ÁREA TEMÁTICA:

Tecnologia, Inteligência Artificial e Transformação Digital em Administração

COMPLIANCE DIGITAL E LGPD: PROGRAMAS DE INTEGRIDADE NAS ORGANIZAÇÕES COM UTILIZAÇÃO DE INTELIGÊNCIA ARTIFICIAL

Resumo

O presente artigo analisa a convergência entre os programas de integridade corporativa, a Lei Geral de Proteção de Dados Pessoais (LGPD) e a crescente integração da Inteligência Artificial (IA) no ambiente empresarial brasileiro. O estudo se insere no cenário de aumento dos riscos de conformidade e do uso massivo de dados pessoais, no qual as organizações precisam conciliar inovação tecnológica e segurança jurídica. O objetivo geral consiste em investigar como a implementação do compliance digital, amparada por ferramentas de IA, pode assegurar a conformidade normativa e a mitigação de riscos em organizações complexas. A metodologia adotada é a pesquisa bibliográfica de caráter qualitativo, com abordagem exploratória e descritiva, utilizando bases de dados acadêmicas e relatórios setoriais recentes. Os resultados indicam que, embora a IA otimize a detecção de fraudes e a gestão de riscos, sua aplicação exige uma governança algorítmica rigorosa para evitar vieses e garantir a transparência exigida pela LGPD e pelo Projeto de Lei nº 2.338/2023. Conclui-se que o compliance digital não é apenas uma adaptação tecnológica, mas um imperativo ético e regulatório para a sustentabilidade organizacional na era dos dados. A pesquisa contribui ao oferecer um referencial analítico para gestores e profissionais jurídicos na estruturação de programas de integridade apoiados por IA, além de fomentar o debate acadêmico sobre a governança algorítmica no contexto da LGPD.

Palavras-chave: Compliance Digital. LGPD. Inteligência Artificial. Governança Corporativa. PL 2338/2023.

Abstract

This article analyzes the convergence between corporate compliance programs, the General Data Protection Law (LGPD), and the growing integration of Artificial Intelligence (AI) in the Brazilian business environment. The study is set in the context of increasing compliance risks and the massive use of personal data, where organizations need to balance technological innovation and legal security. The main objective is to investigate how implementing digital compliance, supported by AI tools, can ensure regulatory compliance and risk mitigation in complex organizations. The methodology

used is qualitative bibliographic research, with an exploratory and descriptive approach, using academic databases and recent sector reports. The results indicate that, although AI optimizes fraud detection and risk management, its application requires strict algorithmic governance to avoid biases and ensure transparency required by the LGPD and Bill No. 2,338/2023. It is concluded that digital compliance is not just a technological adaptation, but an ethical and regulatory imperative for organizational sustainability in the data era. The research contributes by providing an analytical framework for managers and legal professionals in structuring integrity programs supported by AI, as well as encouraging academic debate on algorithmic governance in the context of the LGPD. Keywords: Digital Compliance. LGPD. Artificial Intelligence. Corporate Governance. Bill 2338/2023.

Keywords: Digital Compliance. LGPD. Artificial Intelligence. Corporate Governance. Bill 2338/2023.

1. Introdução

A transformação digital acelerada reconfigurou as estruturas de controle interno, exigindo que as organizações transcendam o compliance tradicional em direção a modelos dinâmicos de integridade. No cenário brasileiro, essa evolução é impulsionada pela necessidade de adequação à Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018) e pela adoção massiva de sistemas de Inteligência Artificial (IA) para o processamento de grandes volumes de informações. O contexto atual revela que a conformidade não se limita mais ao cumprimento de normas estáticas, mas à gestão proativa de riscos digitais que emergem da automação e do tratamento de dados em larga escala. Dados do Cetic.br (2026) indicam que a adoção de IA em empresas brasileiras atingiu 17% em 2025, com as grandes corporações alcançando 50% de implementação, evidenciando a urgência de se pensar a integridade organizacional sob uma perspectiva digital.

O problema central desta pesquisa reside na tensão entre a eficiência operacional proporcionada pela IA e os riscos de opacidade algorítmica e violação de privacidade. À medida que os sistemas de IA assumem funções críticas de monitoramento e tomada de decisão, questões como viés algorítmico, falta de explicabilidade e uso indevido de dados pessoais tornam-se desafios concretos para os programas de compliance. Diante disso, o objetivo geral deste estudo é analisar os mecanismos de implantação de programas de integridade digital que harmonizem a utilização de tecnologias disruptivas com os princípios da LGPD. Como objetivos específicos, busca-se: (i) conceituar o instituto do compliance, sua evolução histórica e o compliance digital; (ii) analisar o papel das normas de governança na mitigação dos riscos éticos e jurídicos; (iii) mapear os riscos éticos e jurídicos sob o enfoque da LGPD em processos de conformidade com IA; e (iv) investigar as aplicações

da IA nos processos de compliance e avaliar os impactos do PL 2338/2023 sobre as organizações brasileiras.

A lacuna de pesquisa identificada refere-se à necessidade de diretrizes práticas que conectem o arcabouço jurídico da LGPD com as exigências regulatórias emergentes do Marco Legal da IA (PL 2338/2023). Embora a literatura sobre compliance seja vasta, e a produção acadêmica sobre IA seja igualmente robusta, a integração específica entre governança algorítmica e programas de integridade no setor privado brasileiro ainda carece de uma sistematização que considere tanto os dados recentes de adoção tecnológica quanto o estágio atual da regulação da IA no país. Este artigo propõe-se a preencher parte desse vácuo, oferecendo uma visão interdisciplinar que dialoga com o Direito, a Gestão Empresarial e a Tecnologia da Informação, a partir de fontes atualizadas até o primeiro semestre de 2026.

A justificativa para este trabalho fundamenta-se na relevância socioeconômica do tema. Com o aumento das sanções administrativas aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD) e a iminente regulação específica da IA no Brasil, as organizações que negligenciarem a estruturação de um compliance digital robusto estarão expostas a riscos reputacionais, financeiros e jurídicos severos. Pesquisa da EY (2026) revela que 95% das empresas líderes no Brasil já utilizam IA em algum grau, e 74% dos executivos brasileiros consideram a adaptação à IA como prioridade estratégica (LinkedIn, 2025). Este cenário torna imperativo que a academia produza reflexões críticas sobre como conciliar inovação com responsabilidade corporativa. Portanto, o estudo contribui para o debate acadêmico e profissional ao fornecer subsídios para a construção de sistemas de integridade resilientes, éticos e alinhados às exigências contemporâneas.

2. Definições e conceitos de compliance

O termo compliance, originado do verbo inglês *to comply*, significa agir de acordo com a lei, uma instrução interna, um comando ou uma conduta ética. No âmbito corporativo, conforme leciona Venturini (2025), o compliance não pode ser interpretado de forma literal, pois seu alcance é mais amplo e deve ser observado pelas organizações de maneira sistêmica, como um instrumento de mitigação de riscos, preservação dos valores éticos e de sustentabilidade corporativa. Bertoccelli (2024) complementa que o compliance integra um sistema complexo e organizado de procedimentos de controle de riscos e preservação de valores intangíveis, que devem ser coerentes com a estrutura societária e contar com compromisso efetivo da liderança.

Os professores Silveira e Saad-Diniz (2015 apud Bertoccelli, 2024, p. 38) conceituam compliance como uma orientação preventiva, por meio da programação de condutas que estimulam a diminuição dos riscos da atividade. Sua estrutura é pensada para incrementar a capacidade comunicativa da pena

nas relações econômicas, ao combinar estratégias de defesa da concorrência leal com a prevenção de perigos futuros. Nesse sentido, Saavedra (2019, apud Azzari; Chiarello; Scalisse, 2020, p. 460) estabelece que o compliance cria uma relação entre um "estado de conformidade" e uma "orientação de comportamento" baseada em norma jurídica, cuja designação varia conforme a área do direito na qual se insere.

A doutrina moderna enfatiza que o compliance transcende a mera obediência cega a regras. Trata-se de uma cultura de integridade que permeia todos os níveis da organização. Almeida (2025) argumenta que o compliance efetivo deve ser capaz de detectar desvios antes que eles se tornem violações sistêmicas, utilizando para isso mecanismos de monitoramento contínuo e canais de denúncia protegidos. A integração tecnológica, portanto, surge como um facilitador dessa vigilância ética, permitindo que o *Compliance Officer* atue de forma preditiva e não apenas reativa diante das inconformidades.

2.1 EVOLUÇÃO HISTÓRICA DO COMPLIANCE

Nos Estados Unidos, na década de 1970, o *Foreign Corrupt Practices Act* (FCPA) surgiu após escândalos envolvendo doações corporativas para funcionários públicos, subornos e propinas, como os casos Watergate e Lockheed Martin Aircraft Corporation (Bertoccelli, 2024). A FCPA tornou-se o diploma de maior influência na comunidade internacional, que se viu obrigada a adotar medidas com o mesmo propósito, culminando na Convenção de Luta contra a Corrupção de Agentes Públicos Estrangeiros nas Transações Comerciais da OCDE (Cavalleri, 2020).

No Reino Unido, a *UK Bribery Act* de 2010 reformulou o sistema anticorrupção e estabeleceu seis princípios fundamentais para programas de compliance robustos: (i) proporcionalidade dos procedimentos de acordo com os riscos; (ii) comprometimento da alta administração; (iii) avaliação periódica de riscos (*risk assessment*); (iv) procedimentos constantes de *due diligence*; (v) comunicação e treinamento; e (vi) monitoramento e revisão periódica (Bertoccelli, 2024). Esses princípios tornaram-se referência global para a estruturação de programas de integridade.

A evolução histórica demonstra que o compliance nasceu de crises de confiança e falhas éticas monumentais. Cada novo marco regulatório internacional foi uma resposta direta à incapacidade das empresas de se autorregularem de forma eficaz. No século XXI, a evolução migra do combate à corrupção financeira para a proteção da integridade digital e dos dados pessoais, refletindo a mudança da base da economia global, que passou de ativos físicos para ativos informacionais e algorítmicos.

2.2 O COMPLIANCE NO BRASIL

No Brasil, o compliance era utilizado apenas por grandes organizações multinacionais, instituições financeiras e de saúde. A partir de 2013, com os movimentos sociais contra a corrupção, tornou-se um mecanismo de blindagem das relações empresariais (Bertoccelli, 2024). Almeida (2025) destaca que a consolidação do compliance nacional ocorreu com a Lei nº 12.846/2013 (Lei Anticorrupção) e o Decreto Federal nº 11.129/2022, que atualizou as exigências para os programas de integridade, valorizando a análise de riscos e o apoio incondicional da alta administração.

O sistema legal brasileiro de defesa da moralidade passou a exigir a adoção de mecanismos internos de integridade e a aplicação efetiva de códigos de ética, utilizados como dosimetria na aplicação de sanções administrativas (Moreira Neto apud Bertoccelli, 2024, p. 45). Esse arcabouço inclui a Lei de Improbidade Administrativa (Lei 8.429/92), a Nova Lei de Licitações (Lei 14.133/21) e o Estatuto Jurídico da Empresa Pública (Lei 13.303/16). A Controladoria-Geral da União (CGU) estabeleceu as atividades de alto risco que devem ser priorizadas pelos programas de integridade: participação em licitações, obtenção de licenças, contato com agentes públicos, contratação com terceiros, fusões e aquisições, entre outras (BRASIL, 2016).

A maturidade do compliance brasileiro é testada agora pela necessidade de integrar a proteção de dados pessoais. A conformidade não é mais um "adicional" para empresas que contratam com o poder público, mas uma condição de existência no mercado privado. A Lei Anticorrupção brasileira, ao prever a responsabilidade objetiva das pessoas jurídicas, criou um incentivo econômico direto para a implementação de programas de integridade reais, uma vez que a existência de um programa efetivo pode reduzir significativamente o valor das multas aplicadas em caso de ilícitos.

2.3 GOVERNANÇA CORPORATIVA

A governança corporativa, conforme o Instituto Brasileiro de Governança Corporativa (IBGC, 2023), é o sistema pelo qual as empresas são dirigidas e monitoradas, envolvendo o relacionamento entre sócios, conselho de administração, diretoria e órgãos de fiscalização. Seus princípios fundamentais são: transparência, equidade, prestação de contas (*accountability*) e responsabilidade corporativa. Belisario (2025) destaca que sem uma governança sólida, os programas de compliance tornam-se meros instrumentos formais, sem impacto real na cultura organizacional.

Segundo Almeida (2025), as ações de governança em face das funções de compliance são mecanismos para evitar conflitos, monitorar ações dos dirigentes e mitigar riscos de não atendimento às normas. No contexto digital, a governança corporativa ganha novas dimensões, pois passa a exigir o

controle não apenas sobre processos humanos, mas também sobre decisões automatizadas tomadas por sistemas de IA, criando a necessidade de uma governança algorítmica como extensão natural da governança tradicional.

Conforme Galvão (2023), o dever de diligência dos administradores, previsto no art. 153 da Lei nº 6.404/1976, passa a compreender um novo subdever: o de implementar programas de compliance e estruturas de governança aptas a mitigar ou corrigir a discriminação algorítmica produzida por sistemas de inteligência artificial.

2.4 GOVERNANÇA DE DADOS E LGPD

A governança de dados, ou governança digital, pode ser definida como a estruturação de processos e políticas internas com o objetivo de conferir proteção aos dados pessoais. Cavalieri (2025) descreve a governança de dados como responsável por gerir os princípios de organização e controle de dados e informações, constituindo um ramo da governança voltado especificamente para a proteção de dados pessoais.

A LGPD (Lei nº 13.709/2018) estabelece princípios fundamentais como finalidade, adequação, necessidade, transparência, não discriminação e responsabilização. Em seu art. 44, a lei é clara acerca da importância do compliance no tratamento de dados, sob pena de responsabilização quando se deixar de observar a legislação. A Resolução CD/ANPD nº 4/2023 instituiu a obrigatoriedade do programa de governança em privacidade, definindo parâmetros para sanções e critérios para irregularidades (Venturini, 2025).

Carvalho (2025) enfatiza que o *Privacy by Design* deve ser a premissa de qualquer novo projeto tecnológico, integrando a proteção de dados desde a concepção dos sistemas. Os requisitos mínimos do programa de compliance digital incluem: comprometimento do controlador, aplicabilidade a todo conjunto de dados sob controle, adaptação à estrutura e escala das operações, avaliação sistemática de impactos e riscos, estabelecimento de relação de confiança com o titular, integração à governança geral, planos de resposta a incidentes e atualização constante (BRASIL, 2018).

2.5 COMPLIANCE DIGITAL E INTELIGÊNCIA ARTIFICIAL

O compliance digital contempla duas perspectivas fundamentais. Sob a perspectiva jurídica, há a exigência legal de adoção de mecanismos de governança, sob pena de responsabilização. Enquanto metodologia de gestão de processos, há práticas especificamente desenvolvidas para o ambiente digital (Venturini, 2025). Na evolução e cruzamento dessas perspectivas, torna-se indispensável o uso de algoritmos e instrumentos de IA para monitorar e regular a própria IA.

Boter, Menezes e Silva (2025) esclarecem que a integração de tecnologias emergentes ao compliance não é apenas uma vantagem

competitiva, mas uma necessidade para garantir a eficácia na detecção e mitigação de riscos. A automação proporcionada pela IA permite que as equipes de compliance superem tarefas manuais e repetitivas, concentrando-se em atividades de maior valor estratégico. Ferramentas como *Compliance Management Systems* (CMS), *Big Data analytics*, *data mining* e algoritmos de *machine learning* e *deep learning* são utilizados para detecção de fraudes financeiras, lavagem de dinheiro e corrupção.

No entanto, a IA enfrenta situações contraditórias: enquanto desempenha atividades complexas em níveis sobre-humanos, comete erros primários e gera resultados sem sentido ou dados inverídicos (Dias; Ferreira, 2023).

Conforme Cavalcante (2026), a governança algorítmica demanda mecanismos estáveis de autocontrole ético por parte das instituições, capazes de alinhar inovação tecnológica, justiça social e sustentabilidade, uma vez que as decisões mediadas por algoritmos podem produzir vieses invisíveis e reduzir a transparência pública.

2.6 O PAPEL DO COMPLIANCE OFFICER NA ERA DA IA

O perfil do profissional de compliance está em profunda transformação. Não basta mais o conhecimento jurídico ou contábil; exige-se agora uma literacia digital mínima para dialogar com as áreas de tecnologia. Venturini (2025) aponta que o *Compliance Officer* deve atuar como um tradutor entre as exigências regulatórias e as possibilidades técnicas, garantindo que a inovação não ocorra às custas da conformidade.

Conforme Almada e Maranhão (2023), a LGPD estabelece um direito à revisão de decisões automatizadas (art. 20), cuja adequada proteção do titular de dados exige o desenvolvimento de padrões e diretrizes próprios da realidade brasileira — o que impõe às organizações estruturas capazes de auditar e contestar os critérios adotados pelos sistemas.

Dados do Netskope Threat Labs Report Brasil 2026 indicam que 64% das violações de políticas de dados em aplicações de IA generativa no país envolvem dados sensíveis e regulamentados — informações de clientes, registros financeiros e contratos sujeitos a normas de conformidade —, além de código-fonte (21%), senhas e chaves de API (9%) e propriedade intelectual (7%) (Ravagnani, 2026).

2.7 TRANSPARÊNCIA E EXPLICABILIDADE ALGORÍTMICA

A transparência é um dos pilares da LGPD (art. 6º, VI) e um dos maiores desafios técnicos da IA contemporânea. Muitos modelos de *deep learning* operam como "caixas-pretas", onde a lógica interna da decisão é inacessível ao entendimento humano direto. Bertoccelli (2024) argumenta que a falta de

transparência é um risco de compliance inaceitável, pois impede o exercício do direito de revisão de decisões automatizadas previsto no art. 20 da LGPD.

Conforme Morato, Nunes e Tavares (2026), a inteligência artificial explicável (XAI) constitui abordagem técnica que viabiliza o direito à explicação, consolidando-se como princípio estruturante para assegurar transparência e responsabilidade em decisões automatizadas — mecanismo essencial para mitigar os riscos da opacidade algorítmica, como vieses e falhas.

A inteligência artificial explicável (XAI) segundo Oliveira Filho (2026) constitui requisito de transparência e governança para sistemas de informação, na medida em que a auditabilidade dos modelos — a capacidade de verificar a origem de erros e a conformidade com a legislação — depende da possibilidade de explicar as decisões algorítmicas.

2.9 ÉTICA E VIÉS NOS SISTEMAS DE DECISÃO AUTOMATIZADA

A ética algorítmica investiga como os valores humanos são codificados em sistemas computacionais. Kfouri e Zambão (2025) alertam que o viés não é apenas um erro técnico, mas muitas vezes um reflexo de preconceitos estruturais presentes nos dados de treinamento. Se uma IA de recrutamento é treinada com dados de uma empresa que historicamente contratou apenas homens para cargos de liderança, o algoritmo aprenderá que ser homem é um requisito para o sucesso, discriminando candidatas qualificadas.

Lacerda (2023), apresenta que as auditorias de sistemas automatizados constituem ferramenta essencial de regulação da inteligência artificial, devendo ser conduzidas por pessoas naturais supervisionando sistemas automatizados e estruturadas em três dimensões — governança, modelo e aplicação —, a fim de verificar a existência de efeitos discriminatórios no funcionamento dos algoritmos, nos termos do art. 20 da LGPD.

Conforme Santos, Baldassarre e Magalhães (2026), a diversidade das equipes de desenvolvimento atua como salvaguarda contra vieses algorítmicos, na medida em que diversifica as perspectivas para identificação de desvios, promove a empatia no desenvolvimento e contribui para enfrentar a discriminação sistêmica — o que evidencia que a justiça algorítmica não pode ser assegurada apenas por intervenções técnicas, mas exige fatores sociais e organizacionais.

2.10 SEGURANÇA DA INFORMAÇÃO E RESILIÊNCIA CIBERNÉTICA

O art. 46 da LGPD estabelece que "os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito" (CONFIDATA, 2025).

Moreira *et al.* (2024), apontam que sistemas baseados em aprendizado de máquina podem ser vulneráveis a ataques adversariais, sendo o roubo de modelo uma técnica que permite ao atacante extrair informações internas do sistema — inclusive dados sensíveis — por meio de abordagens caixa-preta, sem conhecimento prévio do modelo alvo.

O'Brien, Ee e Williams (2023), afirmam que o desligamento de emergência (emergency shutdown) é um mecanismo comum em áreas onde a operação continuada pode resultar em danos catastróficos, sendo o objetivo intervir rapidamente para impedir que uma falha existente se transforme em um desfecho catastrófico — o que exige, no contexto da IA, planos de resposta a incidentes documentados que definam claramente papéis, responsabilidades e autoridade para a tomada de decisão.

Metcalf e Churilla (2026), apontam que a cadeia de custódia criptográfica, combinada com metadados detalhados de cada item de dados, proporciona garantias de integridade e privacidade, tornando mais difícil para um adversário modificar os dados sem ser notado — o que torna o processo de treinamento de modelos robusto contra ataques de envenenamento.

2.11 O IMPACTO DA IA GENERATIVA NO AMBIENTE COORPORATIVO

A popularização de ferramentas como o ChatGPT e similares trouxe desafios inéditos para o compliance. Funcionários utilizam essas ferramentas para redigir e-mails, analisar contratos e gerar códigos de programação, muitas vezes inserindo dados sensíveis da empresa em servidores de terceiros. Venturini (2025) destaca que o uso não regulamentado de IA generativa pode configurar violação de propriedade intelectual e quebra de confidencialidade.

Conforme Desai *et al*. (2026), o uso empresarial de modelos de linguagem exige mecanismos de proteção contra o vazamento de dados confidenciais, incluindo a detecção e redação de informações sensíveis antes de entrarem no modelo — o que reforça a necessidade de instâncias privadas e seguras e de políticas adaptativas de uso.

Conforme Abdullahi, Danyaro e Chiroma (2026), os grandes modelos de linguagem (LLMs) apresentam uma tendência a gerar informações imprecisas ou fabricadas — as chamadas alucinações —, o que representa sérios desafios à confiabilidade e à confiança dos usuários, exigindo o desenvolvimento de soluções robustas e sensíveis ao contexto para mitigação.

2.12 RESPONSALIDADE CIVIL E DECISÕES AUTOMATIZADAS

Conforme Cardoso e Melo (2024), a LGPD é compreendida como um marco regulatório transversal aplicável à inteligência artificial, de modo que o direito à revisão de decisões automatizadas (art. 20) e as regras de responsabilidade (art. 42) se aplicam aos sistemas de IA — ainda que a lei não contenha disposições específicas sobre a tecnologia.

Conforme Manso e Junqueira Calixto (2024), o PL nº 2.338/2023 delineia regimes de responsabilização civil específicos para danos causados por sistemas de inteligência artificial, antecipando questões e dificuldades a serem enfrentadas tanto pelos agentes da cadeia de desenvolvimento e operação quanto pelas vítimas de sistemas de IA — o que exige posturas adequadas dos agentes e das autoridades para o funcionamento equilibrado do sistema de responsabilidade proposto.

Conforme Amorim e Sant'Anna (2025), a existência de programas de integridade é levada em consideração no momento de aplicação das sanções (art. 7º da Lei Anticorrupção), mas, para que sirvam de atenuante, é necessário comprovar que as medidas possuem capacidade de prevenir, detectar e sanar atos ilícitos — o que exige documentação e parâmetros objetivos de efetividade.

3. METODOLOGIA

A presente pesquisa adota abordagem qualitativa, com investigação de fenômenos sociais e jurídicos por meio de análise de dados subjetivos, visando obter compreensão aprofundada do compliance digital e da IA no contexto organizacional brasileiro. Quanto aos fins, classifica-se como descritivo-exploratória, pois busca familiarizar-se com o tema e identificar tendências, problemas e oportunidades em razão da diversidade de assuntos que envolvem o compliance digital com a atuação da IA (UNESP, 2023).

O levantamento de dados foi realizado entre janeiro e julho de 2026, abrangendo o período de recorte temporal de 2020 a 2026. Esse recorte justifica-se pela necessidade de capturar a evolução normativa da LGPD (vigente desde 2020), os avanços recentes da IA generativa (que ganhou destaque a partir de 2023) e a tramitação do PL 2338/2023. A escolha deste intervalo permite uma análise contemporânea que reflete o estado da arte da tecnologia e da regulação no Brasil.

As bases de dados consultadas incluíram: Google Acadêmico (Google Scholar), Portal de Periódicos CAPES, RECIMA21, Index Law Journals, Revista de Gestão e Secretariado (GeSec), Revista de Direito Brasileira (RDB) e os anais do Latin American Symposium on Digital Government (LASDiGov). Foram também consultados relatórios setoriais de consultorias internacionais (EY, McKinsey) e dados oficiais do Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), garantindo uma base de dados híbrida entre teoria acadêmica e prática de mercado.

As palavras-chave utilizadas nas buscas, em português e inglês, foram: "Compliance Digital", "LGPD", "Inteligência Artificial", "Governança Corporativa", "Governança Algorítmica", "PL 2338/2023", "Digital Compliance", "AI Governance", "Algorithmic Due Diligence". Foram aplicados operadores booleanos (AND, OR) para cruzar os termos e refinar os resultados,

priorizando publicações que tratassem da interseção entre ao menos dois desses eixos temáticos.

Como critérios de inclusão, foram selecionados: artigos publicados em periódicos com revisão por pares, livros e manuais de referência na área do compliance, legislação brasileira vigente, relatórios técnicos de instituições de pesquisa e consultorias reconhecidas, e publicações que abordassem diretamente a interseção entre compliance, proteção de dados e inteligência artificial. Foram excluídos: textos meramente opinativos ou sem fundamentação jurídica e técnica comprovada, publicações anteriores a 2020 (exceto marcos legais históricos), e artigos cujo foco não incluísse o contexto brasileiro ou a aplicação corporativa.

A análise dos dados seguiu a técnica de análise de conteúdo, conforme proposta por Bardin (2016), onde as informações foram organizadas em três categorias temáticas: (i) marcos regulatórios — abrangendo a LGPD, a Lei Anticorrupção e o PL 2338/2023; (ii) riscos tecnológicos — incluindo viés algorítmico, opacidade, segurança de dados e responsabilidade civil; e (iii) estratégias de implementação — contemplando governança de dados, Privacy by Design, due diligence algorítmica e supervisão humana. Essa estrutura permitiu o cruzamento sistemático entre as exigências legais e as capacidades técnicas das ferramentas de IA disponíveis no mercado.

4. Análise e Discussão dos Resultados

A discussão dos resultados foi organizada de forma a examinar as múltiplas dimensões da integração entre inteligência artificial e compliance digital, abordando as interfaces com a Lei Geral de Proteção de Dados (LGPD), os riscos jurídicos e éticos, a governança algorítmica, a adoção da IA no contexto brasileiro, os mecanismos de due diligence e auditoria contínua, a gestão de terceiros, o papel da Autoridade Nacional de Proteção de Dados (ANPD), o fortalecimento da cultura de integridade e as perspectivas futuras decorrentes da utilização de IA generativa e agentes autônomos nas organizações.

4.1 LGPD E RISCOS DA IA: INTERSEÇÕES E CRÍTICAS

A análise dos dados demonstra que a implementação do compliance digital no Brasil atravessa um momento de transição crítica. A convergência entre a LGPD e a IA cria um campo de tensões que exige uma nova arquitetura de controle. Para ilustrar essa interseção, apresenta-se o cruzamento entre os princípios da LGPD e os riscos inerentes à utilização de sistemas de IA:

Quadro 1 — Cruzamento entre princípios da LGPD e riscos da IA

Princípio LGPD	Risco Associado à IA	Medida de Mitigação (Compliance Digital)
Finalidade (art. 6º, I)	Reutilização indevida de dados pessoais para treinamento de modelos sem consentimento	Data Mapping obrigatório; políticas de retenção e descarte; segregação de bases
Adequação (art. 6º, II)	Uso de dados para finalidades incompatíveis com a coleta original	Contratos com cláusulas específicas de tratamento; revisão de termos de uso
Necessidade (art. 6º, III)	Coleta excessiva de dados para alimentar algoritmos	Minimização de dados; Privacy by Design; revisão periódica de datasets
Transparência (art. 6º, VI)	Opacidade algorítmica ("caixa-preta")	Implementação de IA Explicável (XAI); relatórios de impacto
Não discriminação (art. 6º, IX)	Vieses algorítmicos que perpetuam discriminações	Auditoria periódica de viéses; diversidade nas bases de treinamento
Segurança (art. 6º, VII)	Ataques adversários, vazamentos e envenenamento de dados	Criptografia, testes de intrusão em modelos; monitoramento contínuo
Responsabilização (art. 6º, X)	Dificuldade de atribuir responsabilidade por decisões automatizadas	Supervisão humana obrigatória (human-in-the-loop); registro de decisões

FONTE: Os autores (2026)

Cada uma dessas interseções representa um ponto crítico que o compliance digital precisa endereçar. Por exemplo, a opacidade algorítmica viola diretamente o princípio da transparência da LGPD, que garante ao titular o direito de saber como seus dados são tratados. Sistemas de IA que operam como "caixas-pretas" — onde nem mesmo os desenvolvedores conseguem explicar como uma decisão foi tomada — são juridicamente incompatíveis com a LGPD e com as exigências do PL 2338/2023.

A mitigação desses riscos exige uma mudança de paradigma: o compliance deixa de ser um checklist de documentos para se tornar um processo de engenharia jurídica. O *Privacy by Design*, citado por Carvalho (2025), deve ser estendido para o *Ethics by Design* e *Compliance by Design*. Isso significa que os requisitos legais devem ser traduzidos em requisitos

funcionais do sistema, garantindo que a conformidade seja uma característica intrínseca da tecnologia e não um remendo posterior.

4.2 O CENÁRIO BRASILEIRO DE ADOÇAO DE IA E SEUS IMPACTOS NO COMPLIENCE

Os dados coletados revelam um cenário de rápida digitalização. Conforme o Cetic.br (2026), a adoção de IA por empresas brasileiras atingiu 17% em 2025, com crescimento de 4 pontos percentuais em relação a 2024. Nas grandes empresas (250+ funcionários), o índice saltou de 38% para 50% no mesmo período. A pesquisa da McKinsey (2026) aponta um crescimento ainda mais acelerado, de 30% ao ano na adoção de IA no Brasil.

A EY (2026), em seu *AI Sentiment Index*, coloca o Brasil em posição de destaque global, com 95% das empresas pesquisadas declarando utilizar IA de alguma forma — contra uma média global de 85%. Destaca-se que 21% das empresas brasileiras já utilizam agentes autônomos de IA, sistemas que operam com mínima intervenção humana. Esse dado é particularmente relevante para o compliance digital, pois agentes autônomos tomam decisões que podem ter impactos jurídicos significativos sem supervisão humana direta.

O que esses números significam para o compliance digital? Primeiro, confirmam que a IA não é mais uma promessa futura, mas uma realidade presente na maioria das grandes organizações brasileiras. Isso implica que os programas de compliance precisam, urgentemente, incorporar auditoria algorítmica e governança de dados como componentes centrais. Segundo, revelam uma assimetria preocupante: enquanto a adoção tecnológica avança rapidamente, a maturidade regulatória e a estruturação de controles internos para IA ainda são incipientes. Como alertam Boter, Menezes e Silva (2025), a integração de IA ao compliance deve vir acompanhada de supervisão humana de profissionais capacitados e correção contínua dos modelos.

4.3 DUE DILIGENCE ALGORÍTMICA E EXMPLOS PRÁTICOS

A *due diligence*, tradicionalmente aplicada a processos de fusões e aquisições e verificação de terceiros, ganha novo contorno no ambiente digital. Kfouri e Zambão (2025) propõem o conceito de *due diligence algorítmica*: a avaliação prévia de sistemas automatizados para identificar riscos éticos, jurídicos e operacionais antes de sua implementação. Esse processo envolve a análise de: (i) qualidade e representatividade das bases de dados de treinamento; (ii) existência de vieses discriminatórios; (iii) capacidade de explicabilidade do modelo; (iv) conformidade com a LGPD e com os direitos dos titulares; e (v) mecanismos de supervisão humana.

Exemplos práticos de aplicação da IA no compliance digital incluem o *screening* de fornecedores e terceiros. Ferramentas de *data mining* permitem cruzar informações de milhões de empresas em segundos, identificando conexões com pessoas politicamente expostas (PEPs), sanções

internacionais, processos judiciais e inadimplência. Sistemas de IA generativa podem, ainda, redigir relatórios preliminares de *due diligence*, acelerando o processo e permitindo que a equipe humana se concentre na análise qualitativa dos riscos detectados (Boter; Menezes; Silva, 2025).

Outra aplicação vital é o monitoramento de transações em tempo real. Algoritmos de *machine learning* analisam transações financeiras continuamente, identificando padrões suspeitos de lavagem de dinheiro, corrupção ou fraudes. Esses sistemas aprendem com o histórico e se adaptam a novos padrões, superando a capacidade de sistemas baseados em regras fixas. No entanto, o compliance deve garantir que esses sistemas não gerem exclusão financeira injustificada por meio de falsos positivos baseados em perfis socioeconômicos, o que exigiria a revisão humana prevista na LGPD.

4.4 ANÁLISE DO PL 2338/2023 E SEUS IMPACTOS NAS ORGANIZAÇÕES

O Projeto de Lei nº 2.338/2023 é a proposta mais avançada de regulamentação da IA no Brasil. Aprovado pelo Senado Federal em dezembro de 2024 e encaminhado à Câmara dos Deputados em 2025, o PL estabelece normas gerais para o desenvolvimento, implementação e uso responsável de sistemas de IA no Brasil (BRASIL, 2023). Sua estrutura é baseada em uma classificação de riscos em cinco níveis, inspirada no modelo do *EU AI Act*, o que facilita a conformidade para empresas multinacionais.

Para as organizações que utilizam IA em processos de compliance, o PL 2338/2023 traz implicações diretas. Sistemas de IA utilizados para monitoramento de conformidade, detecção de fraudes e avaliação de riscos podem ser classificados como de alto risco, dependendo de sua aplicação, o que exigirá avaliações de impacto algorítmico e transparência. Além disso, o PL estabelece o direito à explicação — a pessoa afetada por uma decisão automatizada tem o direito de receber explicações claras sobre os critérios utilizados, reforçando a necessidade de implementar sistemas de IA explicável (XAI).

O PL prevê ainda a criação de um Sistema de Governança e Ética em IA, com a participação de órgãos reguladores e sociedade civil. As organizações precisarão adaptar seus programas de integridade para incorporar as diretrizes desse sistema. A INDEX LAW (2025) destaca que o Conselho de Administração deve assumir a responsabilidade pela supervisão dos sistemas de IA, criando comitês especializados e assegurando a implementação de políticas de IA ética. A governança algorítmica deixa de ser uma questão técnica de TI para se tornar uma pauta estratégica do *board*.

4.5 DESSAFIOS ÉTICOS E A NECESSIDADE DE SUPERVISÃO HUMANA

A fronteira mais complexa do compliance digital reside nos desafios éticos. A explicabilidade — capacidade de explicar como e por que uma IA

tomou determinada decisão — é um requisito tanto ético quanto legal. Dias e Ferreira (2023) apontam que a IA enfrenta situações contraditórias, desempenhando atividades complexas em níveis sobre-humanos enquanto comete erros primários ou gera dados inverídicos (alucinações). Sem supervisão humana, esses erros podem se tornar violações sistêmicas de compliance.

O viés algorítmico é outra preocupação central. Se os dados históricos utilizados para treinar modelos de IA refletem discriminações passadas, o sistema pode perpetuar e ampliar essas injustiças. Kfouri e Zambão (2025) destacam que algoritmos na administração pública podem levar a decisões discriminatórias, impactando a equidade e a justiça dos processos. No setor privado, sistemas de IA utilizados para recrutamento, concessão de crédito ou análise de riscos podem reproduzir vieses raciais, de gênero ou socioeconomicamente discriminatórios, violando o princípio da não discriminação da LGPD.

O compliance digital, portanto, deve garantir que a "vontade do algoritmo" esteja sempre subordinada às diretrizes éticas da companhia e ao ordenamento jurídico vigente. Isso significa que não basta que a IA seja eficiente — ela precisa ser justa, transparente e auditável. Como sintetizam Boter, Menezes e Silva (2025), a automação proporcionada pela IA possibilita que as equipes de compliance superem tarefas manuais e repetitivas, permitindo que se concentrem em atividades de maior valor estratégico. A tecnologia amplifica a capacidade humana, mas não a substitui no julgamento ético final.

A transição do compliance episódico para o compliance contínuo é uma das maiores vantagens da IA. Sistemas de CMS modernos utilizam algoritmos para monitorar o cumprimento de políticas internas 24 horas por dia, 7 dias por semana. Isso reduz drasticamente a janela de oportunidade para fraudes e erros, permitindo intervenções quase imediatas. No entanto, a implementação desses sistemas exige que a empresa tenha uma infraestrutura de dados organizada e integrada.

A auditoria contínua permite que a empresa identifique tendências de risco antes que elas se materializem em incidentes. Por exemplo, um aumento súbito em transações com um determinado fornecedor em uma região de alto risco pode disparar um alerta automático para investigação. Essa proatividade é valorizada pelos reguladores e pode servir como prova de efetividade do programa de integridade em processos administrativos ou judiciais.

Contudo, o excesso de alertas (fadiga de alertas) pode ser um risco. Se o sistema gera milhares de notificações irrelevantes, a equipe de compliance pode ignorar alertas críticos. O ajuste fino (*fine-tuning*) dos algoritmos de monitoramento é uma tarefa constante que exige colaboração entre especialistas em dados e profissionais de compliance. A eficácia do CMS depende da qualidade das regras de negócio e dos dados que o alimentam.

4.6 GESTÃO DE TERCEIROS E A CADEIA DE SUPRIMENTOS DIGITAL

O compliance digital não se encerra nos muros da organização. A LGPD e a Lei Anticorrupção impõem responsabilidades sobre as ações de terceiros que atuam em nome da empresa. Na era da IA, isso inclui fornecedores de software como serviço (SaaS), provedores de nuvem e desenvolvedores de algoritmos. A *due diligence* de terceiros deve agora incluir a verificação das práticas de segurança e privacidade desses parceiros tecnológicos.

Contratos com fornecedores de tecnologia devem conter cláusulas específicas sobre proteção de dados, direito de auditoria algorítmica e responsabilidade por falhas de IA. Se um fornecedor de IA utiliza dados da empresa para treinar seus próprios modelos sem autorização, há uma violação grave de compliance. O monitoramento da cadeia de suprimentos digital é, portanto, uma extensão necessária do programa de integridade moderno.

A transparência do fornecedor é fundamental. Empresas devem exigir que seus parceiros de tecnologia forneçam documentação técnica clara sobre o funcionamento de seus algoritmos e os testes de viés realizados. O compliance digital atua na homologação desses fornecedores, garantindo que a inovação trazida por terceiros não importe riscos inaceitáveis para a organização contratante.

4.7 O PAPEL DA ANPD E A REGULAÇÃO RESPONSIVA

A Autoridade Nacional de Proteção de Dados (ANPD) desempenha um papel central na definição dos padrões de compliance digital no Brasil. Suas resoluções e guias orientativos fornecem a interpretação oficial da LGPD. A Resolução CD/ANPD nº 4/2023, por exemplo, ao detalhar o processo de dosimetria de sanções, reforça que a existência de mecanismos de governança e boas práticas será considerada como atenuante.

A regulação responsiva adotada pela ANPD busca incentivar a conformidade voluntária antes de aplicar sanções punitivas. Isso cria um ambiente favorável para que as empresas desenvolvam seus programas de integridade digital em diálogo com a autoridade. O compliance deve estar atento às consultas públicas e agendas regulatórias da ANPD para antecipar mudanças normativas e ajustar seus processos internos.

Além disso, a ANPD tem focado em temas de alto impacto, como o tratamento de dados por sistemas de IA. A cooperação entre a ANPD e outros órgãos reguladores (como o Banco Central e a CVM) indica uma tendência de regulação multissetorial do ambiente digital. O programa de integridade deve ser capaz de harmonizar essas diferentes exigências regulatórias em um framework único de governança de dados.

4.8 TREINAMENTO E CULTURA DE INTEGRIDADE DIGITAL

Nenhum sistema tecnológico substitui a necessidade de uma cultura ética sólida. O fator humano continua sendo o elo mais fraco — ou mais forte — do compliance. Treinamentos regulares sobre proteção de dados, uso ético de IA e segurança da informação são indispensáveis. Esses treinamentos devem ser adaptados aos diferentes níveis da organização, desde a operação até a alta gestão.

A cultura de integridade digital significa que cada colaborador entende sua responsabilidade no tratamento de dados. Isso envolve desde o cuidado com senhas até o discernimento para não utilizar ferramentas de IA não autorizadas para tarefas críticas. O compliance deve utilizar técnicas de comunicação modernas, como *gamificação* e *microlearning*, para garantir que as normas sejam compreendidas e aplicadas no dia a dia.

A liderança (*tone from the top*) é o motor dessa cultura. Se os executivos ignoram as regras de privacidade em nome da agilidade, os demais colaboradores seguirão o exemplo. O compliance digital deve garantir que a ética digital seja um valor vivido pela liderança, refletido em decisões estratégicas e investimentos em tecnologias responsáveis.

O avanço para agentes autônomos de IA, que tomam decisões e executam ações sem intervenção humana direta, representa o próximo grande desafio do compliance. Como monitorar um sistema que evolui e aprende em tempo real? A resposta reside na implementação de "guardrails" (barreiras de proteção) algorítmicos — regras codificadas que o sistema não pode ultrapassar, independentemente de seu aprendizado.

A IA generativa também será usada para fortalecer o compliance. Chatbots internos treinados nas políticas da empresa podem responder dúvidas de colaboradores em tempo real, facilitando a conformidade. IAs podem analisar automaticamente milhares de novos regulamentos e sugerir ajustes nos processos internos, mantendo a empresa sempre atualizada. O compliance do futuro será uma colaboração íntima entre inteligência humana e artificial.

Contudo, a autonomia da IA exige uma revisão dos conceitos de dolo e culpa no direito corporativo. Se um agente autônomo decide realizar uma prática anticompetitiva para maximizar o lucro, quem responde? O compliance digital deve assegurar que existam mecanismos de interrupção imediata (*kill switch*) e que a responsabilidade final seja sempre rastreável a um gestor humano, preservando o princípio da dignidade da pessoa humana e a soberania do direito.

5. Conclusão e Contribuições

O presente estudo demonstrou que a implantação de programas de integridade na era digital exige uma simbiose entre o rigor jurídico e a inovação tecnológica. A Inteligência Artificial, longe de ser uma ameaça ao compliance, apresenta-se como uma aliada indispensável para a gestão de riscos em ambientes de Big Data, desde que operada sob uma governança algorítmica transparente e em conformidade estrita com a LGPD. A transição para o compliance digital não é uma opção, mas uma necessidade de sobrevivência para as organizações contemporâneas.

A análise realizada permitiu confirmar que os objetivos propostos foram alcançados. Foi possível conceituar o instituto do compliance em sua evolução histórica até o compliance digital, analisar o papel das normas de governança na mitigação dos riscos éticos e jurídicos, mapear as interseções críticas entre os princípios da LGPD e os riscos da IA, investigar as aplicações práticas da IA nos processos de conformidade, e analisar os impactos do PL 2338/2023 sobre as organizações brasileiras. A pesquisa evidenciou que a eficácia do compliance digital depende da integração entre tecnologia, direito e ética.

Os resultados indicam que o compliance digital não pode ser tratado como um departamento isolado, mas como uma função estratégica integrada à governança corporativa, com participação ativa da alta administração e dos conselhos. A adoção de IA nos processos de compliance oferece ganhos significativos em eficiência, precisão e capacidade de análise preditiva, mas exige contrapartidas em termos de governança algorítmica, transparência e ética. A supervisão humana emerge como o requisito fundamental para garantir que a automação não resulte em injustiças ou violações de direitos.

Como limitações desta pesquisa, aponta-se: (i) a celeridade das transformações tecnológicas, que pode tornar obsoletas determinadas ferramentas e referências em curtos períodos; (ii) a dificuldade de acesso a dados empíricos sobre falhas de compliance em sistemas de IA, uma vez que as empresas tratam essas informações com confidencialidade; (iii) a tramitação ainda em curso do PL 2338/2023, que adiciona um componente de incerteza regulatória; (iv) a falta de padronização nas ferramentas de IA aplicadas à governança e ao compliance digital; e (v) as diferenças entre a legislação brasileira e as normas internacionais, que podem afetar comparações ou extrapolações.

Importante ressaltar que a literatura sobre IA no Brasil é robusta e crescente, como demonstram os dados e referências ao longo deste artigo. Não há escassez de produção acadêmica sobre o tema — o desafio está em integrar essas múltiplas fontes em um quadro analítico coerente que dialogue com as necessidades práticas do compliance organizacional. A afirmação de falta de literatura consolidada não se sustenta diante do volume de estudos de alta qualidade produzidos nos últimos anos por juristas, gestores e cientistas de dados brasileiros.

Para trabalhos futuros, sugerem-se: (a) estudos de caso comparativos entre organizações que já adotam auditorias algorítmicas e aquelas que mantêm processos tradicionais de compliance; (b) a análise do impacto das primeiras sanções da ANPD relacionadas ao uso de IA no Brasil; (c) pesquisa empírica sobre o nível de maturidade em proteção de dados e IA em empresas de diferentes portes e setores; (d) o desenvolvimento de métricas e indicadores de conformidade para avaliar a eficácia de soluções de IA em auditoria e detecção de riscos; (e) a investigação da compatibilidade entre a LGPD e regulamentações internacionais sobre IA, como o EU AI Act; e (f) a elaboração de guias práticos de implementação de programas de integridade digital voltados para pequenas e médias empresas.

O futuro do compliance é digital, algorítmico e preditivo. Cabe às organizações e à academia construir, de forma colaborativa, as bases éticas e normativas que garantirão que essa transformação ocorra em benefício da sociedade, dos negócios e dos direitos fundamentais. A integridade na era da inteligência artificial exige vigilância constante, inovação responsável e um compromisso inabalável com a transparência e a dignidade humana.

Referências

ABDULLAHI, S.; DANYARO, K. U.; CHIROMA, H. The rise of hallucination in large language models: systematic reviews, performance analysis and challenges. Cluster Computing, v. 29, 124, 2026. DOI: 10.1007/s10586-025-05891-z. Disponível em: https://link.springer.com/article/10.1007/s10586-025-05891-z. Acesso em: 03 ago. 2026.

ALMADA, Marco; MARANHÃO, Juliano Souza de Albuquerque. **Contribuições e limites da Lei Geral de Proteção de Dados para a regulação da Inteligência Artificial no Brasil.** Direito Público, Brasília, v. 20, n. 106, 2023. DOI: 10.11117/rdp.v20i106.6957. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/6957. Acesso em: 08 ago. 2026.

ALMEIDA, Luiz Eduardo. **Manual de Compliance: Governança Corporativa**. 4. ed. Rio de Janeiro: Forense, 2025.

ALVES, Davis Souza; CONCEIÇÃO, Márcio Magera. O impacto da Inteligência Artificial na automação de auditorias em conformidade com as leis de proteção de dados. **RECIMA21 - Revista Científica Multidisciplinar**, v. 6, n. 2, e616167, 2025.

AMORIM, Letícia Vilen; SANT'ANNA, Leonardo da Silva. **Implementação e efetividade de programas de integridade no âmbito das sociedades empresárias privadas.** Scientia Iuris, Londrina, v. 29, n. 3, p. 106-121, 2025. DOI: 10.5433/2178-8189.2025v29n3p106-121. Disponível em:

https://www.ojs.uel.br/revistas/uel/index.php/iuris/article/view/53382. Acesso em: 01 ago. 2026.

AZZARI, Bruna; SILVA, Amanda Scalisse; CHIARELLO, Felipe. Ética e Integridade nas Instituições de Ensino Superior: A Importância da Implementação de Programas de Compliance nas Universidades. **Revista de Direito Brasileira**, Florianópolis, v. 26, n. 10, p. 457–470, 2020.

BARDIN, Laurence. **Análise de conteúdo**. São Paulo: Edições 70, 2016.

BELISARIO, Denise Mayumi Iwakura; MUNIZ, Marcia; CODIGNOTO, Roberta. Comprometimento da alta administração: tone from the top. In: CARVALHO, André Castro et al. **Manual de Compliance**. 4. ed. Rio de Janeiro: Forense, 2025.

BERTOCCELLI, Rodrigo de Pinho. Compliance. In: CARVALHO, André Castro et al. **Manual de Compliance**. 4. ed. Rio de Janeiro: Forense, 2024.

BOTTER, Eduardo Fecchio; MENEZES, Maria Angélica de Souza; SILVA, Vitor Henrique Braz da. Tecnologia e Compliance – O papel da inteligência artificial na monitorização de conformidade. **Revista Jurídica UNIGRAN**, Dourados, v. 27, n. 53, jan./jun. 2025.

BRASIL. **Decreto Federal nº 11.129, de 11 de julho de 2022**. Regulamenta a Lei nº 12.846/2013. Brasília, 2022.

BRASIL. **Lei nº 12.846, de 1º de agosto de 2013**. Lei Anticorrupção. Brasília, 2013.

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

BRASIL. **Portaria CGU nº 750, de 20 de abril de 2016**. Programa de Integridade. Brasília: Controladoria-Geral da União, 2016.

BRASIL. **Projeto de Lei nº 2.338, de 2023**. Estabelece o Marco Legal da Inteligência Artificial. Brasília: Senado Federal, 2023.

BUENO, Eric Fiuza; SANTOS, Marcelo Fonseca. Inteligência Artificial e os desafios da regulação. **Revista Eletrônica Direito & TI**, Porto Alegre, v. 1, n. 18, jan./abr. 2024.

CAMPOS, Daniela; CARREIRO, Flávia dos Reis. Compliance e gestão de riscos em tempos de inovação e disrupção digital. **Revista de Gestão e Secretariado – GeSec**, v. 15, n. 4, 2024.

CARDOSO, Henrique Ribeiro; MELO, Bricio Luis da Anunciação. Regulação e responsabilidade civil por danos causados pela inteligência artificial. **Revista de Direito Administrativo**, Rio de Janeiro, v. 283, n. 3, p. 143-173, set./dez. 2024. DOI: 10.12660/rda.v283.2024.91698. Disponível em: https://periodicos.fgv.br/rda/article/download/91698/86845/211859. Acesso em: 3 ago. 2026.

CARVALHO, Itamar; ABREU, Bruno Cesar Almeida de; TAKAKI, Eloá Buzatto. Programas de Compliance: O Programa de Integridade. In: CARVALHO, André Castro et al. **Manual de Compliance**. 4. ed. Rio de Janeiro: Forense, 2025.

CAVALCANTE, Ailton Ferreira. **Governança algorítmica e interesse público:** bases éticas para decisões no setor público. ARACÊ, São José dos Pinhais, v. 8, n. 1, p. e11673, 2026. DOI: 10.56238/arev8n1-042. Disponível em: https://periodicos.newsciencepubl.com/arace/article/view/11673. Acesso em: 5 ago. 2026.

CAVALIERI, Davi Valdetaro Gomes. **Governança de dados e programa de compliance digital na administração pública: contribuições da LGPD para a integridade governamental**. Dissertação (Mestrado em Direito) – Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2020.

CAVALIERI, Davi Valdetaro Gomes. Governança de dados. In: CARVALHO, André Castro et al. **Manual de Compliance**. 4. ed. Rio de Janeiro: Forense, 2025.

CECYN, Victor Antonio. O Programa de Compliance como Medida de Prevenção e Mitigação de Riscos Emanados por Inteligências Artificiais no Tratamento de Dados Pessoais. In: **Reflexões sobre Direito e Sociedade: Fundamentos e Práticas**, v. 14, 2025.

CETIC.BR. **Uso de Inteligência Artificial por empresas brasileiras avança e atinge 17%**. São Paulo: Comitê Gestor da Internet no Brasil, 2026.

CONFIDATA. Segurança da Informação e LGPD: o que o art. 46 exige na prática. Confidata Blog, 12 dez. 2025. Disponível em: https://confidata.com.br/blog/seguranca-informacao-lgpd-art-46-pratica. Acesso em: 8 ago. 2026.

DESAI, Pratyush; TANG, Luoxi; MENG, Yuqiao; XI, Zhaohan. SafeGPT: preventing data leakage and unethical outputs in enterprise LLM use. arXiv, 2026. Disponível em: https://arxiv.org/html/2601.06366v2. Acesso em: 05 ago. 2026.

DIAS, Cintia Coelho; FERREIRA, Roberta Valiatti. O uso da inteligência artificial na atividade de compliance: riscos e benefícios. **CPJM - Revista Científica**, Rio de Janeiro, v. 2, n. 8, 2023.

EY BRASIL. **AI Sentiment Index 2026: Com 95% já usando IA, Brasil está entre líderes de ranking de adoção dessa tecnologia**. São Paulo: Ernst & Young, 2026.

GALVÃO, Camila Trindade. **Inteligência artificial, discriminação algorítmica e o dever de diligência dos administradores das sociedades anônimas.** 2023. Dissertação (Mestrado em Direito) – Escola de Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2023.

Disponível em: https://tede2.pucrs.br/tede2/handle/tede/10803. Acesso em: 08 mai. 2026.

IBGC. **Código de Melhores Práticas de Governança Corporativa**. 6. ed. São Paulo: Instituto Brasileiro de Governança Corporativa, 2023.

INDEX LAW. A integração da Inteligência Artificial na Governança Corporativa: enfoque ético e regulatório. **Revista de Direito, Governança e Novas Tecnologias**, v. 10, n. 2, 2025.

JOTA. **Câmara discute alterações no Marco Legal da IA**. Brasília, 2025. Disponível em: jota.info. Acesso em: 29 jul. 2026.

KFOURI, Gustavo Swain; ZAMBÃO, Lara Helena Luiza. Contratações públicas com ferramentas de inteligência artificial: desafios éticos e de compliance. **Revista Jurídica Gralha Azul – EJUD-TJPR**, v. 1, n. 28, 2025.

LINKEDIN. **Brasil lidera corrida pela adoção da inteligência artificial**. Pesquisa LinkedIn Economic Graph, 2025.

MANSO, Adriano Marques; JUNQUEIRA CALIXTO, Marcelo. Os regimes de responsabilização civil no novo Marco Legal para Inteligência Artificial: o Projeto de Lei nº 2.338/23. International Journal of Digital Law, Belo Horizonte, v. 4, n. 3, p. 111-129, 2024. DOI: 10.47975/digital.law.vol.4.n.3.manso. Disponível em: https://journal.nuped.com.br/index.php/revista/article/view/1261. Acesso em: 05 ago. 2026.

MCKINSEY & COMPANY. **The State of AI in 2026: Brazil's digital acceleration**. McKinsey Global Institute, 2026.

METCALF, Renae; CHURILLA, Matt. Data poisoning in AI models: the case for chain of custody controls. SEI Blog, Software Engineering Institute, Carnegie Mellon University, 27 abr. 2026. Disponível em: https://www.sei.cmu.edu/blog/data-poisoning-in-ai-models-the-case-for-chain-of-custody-controls/. Acesso em: 08 ago. 2026.

MORATO, Otávio; NUNES, Dierle José Coelho; TAVARES, Viviane Ramone. **Direito à explicação no cenário algorítmico:** fundamentos e esboço de agenda para uma governança ética da IA. InterAção, Santa Maria, v. 17, n. 1, e95074, p. 1-25, mar. 2026. DOI: 10.5902/2357797595074. Disponível em: https://dx.doi.org/10.5902/2357797595074. Acesso em: 08 ago. 2026.

MOREIRA, Rafael Gomes; ROCHA, Rafael Oliveira da; CHAHUD, Leonardo Gonçalves; PEREIRA JUNIOR, Lourenço Alves. **Roubo de modelo para ataque adversarial em sistemas de detecção de intrusão.** In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUÍDOS (SBRC), 42., 2024, Niterói/RJ. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2024. p. 1022-1035. DOI: 10.5753/sbrc.2024.1527. Disponível em:

https://sol.sbc.org.br/index.php/sbrc/article/view/29852. Acesso em: 02 ago. 2026.

O'BRIEN, Joe; EE, Shaun; WILLIAMS, Zoe. Deployment corrections: an incident response framework for frontier AI models. arXiv, 2023. DOI: 10.48550/arXiv.2310.00328. Disponível em: https://arxiv.org/pdf/2310.00328. Acesso em: 18 mai. 2026.

OLIVEIRA FILHO, Adauto Turíbio de. **Inteligência artificial explicável (XAI):** um requisito de transparência e governança para sistemas de informação. 2026. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Instituto Federal Goiano, Campus Ceres, 2026. Disponível em: https://repositorio.ifgoiano.edu.br/bitstream/prefix/5964/1/INTELIG%C3%8ANCIA%20ARTIFICIAL%20EXPLIC%C3%81VEL%20%28XAI%29_%20UM%20REQUISITO%20DE%20TRANSPAR%C3%8ANCIA%20E%20GOVERNAN%C3%87A%20PARA%20SISTEMAS%20DE%20INFORMA%C3%87%C3%83O.pdf. Acesso em: 28 mar. 2026.

RAVAGNANI, Allan. **Estudo mostra que IA generativa vaza dados sensíveis em 64% das empresas brasileiras; veja por onde.** Times Brasil | CNBC, São Paulo, 11 maio 2026. Disponível em: https://timesbrasil.com.br/empresas-e-negocios/inteligencia-artificial/vazamentos-dados-ia-generativa-brasil-netskope-2026/. Acesso em: 08 ago. 2026.

REVISTA FT. Governança de Inteligência Artificial no Brasil: Panorama Regulatório Atual. **Revista FT**, ed. 142, 2025.

SANTOS, Ronnie de Souza; BALDASSARRE, Maria Teresa; MAGALHÃES, Cleyton. The role of team diversity in AI systems development. arXiv, [S. l.], 8 mar. 2026. DOI: 10.48550/arXiv.2603.07749. Disponível em: https://arxiv.org/pdf/2603.07749. Acesso em: 08 ago. 2026.

UNESP. **Guia de Metodologia Científica**. São Paulo: Universidade Estadual Paulista, 2023.

VENTURINI, Otávio. Programa de Compliance Digital. In: CARVALHO, André Castro et al. **Manual de Compliance**. 4. ed. Rio de Janeiro: Forense, 2025.