. Research synthesis and meta-analysis: a step-by-step approach. 5. ed. Thousand Oaks: Sage Publications, 2017.

DOS SANTOS, R.; EVANGELISTA, M. Impactos da LGPD em pequenas empresas: um estudo multicaso sobre conformidade e resiliência digital. Revista de Gestão e Tecnologia, v. 13, n. 2, p. 88-105, 2023.

EUROPEAN UNION. Artificial Intelligence Act (Regulation (EU) 2024/1689). Official Journal of the European Union, Brussels, L series, 2024. Disponível em: http://data.europa.eu/eli/reg/2024/1689/oj. Acesso em: 15 jan. 2026.

FLORIDI, Luciano. A ética da inteligência artificial: princípios, desafios e oportunidades. 2023.

JACOBIDES, M. G.; CENNAMO, C.; GAWER, A. Towards a theory of ecosystems. Strategic Management Journal, v. 39, n. 8, p. 2255-2276, 2019.

JOBIN, A.; IENCA, M.; VAYENA, E. The global landscape of AI ethics guidelines. Nature Machine Intelligence, v. 1, n. 9, p. 389-399, 2019.

KFOURI, Gustavo Swain; ZAMBÃO, Lara Helena Luiza. CONTRATAÇÕES PÚBLICAS COM FERRAMENTAS DE INTELIGÊNCIA ARTIFICIAL: DESAFIOS ÉTICOS E DE COMPLIANCE. REVISTA JURÍDICA GRALHA AZUL-TJPR, v. 1, n. 28, 2025.

LEITÃO, A. S. Inteligência Artificial e a Reconfiguração da Propriedade Intelectual. 2. ed. São Paulo: Revista dos Tribunais, 2025.

LINGENS, B. et al. Ecosystem design: How firms create and capture value in collaborative networks. Journal of Business Strategy, v. 42, n. 1, p. 1-12, 2021.

MORO, S. C.; GLITZ, F. E. Z. Joint Ventures e alianças estratégicas: uma visão jurídica e gerencial. 2. ed. Curitiba: Juruá, 2013.

NAMBISAN, S. et al. The digital transformation of innovation and entrepreneurship: Progress, challenges and key themes. Research Policy, v. 48, n. 8, p. 103773, 2019.

PEREIRA FILHO, Nivanildo; DE ARAUJO LIMA, Rogerio. Governança algorítmica e políticas públicas: desafios éticos e impactos da inteligência artificial na tomada de decisão governamental. RECIMA21-Revista Científica Multidisciplinar-ISSN 2675-6218, v. 6, n. 1, p. e616051-e616051, 2025.

PINHEIRO, Caroline Rosa; BREGA, Gabriel Ribeiro. Inteligência Artificial e Compliance - A (In)suficiência dos Marcos de Proteção de Dados. Revista Semestral de Direito Empresarial, Rio de Janeiro, n. 28, p. 161-196, jan./jun. 2021

RIALTI, R. et al. Big data analytics capabilities and strategic agility: the mediating role of ambidexterity. Management Decision, v. 58, n. 6, p. 1091-1104, 2020.

RIBEIRO, F.; MOREIRA, L. Governança Digital e Algorítmica: Desafios para as PMEs Brasileiras frente à Economia de Dados. Revista Brasileira de Administração Científica, v. 17, n. 1, p. 45-62, 2026.

SANTOS, Bruna Luiza. Cooperação universidade-empresa. Fatores determinantes para a relação POLO/UFSC e EMBRACO. Revista Iberoamericana de Ciência, Tecnologia e Sociedade - CTS. 2016. P. 127-144.

SILVA, M. A. Estratégia e Orquestração de Ecossistemas na Economia de Dados. Rio de Janeiro: FGV Editora, 2024.

SNYDER, H. Literature review as a research methodology: An overview and guidelines. Journal of Business Research, v. 104, p. 333-339, nov. 2019.

TEECE, D. J. Handover of strategic management to the next generation. Strategic Management Review, v. 1, n. 1, p. 3-45, 2020.

VOLBERDA, H. W. et al. The digital transformation of strategy: A review and research agenda. Long Range Planning, v. 54, n. 5, p. 102-120, 2021.

ZARPELON, Felipe de Mattos. Formação e difusão de redes de cooperação: a análise de uma política pública a partir da lente teórica do trabalho institucional. 2016. Disponível em: http://www.repositorio.jesuita.org.br/handle/UNISINOS/5354. Acesso em 10 abri. 2026

---

[1] Mestre em Gestão e Negócios pela Universidade do Vale do Rio dos Sinos - UNISINOS. E-mail: acesse o artigo original para visualizar o e-mail

[2] Mestra em Direito da Empresa e dos Negócios pela Universidade do Vale do Rio dos Sinos - UNISINOS. E-mail: acesse o artigo original

para visualizar o e-mail