RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano V, v.2 2025 | submissão: 26/10/2025 | aceito: 28/10/2025 | publicação: 30/10/2025

Regulação da inteligência artificla no Brasil: direitos Fundamentais, responsabilidade e riscos constitucionais

Regulation of artificial intelligence in Brazil: Fundamental rights, responsibility, and constitutional risks

Ilan Haim Benchimol dos Reis Conte - Acadêmico do Curso de Direito da Faculdade Santa Teresa -FST. E-mail: ilanbenchimolconte86@gmail.com
Artigo apresentado para Avaliação de Desempenho Geral – ADG, orientado pelo Prof.º Paulo Eduardo Queiroz da Costa.

João Vitor Moraes Barbosa - Acadêmico do Curso de Direito da Faculdade Santa Teresa – FST. Email: jvvitormoraes@hotmail.com
Artigo apresentado para Avaliação de Desempenho Geral – ADG, orientado pelo Prof.º Paulo Eduardo Queiroz da Costa.

Paulo Eduardo Queiroz da Costa – Professor e Orientador

RESUMO
Este artigo analisa a regulação da inteligência artificial (IA) no Brasil, com foco nos direitos fundamentais, responsabilidade jurídica e riscos constitucionais. A partir do Projeto de Lei nº 2.338/2023 e da Lei Geral de Proteção de Dados (LGPD), o estudo examina o equilíbrio entre inovação tecnológica e proteção de direitos como privacidade, dignidade, igualdade e não discriminação. Destaca os desafios na atribuição de responsabilidade em sistemas autônomos, especialmente diante da opacidade algorítmica, e a necessidade de transparência. Também aborda riscos como viés, vigilância, manipulação informacional e decisões automatizadas que afetam direitos. Compara o modelo brasileiro ao europeu e propõe diretrizes para aprimorar a legislação. Conclui que a regulação da IA exige abordagem multidisciplinar, participação democrática e compromisso ético com a justiça social e a Constituição.
Palavras-chave: Inteligência artificial. Regulação. Direitos fundamentais. Responsabilidade jurídica. Riscos constitucionais.

ABSTRACT
This article analyzes the regulation of artificial intelligence (AI) in Brazil, focusing on the protection of fundamental rights, legal liability, and emerging constitutional risks. Based on Bill No. 2,338/2023 and the General Data Protection Law (LGPD), the study explores how the legal framework seeks to balance technological innovation with constitutional guarantees such as privacy, dignity, equality, and nondiscrimination. It discusses the challenges of assigning liability in autonomous systems, especially considering algorithmic opacity, and highlights risks such as bias, surveillance, informational manipulation, and automated decision-making that affect fundamental rights. The paper compares the Brazilian model with the European approach and proposes guidelines for improving legislation. It concludes that AI regulation in Brazil requires a multidisciplinary approach, democratic participation, and an ethical commitment to social justice and the Federal Constitution.
Keywords: Artificial intelligence. Regulation. Fundamental rights. Legal liability. Constitutional risks.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano V, v.2 2025 | submissão: 26/10/2025 | aceito: 28/10/2025 | publicação: 30/10/2025

INTRODUÇÃO

A inteligência artificial (IA) representa uma das mais profundas transformações tecnológicas da contemporaneidade, redefinindo relações sociais, econômicas e jurídicas em escala global. Algoritmos de aprendizado de máquina, sistemas de reconhecimento facial, assistentes virtuais e plataformas de decisão automatizada já permeiam o cotidiano, influenciando desde escolhas de consumo até decisões judiciais e políticas públicas. Esse avanço tecnológico, contudo, não é neutro: ele carrega consigo desafios éticos, jurídicos e políticos que exigem respostas urgentes do Direito e do Estado.

No Brasil, o debate sobre a regulação da inteligência artificial ganhou impulso nos últimos anos, especialmente com a tramitação do Projeto de Lei nº 2.338/2023, que busca estabelecer diretrizes para o desenvolvimento, a implementação e o uso de sistemas de IA. Esse movimento regulatório se insere em um contexto mais amplo de preocupação global com os impactos da automação sobre direitos fundamentais, democracia e justiça social. A experiência europeia com o Regulamento de Inteligência Artificial, a regulação setorial nos Estados Unidos e os debates na América Latina demonstram que a IA não pode ser tratada como mera inovação tecnológica, mas como fenômeno que exige governança ética e juridicamente fundamentada.

A relevância deste estudo se justifica pela necessidade de compreender como o ordenamento jurídico brasileiro está respondendo aos desafios impostos pela IA, especialmente no que diz respeito à proteção de direitos fundamentais consagrados na Constituição Federal de 1988. A inteligência artificial, ao automatizar decisões que afetam a vida das pessoas, pode reproduzir e amplificar discriminações históricas, violar a privacidade, comprometer a autonomia individual e desafiar princípios como transparência, devido processo legal e dignidade humana. Sem uma regulação adequada, corre-se o risco de que a IA se torne um instrumento de aprofundamento de desigualdades e violações de direitos.

Além disso, a questão da responsabilidade jurídica em sistemas de IA apresenta complexidades inéditas para o Direito. Quando um algoritmo toma uma decisão que causa danos — seja negando um crédito, influenciando um julgamento ou provocando um acidente com veículo autônomo —, quem deve ser responsabilizado? O desenvolvedor, o operador, o proprietário do sistema ou a própria IA? A ausência de respostas claras a essas perguntas gera insegurança jurídica e pode comprometer a efetividade da tutela jurisdicional.

Este artigo também se volta para os riscos constitucionais emergentes decorrentes do uso inadequado ou abusivo de sistemas de inteligência artificial. Entre esses riscos, destacam-se: o viés algorítmico, que pode perpetuar discriminações baseadas em raça, gênero, classe

Ano V, v.2 2025 | submissão: 26/10/2025 | aceito: 28/10/2025 | publicação: 30/10/2025

social ou origem geográfica; a vigilância em massa, que ameaça o direito à privacidade e à liberdade de expressão; a manipulação informacional, que compromete a integridade do debate democrático; e a automação de decisões administrativas e judiciais sem a devida supervisão humana, o que pode violar o princípio da motivação e o direito ao contraditório.

Diante desse cenário, o problema central que orienta este estudo é: como o Brasil está estruturando a regulação da inteligência artificial de modo a garantir a proteção de direitos fundamentais, estabelecer regimes adequados de responsabilidade jurídica e mitigar riscos constitucionais emergentes?

Para responder a essa questão, o trabalho se organiza em quatro eixos temáticos.

O primeiro aborda o marco regulatório brasileiro em construção, analisando o Projeto de Lei nº 2.338/2023, a aplicação da LGPD a sistemas de IA e outras normas setoriais relevantes. O segundo eixo examina a relação entre inteligência artificial e direitos fundamentais, destacando os desafios para a proteção da privacidade, dignidade, igualdade e liberdade em um contexto de automação crescente. O terceiro eixo discute os regimes de responsabilidade jurídica aplicáveis a sistemas de IA, com ênfase nas dificuldades de atribuição de responsabilidade civil, administrativa e penal. O quarto eixo identifica e analisa os principais riscos constitucionais decorrentes do uso de IA propondo diretrizes para a construção de uma governança algorítmica democrática e constitucionalmente orientada.

Ao final, espera-se contribuir para o debate acadêmico e institucional sobre a regulação da inteligência artificial no Brasil, oferecendo subsídios teóricos e práticos para a construção de um marco normativo que concilie inovação tecnológica, proteção de direitos fundamentais e respeito aos valores democráticos consagrados na Constituição Federal. A regulação da IA não é apenas uma questão técnica, mas' um imperativo ético e político para a construção de um futuro no qual a tecnologia sirva à dignidade humana e à justiça social.

Marco regulatório brasileiro da inteligência artificial

A regulação da inteligência artificial no Brasil encontra-se em fase de consolidação, marcada por iniciativas legislativas, normas setoriais e pela aplicação de princípios constitucionais e legais já existentes. O processo de construção desse marco regulatório reflete a tensão entre a necessidade de fomentar a inovação tecnológica e a urgência de proteger direitos fundamentais, assegurar transparência e estabelecer mecanismos de responsabilização.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano V, v.2 2025 | submissão: 26/10/2025 | aceito: 28/10/2025 | publicação: 30/10/2025

2.1 O Projeto de Lei nº 2.338/2023

O principal instrumento normativo em discussão é o Projeto de Lei nº 2.338/2023, que visa estabelecer princípios, diretrizes e garantias para o desenvolvimento e a

aplicação de sistemas de inteligência artificial no Brasil. Aprovado pelo Senado Federal em dezembro de 2023 e encaminhado à Câmara dos Deputados, o projeto representa o esforço mais abrangente de regulação horizontal da IA no país.

O PL 2.338/2023 adota uma abordagem baseada em riscos, classificando sistemas de IA em diferentes categorias conforme o potencial de dano aos direitos fundamentais. Sistemas de alto risco — como aqueles utilizados em decisões judiciais, concessão de crédito, recrutamento de pessoal, serviços essenciais e segurança pública — estão sujeitos a requisitos mais rigorosos de transparência, auditabilidade e supervisão humana. Já sistemas de risco mínimo ou inexistente possuem regulação mais flexível, incentivando a experimentação e a inovação**.**

Entre os princípios estabelecidos pelo projeto destacam-se: a finalidade, que exige que sistemas de IA sejam desenvolvidos para objetivos legítimos e específicos; a não discriminação, que proíbe o uso de IA para perpetuar preconceitos ou desigualdades; a transparência, que assegura o direito de conhecer a lógica de decisões automatizadas; a segurança e a privacidade, que impõem medidas de proteção de dados pessoais; e a supervisão humana, que garante que decisões críticas não sejam integralmente automatizadas sem revisão.

O projeto também prevê a criação de uma autoridade competente para fiscalizar e regulamentar a aplicação da lei, inspirando-se no modelo da Autoridade Nacional de Proteção de Dados (ANPD). A ausência de um órgão regulador específico tem sido apontada como uma lacuna importante, considerando a complexidade técnica e a interdisciplinaridade exigidas pela governança de IA.

2.2 A LGPD e a proteção de dados em sistemas de IA

Antes mesmo da aprovação de uma lei específica sobre inteligência artificial, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) já oferece importante arcabouço normativo para a regulação de sistemas que utilizam dados pessoais. A LGPD estabelece princípios como finalidade, adequação, necessidade, transparência, segurança e não discriminação, aplicáveis ao tratamento de dados por algoritmos de IA.

Ano V, v.2 2025 | submissão: 26/10/2025 | aceito: 28/10/2025 | publicação: 30/10/2025

O artigo 20 da LGPD é particularmente relevante, ao garantir ao titular de dados o direito de solicitar revisão de decisões automatizadas que afetem seus interesses. Esse dispositivo reconhece que algoritmos não são neutros e que decisões baseadas exclusivamente em processamento automatizado podem gerar efeitos discriminatórios ou arbitrários. A supervisão humana significativa, nesse contexto, é essencial para assegurar a correção de erros e a proteção de direitos.

No entanto, a aplicação da LGPD a sistemas de IA enfrenta desafios. A opacidade dos algoritmos de aprendizado profundo — a chamada "caixa-preta algorítmica" — dificulta a transparência e a auditabilidade exigidas pela lei. Além disso, a inexistência de regulamentação específica sobre viés algorítmico e sobre a responsabilidade por danos causados por sistemas autônomos gera lacunas que precisam ser preenchidas.

2.3 Normas setoriais e iniciativas regulatórias

Além do PL 2.338/2023 e da LGPD, diversas normas setoriais já tratam, direta ou indiretamente, do uso de inteligência artificial. O Código de Defesa do Consumidor (Lei nº 8.078/1990) estabelece responsabilidade objetiva por produtos e serviços defeituosos, o que pode ser aplicado a sistemas de IA que causem danos a consumidores. A legislação trabalhista também é relevante, especialmente diante do uso de algoritmos em processos de recrutamento, avaliação de desempenho e demissão.

No setor público, a Estratégia Brasileira de Inteligência Artificial (EBIA), lançada em 2021 pelo Ministério da Ciência, Tecnologia e Inovações, estabelece diretrizes para o fomento à pesquisa, à inovação e ao uso ético de IA pelo Estado. A estratégia destaca a importância da transparência, da prestação de contas e do respeito aos direitos humanos na implementação de tecnologias inteligentes em serviços públicos.

O Poder Judiciário também tem desenvolvido iniciativas próprias, como a CNJ nº 332/2020, que dispõe sobre ética, transparência e governança na produção e no uso de inteligência artificial no âmbito do Judiciário. Essa norma estabelece que sistemas de IA devem ser desenvolvidos com respeito aos direitos fundamentais, vedando discriminação e garantindo a revisão humana de decisões.

Ano V, v.2 2025 | submissão: 26/10/2025 | aceito: 28/10/2025 | publicação: 30/10/2025

2.4 Lacunas e desafios do marco regulatório

Apesar dos avanços, o marco regulatório brasileiro ainda apresenta lacunas importantes. A ausência de uma lei específica em vigor gera insegurança jurídica, dificultando a responsabilização por danos e a proteção efetiva de direitos. A definição de conceitos fundamentais — como o que constitui um sistema de IA de alto risco, o que caracteriza viés algorítmico e quais são os limites da automação de decisões — ainda carece de maior precisão.

Outro desafio é a coordenação entre diferentes órgãos reguladores. A inteligência artificial perpassa diversos setores — saúde, educação, segurança pública, justiça, serviços financeiros —, exigindo governança integrada e diálogo institucional. A criação de uma autoridade reguladora específica, nos moldes do que prevê o PL 2.338/2023, pode contribuir para maior coerência e efetividade da regulação.

Por fim, é fundamental que a regulação brasileira esteja alinhada com padrões internacionais, sem perder de vista as especificidades locais. A experiência do Regulamento Europeu de Inteligência Artificial, que estabelece uma regulação abrangente e baseada em riscos, oferece importantes lições. Ao mesmo tempo, o Brasil deve considerar suas desigualdades estruturais, seu contexto de vulnerabilidade de dados e a necessidade de garantir que a regulação não seja capturada por interesses econômicos em detrimento da proteção de direitos.

3 inteligências artificial e direitos fundamentais

A relação entre inteligência artificial e direitos fundamentais constitui um dos campos mais sensíveis e complexos da regulação tecnológica. Sistemas de IA, ao automatizar decisões que afetam diretamente a vida das pessoas, podem tanto ampliar o acesso a direitos quanto gerar novas formas de violação e discriminação.

Este capítulo examina como a IA impacta direitos constitucionais essenciais e quais desafios se apresentam para sua proteção.

3.1 Privacidade e proteção de dados pessoais

O direito à privacidade, consagrado no artigo 5º, inciso X, da Constituição Federal, e reforçado pela LGPD, é diretamente afetado pelo uso de sistemas de inteligência artificial.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano V, v.2 2025 | submissão: 26/10/2025 | aceito: 28/10/2025 | publicação: 30/10/2025

Algoritmos de IA dependem de grandes volumes de dados pessoais para treinamento e operação, o que amplia os riscos de coleta abusiva, tratamento inadequado e vazamentos.

A coleta massiva de dados para alimentar sistemas de IA frequentemente ocorre sem o conhecimento ou consentimento adequado dos titulares, violando o princípio da transparência. Além disso, a combinação de dados de diferentes fontes permite a criação de perfis detalhados sobre indivíduos, revelando informações sensíveis que eles não compartilhariam voluntariamente.

O reconhecimento facial, amplamente utilizado em sistemas de segurança pública, é exemplo emblemático dos riscos à privacidade. Estudos demonstram que essas tecnologias apresentam taxas de erro significativamente maiores para pessoas negras, especialmente mulheres, o que combina violação de privacidade com discriminação racial. A ausência de regulação específica permite que órgãos públicos e empresas utilizem reconhecimento facial sem salvaguardas adequadas, gerando vigilância em massa incompatível com o Estado Democrático de Direito.

3.2 Dignidade humana e autonomia individual

A dignidade da pessoa humana, fundamento da República (CF, art. 1º, III), impõe limites éticos ao desenvolvimento e ao uso de inteligência artificial. Sistemas de IA não podem reduzir indivíduos a meros conjuntos de dados ou perfis estatísticos, desconsiderando sua singularidade, contexto e capacidade de autodeterminação.

A automação de decisões sensíveis — como concessão de benefícios sociais, aprovação de crédito, acesso a serviços de saúde ou decisões judiciais — sem supervisão humana adequada pode violar a dignidade ao tratar pessoas como objetos de processamento algorítmico. A ausência de explicabilidade nesses sistemas impede que indivíduos compreendam as razões de decisões que os afetam, comprometendo sua autonomia e capacidade de contestação.

Além disso, a manipulação comportamental por meio de algoritmos de recomendação — comuns em redes sociais e plataformas digitais — pode comprometer a liberdade de escolha e a autonomia individual. Técnicas de persuasão algorítmica exploram vieses cognitivos para influenciar decisões, levantando questões sobre até que ponto esses sistemas respeitam a autodeterminação dos usuários.

Ano V, v.2 2025 | submissão: 26/10/2025 | aceito: 28/10/2025 | publicação: 30/10/2025

3.3 Igualdade e não discriminação

O princípio da igualdade (CF, art. 5º, caput) exige que o Estado e particulares não pratiquem discriminações arbitrárias. No entanto, sistemas de IA frequentemente reproduzem e amplificam preconceitos presentes nos dados utilizados para seu treinamento, gerando discriminação algorítmica.

Estudos internacionais demonstram que algoritmos utilizados em processos de recrutamento podem discriminar mulheres, que sistemas de avaliação de risco criminal apresentam viés racial e que algoritmos de concessão de crédito penalizam moradores de determinadas regiões. No Brasil, pesquisas indicam que sistemas de reconhecimento facial têm desempenho inferior para pessoas negras, o que pode resultar em erros de identificação com graves consequências jurídicas e sociais.

A discriminação algorítmica é especialmente preocupante porque opera de forma opaca e aparentemente neutra, dificultando sua identificação e contestação. Diferentemente da discriminação explícita, o viés algorítmico está embutido na lógica do sistema, o que exige mecanismos específicos de auditoria e correção.

O direito à não discriminação em contextos de IA exige não apenas a vedação de critérios explicitamente discriminatórios, mas também a análise de impacto desproporcional. Mesmo critérios aparentemente neutros podem gerar efeitos discriminatórios quando aplicados a grupos vulneráveis, o que demanda avaliação contínua e correção de sistemas de IA.

3.4 Devido processo legal e contraditório

O devido processo legal (CF, art. 5º, LIV) e o contraditório e a ampla defesa (CF, art. 5º, LV) são garantias fundamentais que também se aplicam a decisões automatizadas. Quando o Estado utiliza sistemas de IA em processos administrativos ou judiciais, deve assegurar que os afetados possam conhecer, compreender e contestar essas decisões.

A opacidade de algoritmos de aprendizado profundo representa um desafio para o contraditório. Se nem mesmo os desenvolvedores conseguem explicar completamente como um sistema chegou a determinada conclusão, como o cidadão poderá exercer seu direito de defesa? A LGPD, em seu artigo 20, reconhece esse problema ao garantir o direito à revisão de decisões automatizadas, mas a implementação prática dessa garantia ainda é incipiente.

Além disso, a automação de decisões judiciais — como a distribuição de processos, a análise de recursos e até mesmo a sugestão de sentenças — deve respeitar a função jurisdicional

Ano V, v.2 2025 | submissão: 26/10/2025 | aceito: 28/10/2025 | publicação: 30/10/2025

como atividade essencialmente humana. A inteligência artificial pode ser ferramenta de auxílio, mas não pode substituir o juiz na análise de provas, na valoração de circunstâncias e na fundamentação de decisões.

3.5 Liberdade de expressão e acesso à informação

A inteligência artificial também impacta a liberdade de expressão (CF, art. 5º, IV e IX) e o direito à informação (CF, art. 5º, XIV), especialmente por meio de algoritmos de curadoria de conteúdo em plataformas digitais.

Esses sistemas determinam quais informações chegam aos usuários, podendo criar bolhas informacionais, amplificar desinformação e censurar conteúdos de forma arbitrária.

A moderação automatizada de conteúdo, embora necessária para combater discursos de ódio e ilegalidades, levanta preocupações sobre censura algorítmica. Sistemas de IA podem remover conteúdos legítimos por erro ou aplicação excessivamente restritiva de políticas, sem garantir ao usuário o direito de contestação efetiva.

Por outro lado, o uso de IA para disseminação de desinformação — por meio de contas automatizadas, deepfakes e manipulação coordenada — ameaça a integridade do debate público e a confiança nas instituições democráticas. A regulação deve equilibrar a proteção da liberdade de expressão com a necessidade de combater abusos e manipulações que comprometem a esfera pública.

Responsabilidade jurídica em sistemas de inteligência artificial

A atribuição de responsabilidade jurídica por danos causados por sistemas de inteligência artificial constitui um dos desafios mais complexos para o Direito contemporâneo. A autonomia crescente desses sistemas, aliada à opacidade de seus processos decisórios, dificulta a identificação de nexo causal e a determinação de responsáveis, exigindo reinterpretação de institutos jurídicos tradicionais.

4.1 Responsabilidade civil

O regime de responsabilidade civil brasileiro, estruturado sobre os artigos 186 e 927 do Código Civil, exige a demonstração de conduta, dano, nexo causal e, em regra, culpa. No entanto, a aplicação desses requisitos a sistemas de IA apresenta dificuldades específicas.

Ano V, v.2 2025 | submissão: 26/10/2025 | aceito: 28/10/2025 | publicação: 30/10/2025

A primeira questão é: quem deve ser responsabilizado quando um sistema de IA causa danos? As possibilidades incluem o desenvolvedor do algoritmo, o fornecedor do sistema, o operador que o implementa, o usuário final ou até mesmo a própria IA, caso se reconheça alguma forma de personalidade jurídica (hipótese ainda não acolhida pelo ordenamento brasileiro).

A responsabilidade do desenvolvedor pode ser fundamentada em defeito de concepção, quando o algoritmo é projetado de forma inadequada ou apresenta viés discriminatório. Já a responsabilidade do fornecedor pode ser objetiva, nos termos do Código de Defesa do Consumidor, quando o sistema é comercializado como produto ou serviço e causa danos ao consumidor.

O operador — aquele que implementa e utiliza o sistema de IA — também pode ser responsabilizado, especialmente quando não adota medidas adequadas de supervisão humana ou quando utiliza o sistema em contexto inadequado. A responsabilidade solidária entre desenvolvedor, fornecedor e operador é possível, cabendo ao prejudicado escolher contra quem demandar.

A opacidade algorítmica levanta questões sobre a inversão do ônus da prova. Diante da dificuldade de o prejudicado demonstrar como o sistema funcionou e onde ocorreu a falha, pode ser aplicada a inversão do ônus probatório, cabendo ao desenvolvedor ou operador demonstrar que adotou todas as medidas técnicas e organizacionais adequadas.

4.2 Responsabilidade administrativa

A responsabilidade administrativa por violações decorrentes do uso de inteligência artificial pode ser aplicada tanto ao setor público quanto ao privado. A LGPD, em seus artigos 52 e 53, prevê sanções administrativas para o tratamento inadequado de dados pessoais, incluindo multas de até 2% do faturamento, limitadas a R$ 50 milhões por infração.

Essas sanções podem ser aplicadas quando sistemas de IA violam princípios da LGPD, como finalidade, adequação, transparência ou não discriminação. A ANPD tem competência para fiscalizar e punir controladores e operadores de dados que utilizam algoritmos de forma inadequada.

No setor público, a responsabilidade administrativa também se aplica a agentes que desenvolvem, implementam ou utilizam sistemas de IA em desacordo com normas legais ou regulamentares. A Lei de Improbidade Administrativa (Lei nº 8.429/1992) pode ser invocada

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano V, v.2 2025 | submissão: 26/10/2025 | aceito: 28/10/2025 | publicação: 30/10/2025

quando o uso de IA resulta em violação de princípios da administração pública, enriquecimento ilícito ou danos ao erário.

A transparência é requisito fundamental para a responsabilização administrativa. Órgãos públicos que utilizam IA em decisões que afetam cidadãos devem divulgar informações sobre os critérios utilizados, as fontes de dados e os procedimentos de revisão humana, sob pena de violação do princípio da publicidade.

4.2 Responsabilidade penal

A responsabilidade penal em contextos de IA é ainda mais complexa, uma vez que o Direito Penal brasileiro adota o princípio da responsabilidade pessoal, exigindo a demonstração de dolo ou culpa. A automação de decisões dificulta a identificação de condutas individuais que possam ser consideradas criminosas.

Quando um sistema de IA é utilizado para a prática de crimes — como fraudes, manipulação de mercado, invasão de privacidade ou disseminação de conteúdo ilícito —, a responsabilidade recai sobre quem controla e dirige o sistema. No entanto, sistemas autônomos que operam de forma imprevisível podem gerar danos sem que haja dolo ou culpa identificável.

A criação de tipos penais específicos para crimes relacionados a IA tem sido debatida internacionalmente. Condutas como desenvolvimento de algoritmos intencionalmente discriminatórios, utilização de IA para manipulação eleitoral ou criação de deepfakes para difamação podem justificar criminalização específica.

A responsabilidade penal de pessoas jurídicas, admitida no Brasil em casos de crimes ambientais (Lei nº 9.605/1998) e contra o sistema financeiro (Lei nº 7.492/1986), pode ser estendida a empresas que desenvolvem ou operam sistemas de IA

que causem danos graves a direitos fundamentais.

4.3 A questão da personalidade jurídica da IA

Um debate ainda incipiente, mas relevante, diz respeito à possibilidade de atribuir personalidade jurídica a sistemas de inteligência artificial altamente autônomos. Alguns autores argumentam que, em situações onde a IA opera de forma completamente independente e imprevisível, seria necessário reconhecer alguma forma de responsabilidade própria do sistema.

Essa proposta, contudo, enfrenta resistências teóricas e práticas. A personalidade jurídica, no ordenamento brasileiro, pressupõe vontade e autodeterminação, atributos que

Ano V, v.2 2025 | submissão: 26/10/2025 | aceito: 28/10/2025 | publicação: 30/10/2025

sistemas de IA, por mais sofisticados, ainda não possuem. Além disso, reconhecer personalidade jurídica a algoritmos poderia criar escudo para desenvolvedores e operadores eximirem-se de responsabilidade.

A solução mais adequada, no estágio atual da tecnologia, é a manutenção da responsabilidade humana, com eventual criação de fundos de compensação para situações em que o responsável não possa ser identificado ou não tenha condições de reparar o dano.

Riscos constitucionais e propostas de governança algorítmica

O uso crescente de inteligência artificial em esferas sensíveis da vida social gera riscos constitucionais que exigem atenção urgente. Este capítulo identifica os principais riscos e propõe diretrizes para uma governança algorítmica democrática e constitucionalmente orientada.

A) Viés algorítmico e discriminação sistêmica

O viés algorítmico é, talvez, o risco mais documentado e preocupante. Quando sistemas de IA são treinados com dados que refletem desigualdades históricas, eles tendem a perpetuar e até amplificar essas discriminações.

No contexto brasileiro, marcado por profundas desigualdades raciais, sociais e regionais, esse risco é particularmente grave.

Pesquisas demonstram que algoritmos de reconhecimento facial apresentam maior taxa de erro para pessoas negras, que sistemas de avaliação de risco

criminal penalizam grupos vulneráveis e que algoritmos de recrutamento discriminam mulheres e pessoas de determinadas origens. Esses vieses não são acidentais: eles refletem estruturas de opressão presentes nos dados e nas escolhas de design dos sistemas.

A mitigação do viés algorítmico exige medidas específicas: auditoria externa e independente de sistemas de alto risco; diversidade nas equipes de desenvolvimento; testes rigorosos antes da implementação; monitoramento contínuo após a implantação; e mecanismos de correção e responsabilização quando discriminações forem identificadas.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano V, v.2 2025 | submissão: 26/10/2025 | aceito: 28/10/2025 | publicação: 30/10/2025

B) Vigilância em massa e controle social

O uso de IA para vigilância em massa representa grave ameaça à privacidade, à liberdade de expressão e à democracia. Sistemas de reconhecimento facial, monitoramento de redes sociais e análise preditiva de comportamentos permitem ao Estado rastrear, perfilar e controlar cidadãos em escala sem precedentes.

No Brasil, a ausência de regulação específica sobre vigilância algorítmica permite que órgãos de segurança pública implementem sistemas de monitoramento sem salvaguardas adequadas. Casos como o uso de reconhecimento facial em espaços públicos, sem autorização judicial ou transparência sobre critérios de seleção, levantam questões sobre compatibilidade com a Constituição Federal.

A vigilância em massa é incompatível com o Estado Democrático de Direito por diversas razões. Primeiro, ela inverte a lógica da presunção de inocência, tratando todos os cidadãos como suspeitos em potencial. Segundo ela inibe o exercício de direitos fundamentais, como a liberdade de expressão e de manifestação, ao criar um ambiente de constante monitoramento. Terceiro, ela concentra poder desproporcional nas mãos do Estado, sem controle democrático efetivo.

A regulação da vigilância algorítmica deve estabelecer limites claros: proibição de reconhecimento facial em tempo real em espaços públicos, salvo em situações excepcionais e com autorização judicial; transparência sobre sistemas de monitoramento utilizados pelo Estado; avaliação de impacto sobre direitos fundamentais antes da implementação; e mecanismos de fiscalização independente e participação social.

C) Manipulação informacional e integridade democrática

A inteligência artificial também pode ser utilizada para manipular o debate público e comprometer a integridade de processos democráticos. Deepfakes, contas automatizadas, microssegmentação de propaganda política e amplificação algorítmica de desinformação representam ameaças à democracia que exigem respostas regulatórias.

As eleições brasileiras de 2018 e 2022 evidenciaram a vulnerabilidade do sistema democrático à manipulação por meio de tecnologias digitais. Embora

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano V, v.2 2025 | submissão: 26/10/2025 | aceito: 28/10/2025 | publicação: 30/10/2025

o Tribunal Superior Eleitoral tenha adotado medidas de combate à desinformação, a sofisticação crescente de sistemas de IA exige atualização constante dos mecanismos de proteção.

Os deepfakes — vídeos, áudios ou imagens gerados por IA que simulam pessoas reais — são particularmente preocupantes. Eles podem ser utilizados para difamar adversários políticos, disseminar informações falsas e manipular a opinião pública. A dificuldade de identificar deepfakes e a velocidade de sua disseminação agravam o problema.

A regulação deve estabelecer obrigações de transparência para sistemas de IA utilizados em contextos eleitorais, proibir o uso de deepfakes para fins de manipulação política, exigir rotulagem de conteúdos gerados por IA e criar mecanismos ágeis de remoção de conteúdos manifestamente falsos que comprometam a integridade do processo eleitoral**.**

D) Automação de decisões públicas e erosão da accountability

A automação de decisões administrativas e judiciais por meio de IA pode comprometer princípios fundamentais como motivação, publicidade e accountability. Quando o Estado utiliza algoritmos para decidir sobre concessão de benefícios, aplicação de penalidades ou até mesmo em processos judiciais, deve garantir que essas decisões sejam transparentes, compreensíveis e passíveis de revisão.

A opacidade algorítmica é incompatível com o dever constitucional de motivação dos atos administrativos e judiciais. Decisões que afetam direitos não podem ser justificadas simplesmente pela afirmação de que "o sistema decidiu assim". É necessário que os critérios, os dados utilizados e a lógica de decisão sejam compreensíveis e auditáveis.

Além disso, a automação integral de decisões públicas pode gerar despersonalização e desumanização do serviço público. O direito de ser ouvido, de apresentar argumentos e de ter suas circunstâncias individuais consideradas é essencial para a dignidade e para a justiça. A IA pode auxiliar a administração pública, mas não pode substituir completamente o juízo humano em decisões que envolvam direitos fundamentais.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano V, v.2 2025 | submissão: 26/10/2025 | aceito: 28/10/2025 | publicação: 30/10/2025

E) Desigualdade algorítmica e exclusão digital

A implementação de sistemas de IA pode amplificar desigualdades existentes e criar novas formas de exclusão.

Comunidades vulneráveis, com menor acesso à tecnologia e à alfabetização digital, são as mais afetadas por decisões automatizadas e as menos capazes de contestá- las.

No Brasil, onde a desigualdade digital é profunda, a automação de serviços públicos sem considerar as barreiras de acesso pode excluir ainda mais grupos já marginalizados. Idosos, pessoas com deficiência, populações rurais e periféricas podem ter dificuldades de interagir com sistemas de IA ficando sem acesso a direitos e serviços.

A regulação deve garantir que a implementação de IA no setor público seja acompanhada de medidas de inclusão digital, que canais alternativos de atendimento humano sejam mantidos e que sistemas sejam projetados com acessibilidade e simplicidade.

F) Propostas para uma governança algorítmica democrática

Diante dos riscos identificados, é fundamental construir uma governança algorítmica que seja democrática, transparente e orientada pela Constituição Federal. As seguintes diretrizes são propostas:

a) Avaliação de impacto sobre direitos fundamentais: Sistemas de IA de alto risco deve ser submetidos a avaliação prévia de impacto sobre direitos fundamentais, com participação de especialistas independentes e da sociedade civil.

b) Transparência e explicabilidade: Desenvolvedores e operadores de sistemas de IA utilizados pelo Estado ou em contextos sensíveis devem divulgar informações sobre funcionamento, dados utilizados, critérios de decisão e métricas de desempenho.

c) Supervisão humana significativa: Decisões automatizadas que afetem direitos fundamentais devem ser passíveis de revisão humana qualificada, garantindo que algoritmos não substituam completamente o juízo humano.

d) Auditoria independente: Sistemas de alto risco deve ser auditados periodicamente

por entidades independentes, que verifiquem a conformidade com normas legais, a ausência de viés discriminatório e a adequação técnica.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano V, v.2 2025 | submissão: 26/10/2025 | aceito: 28/10/2025 | publicação: 30/10/2025

e) Participação social: A regulação e a implementação de sistemas de IA devem envolver consultas públicas, audiências e mecanismos de participação da sociedade civil, especialmente de grupos vulneráveis.

f) Responsabilização efetiva: Devem existir mecanismos claros de responsabilização civil, administrativa e, quando cabível, penal, para desenvolvedores e operadores que causem danos por uso inadequado de IA.

g) Educação e alfabetização digital: Políticas públicas devem promover a educação digital e a compreensão crítica sobre inteligência artificial, capacitando cidadãos para exercerem seus direitos em ambientes algorítmicos.

h) Pesquisa e inovação ética: O Estado deve fomentar pesquisa em IA ética, inclusiva e voltada ao interesse público, apoiando o desenvolvimento de tecnologias que respeitem direitos fundamentais.

6. CONCLUSÃO

A questão da responsabilidade jurídica em sistemas de IA mostrou-se particularmente complexa. A opacidade algorítmica, a autonomia crescente dos sistemas e a multiplicidade de atores envolvidos (desenvolvedores, fornecedores, operadores) dificultam a atribuição de responsabilidade segundo os modelos tradicionais. A inversão do ônus da prova, a responsabilidade solidária e a criação de fundos de compensação são caminhos possíveis, mas que exigem maior desenvolvimento teórico e normativo.

Os riscos constitucionais identificados — viés algorítmico, vigilância em massa, manipulação informacional, erosão da accountability e desigualdade algorítmica — não são meramente hipotéticos. Eles já se manifestam em diversos contextos, afetando especialmente grupos vulneráveis. A ausência de regulação adequada pode transformar a IA em instrumento de aprofundamento de desigualdades e violações de direitos, contrariando os valores democráticos e humanistas que fundamentam a Constituição de 1988.

As propostas de governança algorítmica apresentadas neste trabalho buscam equilibrar inovação e proteção de direitos, reconhecendo que a regulação não deve ser vista como obstáculo, mas como condição para o desenvolvimento sustentável e ético da inteligência artificial. Transparência, participação social, supervisão humana, auditoria independente e responsabilização efetiva são pilares indispensáveis para uma IA constitucionalmente orientada.

Ano V, v.2 2025 | submissão: 26/10/2025 | aceito: 28/10/2025 | publicação: 30/10/2025

É fundamental que o Brasil não reproduza erros cometidos em outras esferas tecnológicas, onde a ausência de regulação permitiu abusos que depois se tornaram difíceis de corrigir. A regulação da IA deve ser proativa, não apenas reativa; deve ser baseada em evidências e em diálogo com múltiplos atores; e deve estar em constante atualização, acompanhando a evolução tecnológica.

Além disso, a regulação brasileira não pode ser mera cópia de modelos estrangeiros. Embora a experiência internacional — especialmente o Regulamento Europeu de Inteligência Artificial — ofereça importantes lições, é necessário considerar as especificidades brasileiras: nossas desigualdades estruturais, nossa vulnerabilidade de dados, nosso contexto de fragilidade institucional e nossa diversidade regional. A regulação da IA no Brasil deve ser construída democraticamente, com ampla participação social e atenção especial aos grupos mais vulneráveis.

O desafio da regulação da inteligência artificial é, em última análise, o desafio de definir que tipo de sociedade queremos construir. Queremos uma sociedade onde a tecnologia sirva à dignidade humana, à justiça social e à democracia, ou aceitaremos que ela aprofunde desigualdades, viole direitos e concentre poder? A resposta a essa pergunta não é técnica, mas política e ética.

Este trabalho buscou contribuir para esse debate, oferecendo análise jurídica rigorosa e propositiva sobre a regulação da IA no Brasil. A construção de um marco regulatório adequado é responsabilidade compartilhada: do Poder Legislativo, que deve aprovar leis equilibradas e efetivas; do Poder Executivo, que deve implementar políticas públicas de fomento à IA ética; do Poder Judiciário, que deve interpretar a legislação à luz dos direitos fundamentais; da academia, que deve produzir conhecimento crítico e independente; das empresas, que devem desenvolver tecnologias responsáveis; e da sociedade civil, que deve participar ativamente da governança algorítmica.

A regulação da inteligência artificial no Brasil não é apenas uma questão técnica ou econômica: é um imperativo constitucional, um compromisso ético e uma exigência democrática. Que a tecnologia seja instrumento de libertação, não de opressão; de inclusão, não de exclusão; de justiça, não de desigualdade. Este é o horizonte que deve orientar a construção do marco regulatório brasileiro da inteligência artificial.

Ano V, v.2 2025 | submissão: 26/10/2025 | aceito: 28/10/2025 | publicação: 30/10/2025

REFERÊNCIAS

BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento.* Rio de Janeiro: Forense, 2019. Acesso em: 19 out. 2025.

BRASIL. *Constituição da República Federativa do Brasil de 1988.* Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 19 out. 2025.

BRASIL. *Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor.* Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 19 out. 2025.

BRASIL. *Lei nº 8.429, de 2 de junho de 1992. Lei de Improbidade Administrativa.* Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8429.htm. Acesso em: 19 out. 2025.

BRASIL. *Lei nº 10.406, de 10 de janeiro de 2002. Código Civil.* Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 20 out. 2025.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).* Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 out. 2025.

BRASIL. Ministério da Ciência, Tecnologia e Inovações. *Estratégia Brasileira de Inteligência Artificial (EBIA).* Brasília: MCTI, 2021. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-summary_brazilian_4-979_2021.pdf. Acesso em: 20 out. 2025.

BRASIL. *Projeto de Lei nº 2.338, de 2023. Dispõe sobre o uso da Inteligência Artificial.* Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 20 out. 2025.

BUOLAMWINI, Joy; GEBRU, Timnit. *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research*, v. 81, p. 1–15, 2018. Acesso em: 20 out. 2025.

CONSELHO NACIONAL DE JUSTIÇA. *Resolução CNJ nº 332, de 21 de agosto de 2020. Dispõe sobre a ética, a transparência e a governança na produção e no uso de Inteligência Artificial no Poder Judiciário.* Disponível em: https://atos.cnj.jus.br/atos/detalhar/3429. Acesso em: 20 out. 2025.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados.* 2. ed. São Paulo: Thomson Reuters Brasil, 2019. Acesso em: 20 out. 2025.

Ano V, v.2 2025 | submissão: 26/10/2025 | aceito: 28/10/2025 | publicação: 30/10/2025

FRAZÃO, Ana; MULHOLLAND, Caitlin (Org.). *Inteligência artificial e direito: ética, regulação e responsabilidade.* 2. ed. São Paulo: Thomson Reuters Brasil, 2020. Acesso em: 21 out. 2025.

MAGRANI, Eduardo. *A internet das coisas.* Rio de Janeiro: FGV Editora, 2018. Acesso em: 21 out. 2025.

MENDES, Laura Schertel; DONEDA, Danilo. *Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. Revista de Direito do Consumidor*, v. 120, p. 469–483, nov./dez. 2018. Acesso em: 21 out. 2025.

MULHOLLAND, Caitlin. *Responsabilidade civil por danos causados por inteligência artificial.* In: FRAZÃO, Ana; MULHOLLAND, Caitlin (Org.). *Inteligência artificial e direito: ética, regulação e responsabilidade.* 2. ed. São Paulo: Thomson Reuters Brasil, 2020. p. 375–408. Acesso em: 22 out. 2025.

NOBLE, Safiya Umoja. *Algorithms of oppression: how search engines reinforce racism.* New York: New York University Press, 2018. Acesso em: 22 out. 2025.

O'NEIL, Cathy. *Weapons of math destruction: how big data increases inequality and threatens democracy.* New York: Crown, 2016. Acesso em: 22 out. 2025.

PASQUALE, Frank. *The black box society: the secret algorithms that control money and information.* Cambridge: Harvard University Press, 2015. Acesso em: 22 out. 2025.

RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje.* Organização de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. Acesso em: 23 out. 2025.

SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional.* 13. ed. Porto Alegre: Livraria do Advogado, 2018. Acesso em: 23 out. 2025.

SCHREIBER, Anderson. *Direitos da personalidade.* 3. ed. São Paulo: Atlas, 2014. Acesso em: 23 out. 2025.

SILVA, Tarcízio. *Visão computacional e racismo algorítmico: branquitude e opacidade no aprendizado de máquina. Revista da Associação Brasileira de Pesquisadores/as Negros/as (ABPN)*, v. 12, n. 31, p. 428–448, 2020. Acesso em: 24 out. 2025.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. *Tratamento de dados pessoais na LGPD: estudo sobre as bases legais.* São Paulo: Thomson Reuters Brasil, 2020. Acesso em: 24 out. 2025.

UNIÃO EUROPEIA. *Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas em matéria de inteligência artificial. Jornal Oficial da União Europeia*, L 1689, 12 jul. 2024. Acesso em: 24 out. 2025.

Ano V, v.2 2025 | submissão: 26/10/2025 | aceito: 28/10/2025 | publicação: 30/10/2025

ZANATTA, Rafael A. F. *Perfilização, discriminação e direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais.* Salvador: JusPodivm, 2019. Acesso em: 24 out. 2025.

ZUBOFF, Shoshana. *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder.* Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2020. Acesso em: 24 out. 2025.