REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

GOVERNANÇA ALGORÍTMICA, CONSTITUCIONALISMO TECNOLÓGICO E DIREITOS FUNDAMENTAIS: DESAFIOS JURÍDICOS DA INTELIGÊNCIA ARTIFICIAL NO ESTADO DEMOCRÁTICO DE DIREITO

ALGORITHMIC GOVERNANCE, TECHNOLOGICAL CONSTITUTIONALISM AND FUNDAMENTAL RIGHTS: LEGAL CHALLENGES OF ARTIFICIAL INTELLIGENCE IN THE DEMOCRATIC RULE OF LAW

Ciências Humanas, Ciências Sociais Aplicadas • 24/07/2026

REGISTRO DOI: 10.70773/revistatopicos/784688151

Marcus Rômulo Brito Pinto[1]

Ana Caroline da Silva Taumaturgo[2]

Lazúli Lua de Carvalho Peres[3]

Ana Paula Felismino da Silva[4]

João Gabriel Amanso da Conceição[5]

Aline Tavares Pereira Felipe[6]

João Paulo Avelino Alves de Sousa[7]

Igor Vasconcelos Canuto[8]

Jumario Gomes de Medeiros Junior[9]

Odaíze do Socorro Ferreira Cavalcante Lima[10]

RESUMO

A expansão dos sistemas de inteligência artificial tem provocado profundas transformações nas estruturas de decisão pública e privada, impondo novos desafios à proteção dos direitos fundamentais e à preservação dos princípios constitucionais que sustentam o Estado Democrático de Direito. A utilização crescente de algoritmos em políticas públicas, segurança, crédito, saúde, educação, relações de consumo, trabalho, comunicação digital, justiça, administração pública e serviços privados amplia a capacidade de processamento informacional, mas também intensifica riscos de discriminação automatizada, opacidade decisória, vigilância, manipulação comportamental, violação de privacidade, exclusão social e enfraquecimento do devido processo legal. Nesse contexto, o presente artigo analisa a emergência do constitucionalismo tecnológico como campo jurídico voltado à regulação das tecnologias inteligentes, à contenção dos riscos decorrentes da governança algorítmica e à reafirmação da centralidade da dignidade humana em ambientes digitais complexos. A pesquisa adota abordagem qualitativa, bibliográfica, documental e jurídico-analítica, fundamentada em doutrina constitucional, teoria dos direitos fundamentais, proteção de dados, ética da inteligência artificial, regulação digital e experiências normativas internacionais, especialmente a Lei Geral de Proteção de Dados, o Marco Civil da Internet, o AI Act europeu, os princípios da OCDE, a Recomendação da UNESCO sobre Ética da IA e o debate brasileiro em torno do marco legal da inteligência artificial. O estudo demonstra que a governança algorítmica desloca parte do poder decisório para sistemas técnicos que classificam, ranqueiam, recomendam, preveem e automatizam decisões com impacto direto sobre pessoas e grupos sociais. Os resultados indicam a necessidade de mecanismos de transparência, explicabilidade,

auditabilidade, responsabilização, avaliação de impacto algorítmico, supervisão humana, controle democrático e proteção contra discriminações automatizadas. Conclui-se que a efetividade dos direitos fundamentais na era da inteligência artificial depende da construção de um constitucionalismo tecnológico capaz de equilibrar inovação, segurança jurídica, proteção de dados, justiça social, controle público e limitação constitucional do poder computacional.

Palavras-chave: governança algorítmica; constitucionalismo tecnológico; inteligência artificial; direitos fundamentais; proteção de dados; Estado Democrático de Direito; transparência algorítmica; regulação digital.

ABSTRACT

The expansion of artificial intelligence systems has deeply transformed public and private decision-making structures, creating new challenges for the protection of fundamental rights and the preservation of constitutional principles that sustain the Democratic Rule of Law. The growing use of algorithms in public policy, security, credit, health, education, consumer relations, labour, digital communication, justice, public administration and private services increases informational processing capacity, but also intensifies risks of automated discrimination, decision-making opacity, surveillance, behavioural manipulation, privacy violations, social exclusion and weakening of due process. In this context, this article analyzes the emergence of technological constitutionalism as a legal field aimed at regulating intelligent technologies, containing the risks arising from algorithmic governance and reaffirming the centrality of human dignity in complex digital environments. The research adopts a qualitative, bibliographic, documentary and legal-analytical approach, based on constitutional doctrine, theory of fundamental

rights, data protection, artificial intelligence ethics, digital regulation and international regulatory experiences, especially the Brazilian General Data Protection Law, the Brazilian Civil Rights Framework for the Internet, the European AI Act, OECD AI Principles, UNESCO Recommendation on the Ethics of Artificial Intelligence and the Brazilian debate on the legal framework for artificial intelligence. The study demonstrates that algorithmic governance shifts part of decision-making power to technical systems that classify, rank, recommend, predict and automate decisions with direct impact on individuals and social groups. The results indicate the need for mechanisms of transparency, explainability, auditability, accountability, algorithmic impact assessment, human oversight, democratic control and protection against automated discrimination. The article concludes that the effectiveness of fundamental rights in the age of artificial intelligence depends on the construction of a technological constitutionalism capable of balancing innovation, legal certainty, data protection, social justice, public oversight and constitutional limitation of computational power.

Keywords: algorithmic governance; technological constitutionalism; artificial intelligence; fundamental rights; data protection; Democratic Rule of Law; algorithmic transparency; digital regulation.

1. INTRODUÇÃO

A inteligência artificial tornou-se uma das tecnologias estruturantes da sociedade contemporânea. Sistemas algorítmicos são utilizados para recomendar conteúdos, analisar perfis de consumo, selecionar candidatos a emprego, prever riscos de crédito, apoiar diagnósticos médicos, identificar padrões de fraude, classificar contribuintes, monitorar espaços públicos, orientar decisões administrativas,

automatizar atendimentos, produzir textos, gerar imagens, analisar processos judiciais e organizar fluxos informacionais em larga escala. Esse avanço altera profundamente a forma como o poder é exercido, distribuído e controlado na sociedade digital (PASQUALE, 2015; O'NEIL, 2016; ZUBOFF, 2019).

A promessa da inteligência artificial está associada à eficiência, rapidez, personalização, redução de custos, automação de tarefas repetitivas e ampliação da capacidade analítica. Contudo, a mesma tecnologia que pode melhorar serviços públicos e privados também pode produzir discriminações, invisibilizar vulnerabilidades, reforçar desigualdades, ampliar vigilância, dificultar contestação de decisões e deslocar responsabilidades humanas para sistemas opacos. A IA, portanto, não é apenas questão técnica; é questão constitucional, democrática e jurídica (BAROCAS; SELBST, 2016; CRAWFORD, 2021; EUBANKS, 2018).

A governança algorítmica designa o conjunto de práticas, regras, arquiteturas, modelos e instituições por meio dos quais decisões são orientadas, mediadas ou automatizadas por sistemas computacionais. Trata-se de fenômeno que desloca parte do poder decisório para infraestruturas digitais capazes de classificar pessoas, prever comportamentos, recomendar ações, atribuir riscos e modular oportunidades. Essa forma de governança pode ocorrer tanto no setor público quanto no setor privado, afetando direitos fundamentais e condições de acesso a bens essenciais (YEUNG, 2018; KITCHIN, 2017).

O constitucionalismo tecnológico surge como resposta a esse novo cenário. Se o constitucionalismo moderno foi construído para limitar o poder político e proteger direitos fundamentais contra

arbitrariedades estatais, o constitucionalismo tecnológico busca limitar formas contemporâneas de poder digital, inclusive aquelas exercidas por grandes plataformas privadas, sistemas automatizados, infraestruturas de dados e modelos de IA. O poder computacional tornou-se elemento relevante da vida social e, por isso, deve ser submetido a princípios constitucionais (CELESTE, 2019; DE GREGORIO, 2022; SUZOR, 2019).

No Estado Democrático de Direito, a tecnologia não pode ser situada acima da Constituição. Sistemas de inteligência artificial precisam respeitar dignidade humana, igualdade, liberdade, privacidade, proteção de dados, devido processo legal, ampla defesa, não discriminação, transparência, controle social, proporcionalidade e responsabilidade. A inovação tecnológica deve ser compatível com o núcleo normativo do constitucionalismo democrático (SARLET, 2022; CANOTILHO, 2003; FLORIDI; COWLS, 2019).

A dificuldade está em aplicar categorias jurídicas tradicionais a sistemas técnicos complexos, probabilísticos e frequentemente opacos. Muitos modelos de IA operam por aprendizado estatístico, extraindo padrões de grandes bases de dados. O resultado pode ser tecnicamente eficiente, mas juridicamente problemático quando produz decisões sem explicação compreensível, sem possibilidade de contestação ou com impactos discriminatórios. O problema não é apenas saber se o algoritmo funciona, mas se ele funciona de modo compatível com direitos fundamentais (WACHTER; MITTELSTADT; FLORIDI, 2017; RUDIN, 2019).

No Brasil, esse debate se articula com a Constituição Federal de 1988, com a Lei Geral de Proteção de Dados Pessoais, com o Marco Civil da Internet e com a discussão legislativa sobre o marco legal da

inteligência artificial. A Emenda Constitucional nº 115/2022 incluiu a proteção de dados pessoais no rol de direitos fundamentais, reforçando o caráter constitucional da governança informacional. A LGPD, por sua vez, trouxe princípios como finalidade, necessidade, transparência, segurança, prevenção, responsabilização e prestação de contas, que dialogam diretamente com a regulação de sistemas algorítmicos (DONEDA, 2021; MENDES, 2020; BIONI, 2021).

No plano internacional, o AI Act europeu consolidou abordagem regulatória baseada em risco, diferenciando usos proibidos, sistemas de alto risco, obrigações de transparência e regras para modelos de propósito geral. A OCDE e a UNESCO também formularam princípios voltados à IA confiável, centrada no ser humano, respeitosa dos direitos humanos, transparente, segura e responsável. Essas experiências revelam uma tendência global: a inteligência artificial deixou de ser tratada apenas como inovação econômica e passou a ser objeto de constitucionalização regulatória (UNIÃO EUROPEIA, 2024; OCDE, 2024; UNESCO, 2021).

Diante desse cenário, o presente artigo parte do seguinte problema de pesquisa: **como a governança algorítmica desafia a proteção dos direitos fundamentais e de que modo o constitucionalismo tecnológico pode oferecer parâmetros jurídicos para regular a inteligência artificial no Estado Democrático de Direito?**

O objetivo geral é analisar os desafios jurídicos da inteligência artificial a partir da relação entre governança algorítmica, constitucionalismo tecnológico e direitos fundamentais. Como objetivos específicos, busca-se: compreender o conceito de governança algorítmica; discutir a emergência do constitucionalismo tecnológico; examinar impactos da IA sobre

privacidade, igualdade, liberdade, devido processo e proteção de dados; analisar experiências normativas nacionais e internacionais; e propor diretrizes para uma governança algorítmica democrática, transparente e responsável.

A hipótese central é que a inteligência artificial exige novo paradigma jurídico-constitucional, pois desloca o poder decisório para sistemas técnicos capazes de produzir impactos massivos, opacos e assimétricos. A proteção dos direitos fundamentais na era digital depende da construção de mecanismos jurídicos de controle algorítmico, avaliação de impacto, transparência, supervisão humana, auditoria e responsabilização.

2. METODOLOGIA

A pesquisa adota abordagem qualitativa, bibliográfica, documental, comparada e jurídico-analítica. A escolha metodológica justifica-se pela natureza interdisciplinar do tema, que envolve Direito Constitucional, Direito Digital, proteção de dados, teoria dos direitos fundamentais, regulação da inteligência artificial, ética tecnológica, ciência de dados, governança pública e filosofia política (MINAYO, 2014; GIL, 2019).

A pesquisa bibliográfica fundamenta-se em autores nacionais e estrangeiros que tratam de constitucionalismo, direitos fundamentais, tecnologia, governança algorítmica, proteção de dados e regulação da inteligência artificial. No campo constitucional, utilizam-se referências como Canotilho, Sarlet, Alexy, Dworkin, Habermas e Bobbio. No campo do Direito Digital e da governança tecnológica, são mobilizados autores como Lessig, Pasquale, Hildebrandt, Cohen, DeNardis, Suzor, De Gregorio, Celeste, Floridi,

Doneda, Mendes e Bioni. No campo crítico da IA, são considerados Barocas e Selbst, O'Neil, Eubanks, Crawford, Zuboff, Wachter, Mittelstadt, Floridi e Rudin.

A pesquisa documental examina normas e documentos relevantes, entre eles a Constituição Federal de 1988, a Lei Geral de Proteção de Dados, o Marco Civil da Internet, o AI Act europeu, os princípios da OCDE sobre inteligência artificial, a Recomendação da UNESCO sobre Ética da IA, o Regulamento Geral de Proteção de Dados da União Europeia e o Projeto de Lei nº 2.338/2023, que propõe marco regulatório brasileiro para inteligência artificial.

A análise comparada é utilizada para identificar tendências regulatórias internacionais. O objetivo não é transpor mecanicamente soluções estrangeiras ao Brasil, mas compreender como diferentes sistemas jurídicos têm enfrentado riscos algorítmicos, especialmente por meio de abordagem baseada em risco, deveres de transparência, avaliação de impacto, direitos dos afetados, auditorias e responsabilização.

O método jurídico-analítico orienta a interpretação dos impactos da IA sobre direitos fundamentais. A análise parte da premissa de que o desenvolvimento tecnológico deve ser submetido à Constituição e aos princípios do Estado Democrático de Direito. Dessa forma, a pesquisa avalia não apenas a eficiência das tecnologias, mas sua legitimidade jurídica, sua proporcionalidade e sua compatibilidade com a dignidade humana.

A estrutura do artigo está organizada em dezessete seções. Após a introdução e a metodologia, são abordados: governança algorítmica; constitucionalismo tecnológico; inteligência artificial e poder;

privacidade e proteção de dados; igualdade e discriminação algorítmica; liberdade de expressão e plataformas; devido processo legal algorítmico; transparência, explicabilidade e auditabilidade; responsabilização; regulação comparada; administração pública algorítmica; resultados; discussão; diretrizes de governança; considerações finais e referências.

3. GOVERNANÇA ALGORÍTMICA: CONCEITO, ALCANCE E RISCOS

A governança algorítmica pode ser compreendida como o uso de sistemas computacionais para orientar, regular, automatizar ou influenciar decisões sociais, econômicas, políticas e administrativas. Ela ocorre quando algoritmos passam a classificar indivíduos, ordenar prioridades, prever comportamentos, distribuir recursos, recomendar conteúdos, detectar riscos ou automatizar decisões. Nesse contexto, o algoritmo não é apenas instrumento técnico, mas parte de uma estrutura de poder (YEUNG, 2018; KITCHIN, 2017).

A palavra “algoritmo” costuma transmitir aparência de neutralidade matemática. No entanto, algoritmos são construídos por pessoas, empresas, governos e instituições, com base em dados, escolhas metodológicas, objetivos econômicos, parâmetros estatísticos e decisões políticas. Por isso, não há governança algorítmica neutra. Todo sistema computacional incorpora pressupostos sobre o que medir, como classificar, quais erros tolerar e quais resultados otimizar (BAROCAS; SELBST, 2016; PASQUALE, 2015).

Na esfera privada, algoritmos são usados para análise de crédito, publicidade comportamental, recomendação de conteúdos, contratação de trabalhadores, precificação dinâmica, moderação de plataformas, seguros, marketing, vigilância de produtividade e

personalização de serviços. Na esfera pública, são utilizados em segurança, fiscalização tributária, concessão de benefícios, saúde, educação, justiça, controle migratório, políticas sociais e gestão urbana (O'NEIL, 2016; EUBANKS, 2018; CRAWFORD, 2021).

Os riscos surgem porque decisões algorítmicas podem ser tomadas em larga escala, com velocidade elevada, baixa transparência e forte impacto sobre pessoas. Um erro humano isolado pode afetar poucos casos; um erro algorítmico sistêmico pode afetar milhares ou milhões de pessoas. Além disso, modelos de IA podem reproduzir vieses históricos presentes nos dados, amplificando discriminações de raça, gênero, classe, território, deficiência, idade ou orientação social (BAROCAS; SELBST, 2016; BENJAMIN, 2019).

A governança algorítmica também pode gerar opacidade. Sistemas complexos de aprendizado de máquina nem sempre oferecem explicações compreensíveis sobre seus resultados. Essa opacidade pode decorrer de segredo empresarial, complexidade técnica, ausência de documentação ou desenho intencionalmente fechado. Quando decisões relevantes são opacas, o cidadão perde capacidade de compreender, contestar e responsabilizar quem decide (PASQUALE, 2015; WACHTER; MITTELSTADT; FLORIDI, 2017).

Outro risco é a automação da desigualdade. Eubanks (2018) demonstra que sistemas automatizados podem administrar pobreza e vulnerabilidade de modo punitivo, classificando pessoas como riscos, fraudes ou custos. Em vez de ampliar direitos, a tecnologia pode reforçar mecanismos de exclusão quando aplicada sem sensibilidade social, sem controle democrático e sem avaliação de impacto.

A governança algorítmica também altera a relação entre Estado e cidadão. Quando decisões administrativas são mediadas por IA, o indivíduo pode enfrentar barreiras técnicas para compreender por que foi negado um benefício, selecionado para fiscalização, classificado como risco ou excluído de uma política pública. O devido processo legal exige que decisões estatais sejam justificadas, proporcionais e contestáveis (CITRON, 2008; HILDEBRANDT, 2015).

A questão central é que algoritmos governam não apenas por coerção direta, mas por modulação. Eles organizam escolhas, exibem opções, ocultam alternativas, priorizam informações, definem reputações e orientam condutas. Esse poder de arquitetura foi antecipado por Lessig (1999), ao afirmar que o código pode funcionar como forma de regulação. Na era da IA, o código não apenas regula ambientes digitais, mas também produz decisões sociais automatizadas.

Portanto, a governança algorítmica exige constitucionalização. Não basta confiar em autorregulação privada ou eficiência técnica. Decisões algorítmicas que afetam direitos fundamentais precisam ser submetidas a limites jurídicos, fiscalização pública, transparência, auditoria e responsabilização.

4. CONSTITUCIONALISMO TECNOLÓGICO E LIMITAÇÃO DO PODER DIGITAL

O constitucionalismo nasceu como projeto de limitação do poder. Sua finalidade histórica foi impedir arbitrariedades, proteger direitos fundamentais, organizar competências e submeter o exercício do poder a regras superiores. No Estado Democrático de Direito,

nenhum poder deve operar sem controle jurídico, legitimidade democrática e responsabilidade (CANOTILHO, 2003; BOBBIO, 1992).

A transformação digital criou novas formas de poder. Grandes plataformas controlam fluxos comunicacionais, dados, mercados, reputações, identidades digitais e infraestruturas de interação social. Sistemas de IA influenciam decisões públicas e privadas. Bancos de dados e modelos preditivos permitem classificar comportamentos e antecipar riscos. O poder contemporâneo não se concentra apenas no Estado; ele também se manifesta em arquiteturas digitais privadas e híbridas (ZUBOFF, 2019; DE GREGORIO, 2022).

O constitucionalismo tecnológico surge para enfrentar esse deslocamento. Ele busca aplicar princípios constitucionais à governança de tecnologias digitais, especialmente quando infraestruturas privadas passam a exercer funções quase públicas. Plataformas de busca, redes sociais, sistemas de pagamento, serviços de nuvem, aplicativos e sistemas de IA podem afetar direitos de expressão, privacidade, igualdade, trabalho, acesso à informação e participação política (CELESTE, 2019; SUZOR, 2019).

Esse novo constitucionalismo não significa criar uma Constituição para cada tecnologia. Significa reconhecer que a Constituição deve orientar o desenho, a regulação e a aplicação de sistemas tecnológicos que estruturam a vida social. A tecnologia não é externa ao Direito; ela passa a compor o ambiente em que direitos são exercidos ou violados (HILDEBRANDT, 2015; COHEN, 2019).

O constitucionalismo tecnológico possui três dimensões. A primeira é normativa: direitos fundamentais devem ser aplicáveis a ambientes digitais. A segunda é institucional: autoridades públicas

precisam criar mecanismos de supervisão, fiscalização e responsabilização. A terceira é arquitetural: sistemas tecnológicos devem ser desenhados com proteção de direitos desde a concepção, em lógica próxima ao privacy by design, safety by design e rights by design (CAVOUKIAN, 2011; FLORIDI; COWLS, 2019).

A dignidade humana é seu eixo central. Sistemas algorítmicos não podem reduzir pessoas a perfis estatísticos, pontuações de risco ou objetos de manipulação comportamental. A pessoa deve permanecer sujeito de direitos, capaz de compreender decisões relevantes, contestar resultados, proteger seus dados e não ser submetida a discriminação automatizada (SARLET, 2022; MENDES, 2020).

O constitucionalismo tecnológico também exige proporcionalidade. A adoção de IA pelo Estado ou por agentes privados em áreas sensíveis deve observar adequação, necessidade e proporcionalidade em sentido estrito. Não basta que o sistema seja útil; é necessário demonstrar que não existe alternativa menos lesiva, que os benefícios superam os riscos e que há salvaguardas suficientes (ALEXY, 2008; SARLET, 2022).

Outro elemento é a accountability. Sistemas de IA não podem criar zonas de irresponsabilidade. O fato de a decisão ter sido produzida por modelo estatístico não elimina responsabilidade de desenvolvedores, fornecedores, operadores, gestores públicos ou empresas usuárias. A delegação técnica não pode significar abdicação jurídica (CITRON; PASQUALE, 2014; KROLL et al., 2017).

O constitucionalismo tecnológico, portanto, afirma que a tecnologia deve ser governada constitucionalmente. O Estado Democrático de

Direito não pode aceitar que decisões automatizadas afetem direitos fundamentais sem transparência, controle, justificativa e possibilidade de contestação.

5. INTELIGÊNCIA ARTIFICIAL, PODER E DEMOCRACIA

A inteligência artificial amplia a capacidade de análise, previsão e automação de decisões. Essa capacidade pode beneficiar políticas públicas, pesquisa científica, diagnóstico médico, gestão ambiental, educação personalizada, segurança cibernética e eficiência administrativa. Entretanto, a IA também altera a distribuição do poder social, pois quem controla dados, infraestrutura computacional e modelos passa a influenciar decisões em escala (CRAWFORD, 2021; ZUBOFF, 2019).

A democracia depende de transparência, pluralismo, deliberação pública, controle institucional e participação cidadã. Sistemas de IA podem fortalecer esses valores quando usados para ampliar acesso a serviços, detectar desigualdades, melhorar gestão pública e apoiar decisões fundamentadas. Porém, podem enfraquecê-los quando operam como mecanismos opacos de vigilância, manipulação informacional, microdirecionamento político ou exclusão automatizada (SUNSTEIN, 2017; BENKLER; FARIS; ROBERTS, 2018).

A personalização algorítmica das informações afeta a esfera pública. Plataformas digitais selecionam conteúdos conforme métricas de engajamento, interesses comerciais e perfis comportamentais. Essa mediação pode produzir bolhas informacionais, radicalização, desinformação e manipulação de preferências. O problema não está apenas na liberdade de expressão individual, mas na integridade do

debate democrático (SUNSTEIN, 2017; BENKLER; FARIS; ROBERTS, 2018).

O uso de IA pelo Estado também exige cautela. Sistemas preditivos em segurança pública, assistência social, fiscalização ou justiça podem produzir decisões com aparência técnica, mas fundadas em dados históricos contaminados por desigualdades. Quando um modelo aprende com padrões discriminatórios do passado, pode projetar esses padrões para o futuro, transformando injustiça histórica em previsão automatizada (O'NEIL, 2016; EUBANKS, 2018).

A democracia exige que decisões públicas sejam justificáveis. Se um cidadão é privado de benefício, submetido a fiscalização, classificado como risco ou afetado por decisão automatizada, deve haver possibilidade de conhecer fundamentos, apresentar defesa e obter revisão humana. A automação não pode eliminar a racionalidade pública exigida pelo Estado de Direito (CITRON, 2008; HILDEBRANDT, 2015).

O poder privado das grandes empresas de tecnologia também desafia categorias tradicionais. Plataformas definem regras de moderação, acesso, visibilidade, monetização e circulação de informações. Em muitos casos, essas decisões afetam direitos em escala superior à atuação de diversos Estados. Daí a necessidade de pensar constitucionalismo também em relação a poderes privados digitais (SUZOR, 2019; DE GREGORIO, 2022).

A IA generativa intensifica esse quadro. Modelos capazes de produzir textos, imagens, vídeos, códigos e sínteses informacionais podem apoiar criatividade e produtividade, mas também facilitar desinformação, deepfakes, fraudes, manipulação de opinião pública

e violação de direitos autorais. O desafio democrático é regular riscos sem sufocar usos legítimos e inovadores (BOMMASANI et al., 2021; BENDER et al., 2021).

A relação entre IA e democracia deve ser tratada sob perspectiva de legitimidade. A pergunta não é apenas se o sistema é eficiente, mas se sua decisão é legítima, controlável, proporcional, não discriminatória e compatível com direitos fundamentais. A democracia não pode ser substituída por tecnocracia algorítmica (HABERMAS, 1997; FLORIDI; COWLS, 2019).

6. PRIVACIDADE, PROTEÇÃO DE DADOS E AUTODETERMINAÇÃO INFORMATIVA

A privacidade é um dos direitos mais impactados pela inteligência artificial. Sistemas de IA dependem de dados para treinamento, validação, operação e aperfeiçoamento. Quanto maior a quantidade e variedade de dados, maior tende a ser a capacidade de inferência. Essa lógica estimula coleta massiva, cruzamento de bases, monitoramento comportamental e criação de perfis detalhados de indivíduos e grupos (DONEDA, 2021; ZUBOFF, 2019).

A proteção de dados pessoais tornou-se direito fundamental justamente porque a vida contemporânea é mediada por fluxos informacionais. Dados não são meros registros neutros; eles permitem inferir hábitos, preferências, saúde, localização, condição econômica, relações sociais, opiniões políticas, religião, vulnerabilidades e comportamentos futuros. Controlar dados significa, em parte, controlar possibilidades de vida (MENDES, 2020; BIONI, 2021).

A LGPD brasileira estabelece princípios que são diretamente aplicáveis à governança algorítmica. Finalidade exige que o tratamento de dados tenha propósito legítimo, específico e informado. Necessidade impõe limitação ao mínimo necessário. Transparência exige informações claras. Segurança e prevenção demandam proteção contra riscos. Responsabilização e prestação de contas impõem dever de demonstrar conformidade (DONEDA, 2021; BIONI, 2021).

A decisão automatizada é ponto sensível. Sistemas de IA podem decidir sobre crédito, seguro, emprego, benefícios, preços, acesso a serviços e riscos. A LGPD prevê direito de solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem interesses do titular. Esse dispositivo é essencial para enfrentar a opacidade algorítmica, embora sua efetividade dependa de regulamentação, fiscalização e interpretação robusta (MENDES, 2020; WACHTER; MITTELSTADT; FLORIDI, 2017).

A autodeterminação informativa significa que a pessoa deve ter controle significativo sobre seus dados e sobre os usos que podem afetar sua vida. Em contexto de IA, esse controle não pode ser reduzido a consentimento formal. Muitas vezes, o titular não compreende a complexidade do tratamento, não possui alternativa real ou não consegue prever inferências futuras. Por isso, a proteção de dados exige bases legais adequadas, minimização, avaliação de impacto e governança institucional (DONEDA, 2021; BIONI, 2021).

A IA também permite inferências sobre dados sensíveis mesmo quando eles não são diretamente coletados. Um sistema pode inferir saúde, religião, orientação política, vulnerabilidade econômica

ou origem social a partir de padrões de navegação, localização ou consumo. Essa capacidade desafia a distinção tradicional entre dados sensíveis e não sensíveis, exigindo análise de risco contextual (BAROCAS; SELBST, 2016; CRAWFORD, 2021).

A vigilância algorítmica é outro problema. O uso de reconhecimento facial, monitoramento biométrico, análise comportamental e rastreamento em espaços públicos pode afetar liberdade, anonimato, participação política e presunção de inocência. Em sociedades democráticas, tecnologias de vigilância devem ser submetidas a legalidade estrita, necessidade, proporcionalidade, finalidade pública legítima e controle independente (LYON, 2018; ZUBOFF, 2019).

Portanto, a proteção de dados é uma das bases do constitucionalismo tecnológico. Sem limites ao tratamento informacional, a inteligência artificial pode transformar cidadãos em objetos permanentes de análise, previsão e manipulação.

7. IGUALDADE, NÃO DISCRIMINAÇÃO E VIÉS ALGORÍTMICO

A igualdade é um dos direitos fundamentais mais desafiados pela inteligência artificial. Sistemas algorítmicos podem discriminar mesmo sem intenção explícita. Isso ocorre porque modelos aprendem padrões a partir de dados históricos, e esses dados podem refletir desigualdades sociais, raciais, territoriais, econômicas ou de gênero. Quando o passado é injusto, o modelo pode reproduzir e automatizar a injustiça (BAROCAS; SELBST, 2016; BENJAMIN, 2019).

A discriminação algorítmica pode ocorrer em diferentes etapas. Pode surgir na coleta de dados, quando determinados grupos são

sub-representados. Pode aparecer na definição da variável-alvo, quando se escolhe medir risco, produtividade ou mérito com indicadores enviesados. Pode ocorrer no treinamento, quando o modelo aprende correlações problemáticas. Pode manifestar-se na implantação, quando o sistema funciona pior para determinados grupos (BAROCAS; SELBST, 2016; O'NEIL, 2016).

O reconhecimento facial é exemplo recorrente. Estudos demonstraram que sistemas biométricos podem apresentar taxas de erro diferentes conforme raça e gênero, especialmente quando treinados com bases pouco representativas. Em contexto de segurança pública, esse tipo de erro pode gerar abordagens indevidas, prisões injustas e reforço de seletividade penal (BUOLAMWINI; GEBRU, 2018; BENJAMIN, 2019).

Na área de crédito, algoritmos podem usar variáveis aparentemente neutras, como endereço, histórico de consumo ou tipo de dispositivo, que funcionam como proxies de classe social ou raça. Na área trabalhista, sistemas de seleção podem penalizar mulheres, pessoas mais velhas ou grupos sub-representados se treinados com dados históricos de contratação discriminatória (O'NEIL, 2016; AJUNWA, 2020).

A igualdade algorítmica não se resolve apenas removendo variáveis sensíveis. Mesmo sem raça, gênero ou deficiência, modelos podem inferir essas características por correlações indiretas. A não discriminação exige avaliação de impacto, testes de equidade, auditorias independentes, diversidade de dados, monitoramento contínuo e possibilidade de contestação (BAROCAS; SELBST, 2016; RAGHAVAN et al., 2020).

O constitucionalismo tecnológico deve reconhecer que neutralidade matemática não equivale a justiça constitucional. Um modelo pode ser estatisticamente preciso e juridicamente discriminatório. A avaliação jurídica deve considerar efeitos concretos sobre grupos vulneráveis, e não apenas métricas globais de acurácia (EUBANKS, 2018; CRAWFORD, 2021).

A proporcionalidade também é relevante. Em sistemas de alto risco, especialmente aqueles usados em segurança pública, assistência social, emprego, crédito, saúde e educação, a exigência de validação, transparência e supervisão deve ser maior. Quanto mais grave o impacto sobre direitos, maior o dever de controle jurídico (ALEXY, 2008; UNIÃO EUROPEIA, 2024).

A igualdade exige ainda participação social. Grupos afetados por sistemas algorítmicos devem ter voz na avaliação de riscos. A auditoria puramente técnica pode ignorar impactos vividos por comunidades vulneráveis. Por isso, governança algorítmica democrática deve incluir escuta pública, controle social e transparência institucional (BENJAMIN, 2019; EUBANKS, 2018).

Assim, a proteção contra viés algorítmico é uma exigência constitucional. A IA não pode ser utilizada para automatizar desigualdades sob aparência de objetividade.

8. LIBERDADE DE EXPRESSÃO, PLATAFORMAS DIGITAIS E MODERAÇÃO ALGORÍTMICA

A liberdade de expressão é profundamente afetada por plataformas digitais e sistemas algorítmicos de recomendação, moderação e ranqueamento. No ambiente informacional contemporâneo, o acesso ao debate público é mediado por plataformas que decidem

quais conteúdos circulam, quais são removidos, quais são monetizados, quais são recomendados e quais permanecem invisíveis (SUZOR, 2019; DE GREGORIO, 2022).

A moderação de conteúdo é necessária para enfrentar discursos ilícitos, violência, abuso, exploração sexual, fraude, spam, desinformação e ataques coordenados. Contudo, quando realizada por sistemas automatizados opacos, pode remover conteúdos legítimos, afetar minorias, restringir debate político e comprometer o pluralismo. O desafio é equilibrar proteção contra danos e preservação da liberdade de expressão (GILLESPIE, 2018; KLONICK, 2018).

Algoritmos de recomendação também influenciam a liberdade informacional. Eles não apenas removem ou mantêm conteúdos; eles definem visibilidade. Um conteúdo pode não ser censurado formalmente, mas pode ser reduzido em alcance, despriorizado ou ocultado por critérios algorítmicos. Essa modulação da atenção é uma forma sutil de poder comunicacional (SUNSTEIN, 2017; ZUBOFF, 2019).

O problema democrático é que plataformas privadas exercem funções quase regulatórias sobre a esfera pública, mas não estão submetidas aos mesmos deveres de transparência, motivação e controle que vinculam o Estado. A liberdade de expressão passa a depender de termos de uso, políticas internas, sistemas automatizados e decisões de empresas transnacionais (SUZOR, 2019; DE GREGORIO, 2022).

A IA generativa acrescenta novos riscos. Deepfakes, textos sintéticos, manipulação de voz e produção massiva de conteúdo automatizado

podem afetar reputações, eleições, segurança, confiança pública e integridade informacional. Ao mesmo tempo, ferramentas generativas também podem ampliar criatividade, acessibilidade, educação e produção cultural. A regulação deve evitar tanto permissividade irresponsável quanto censura excessiva (BOMMASANI et al., 2021; BENDER et al., 2021).

A liberdade de expressão deve ser compreendida em conjunto com outros direitos: honra, imagem, privacidade, igualdade, segurança e participação democrática. O constitucionalismo tecnológico não pode tratar a internet como espaço sem lei, mas também não pode permitir controle algorítmico desproporcional da comunicação social (SARLET, 2022; DE GREGORIO, 2022).

A transparência das plataformas é indispensável. Usuários, pesquisadores e autoridades precisam compreender critérios gerais de recomendação, remoção, impulsionamento e moderação. A opacidade impede avaliação de impactos sobre pluralismo e debate público (GILLESPIE, 2018; PASQUALE, 2015).

A regulação democrática da moderação algorítmica deve incluir devido processo procedimental: notificação, fundamentação, possibilidade de recurso, revisão humana e relatórios públicos. Quando plataformas afetam direitos em escala massiva, devem assumir deveres proporcionais ao seu poder comunicacional (KLONICK, 2018; SUZOR, 2019).

9. DEVIDO PROCESSO LEGAL ALGORÍTMICO

O devido processo legal é um dos pilares do Estado Democrático de Direito. Ele exige que decisões que afetem direitos, interesses ou liberdades sejam tomadas com base em procedimento justo,

possibilidade de defesa, conhecimento dos fundamentos, imparcialidade, proporcionalidade e controle. Quando decisões passam a ser automatizadas, surge a necessidade de pensar um devido processo legal algorítmico (CITRON, 2008; HILDEBRANDT, 2015).

A administração pública não pode negar benefício, selecionar cidadão para fiscalização, classificar risco, impor sanção ou restringir direito com base em sistema opaco, sem motivação compreensível e sem possibilidade de contestação. A automação não elimina os deveres constitucionais de motivação, legalidade, impessoalidade, publicidade e eficiência. Ao contrário, exige reforço desses deveres (CITRON, 2008; KROLL et al., 2017).

O devido processo algorítmico possui pelo menos cinco dimensões. A primeira é o direito à informação: o afetado deve saber quando uma decisão relevante envolve sistema automatizado. A segunda é o direito à explicação suficiente: deve haver fundamentos compreensíveis sobre os fatores determinantes da decisão. A terceira é o direito à contestação: o indivíduo deve poder impugnar resultado injusto. A quarta é o direito à revisão humana: decisões sensíveis não devem ser inteiramente blindadas por automação. A quinta é o direito à auditoria: sistemas devem ser verificáveis por autoridades competentes (WACHTER; MITTELSTADT; FLORIDI, 2017; KROLL et al., 2017).

A explicabilidade não precisa significar exposição integral de código-fonte em todos os casos. Pode envolver documentação técnica, descrição dos dados utilizados, critérios gerais, variáveis relevantes, métricas de desempenho, limitações conhecidas, testes de viés e justificativa individual mínima. O grau de explicação deve ser

proporcional ao risco e ao impacto da decisão (RUDIN, 2019; UNIÃO EUROPEIA, 2024).

A revisão humana deve ser efetiva, não meramente formal. Um servidor ou funcionário que apenas confirma automaticamente o resultado do sistema não exerce controle real. A revisão deve permitir análise crítica, acesso a informações relevantes e poder de modificar a decisão quando houver erro, injustiça ou inadequação (CITRON; PASQUALE, 2014; MENDES, 2020).

O devido processo algorítmico também exige registro. Decisões automatizadas precisam deixar trilhas auditáveis: versão do modelo, dados de entrada, regras aplicadas, parâmetros, resultado, intervenção humana e justificativa. Sem logs e documentação, torna-se impossível fiscalizar responsabilidade (KROLL et al., 2017; MITCHELL et al., 2019).

Na esfera privada, o devido processo também tem relevância quando decisões algorítmicas afetam crédito, emprego, seguro, saúde, educação ou acesso a plataformas essenciais. Embora a intensidade dos deveres possa variar, empresas que produzem impactos relevantes sobre direitos não podem operar em total opacidade (PASQUALE, 2015; ALOISI; DE STEFANO, 2022).

Portanto, o devido processo legal algorítmico é uma exigência do constitucionalismo tecnológico. Decisões automatizadas devem ser informadas, justificáveis, contestáveis, revisáveis e auditáveis.

10. TRANSPARÊNCIA, EXPLICABILIDADE E AUDITABILIDADE

A transparência é um dos princípios mais invocados na regulação da inteligência artificial. Contudo, seu significado precisa ser precisado.

Transparência pode envolver informação ao usuário, publicidade de políticas, acesso a documentação, abertura de dados, explicação de decisões, relatórios de impacto, auditorias e fiscalização institucional. Nem toda transparência é igual, e nem toda transparência é suficiente (PASQUALE, 2015; ANANNY; CRAWFORD, 2018).

A explicabilidade refere-se à capacidade de oferecer razões compreensíveis para uma decisão algorítmica. Em sistemas complexos, especialmente modelos de aprendizado profundo, a explicação pode ser difícil. Ainda assim, decisões que afetam direitos não podem ser aceitas apenas porque "o modelo decidiu". A legitimidade jurídica exige compreensão mínima dos fundamentos (WACHTER; MITTELSTADT; FLORIDI, 2017; RUDIN, 2019).

A auditabilidade é mais robusta que a transparência superficial. Um sistema auditável permite verificação independente de dados, desempenho, vieses, segurança, documentação, logs, processos de desenvolvimento e impactos. Auditoria pode ser interna, externa, pública, regulatória ou comunitária, dependendo do risco. Em sistemas de alto impacto, auditoria independente deve ser regra (KROLL et al., 2017; RAGHAVAN et al., 2020).

A documentação é instrumento essencial. Model cards e datasheets for datasets são propostas relevantes para registrar finalidade, dados utilizados, limitações, métricas, riscos e contexto adequado de uso. Essas práticas ajudam a evitar implantação irresponsável e facilitam prestação de contas (MITCHELL et al., 2019; GEBRU et al., 2021).

A transparência deve alcançar todo o ciclo de vida da IA: concepção, coleta de dados, treinamento, validação, implantação, monitoramento e desativação. Um sistema pode ser seguro no

laboratório e injusto na prática. Por isso, governança algorítmica exige monitoramento contínuo, especialmente quando há mudança de contexto ou degradação do modelo (RUDIN, 2019; CRAWFORD, 2021).

Há limites legítimos à transparência. Segredos industriais, segurança cibernética e proteção contra manipulação podem justificar restrições. Contudo, esses limites não podem servir como escudo absoluto contra fiscalização. O desafio é equilibrar proteção empresarial e direito público à accountability, especialmente em sistemas que afetam direitos fundamentais (PASQUALE, 2015; UNIÃO EUROPEIA, 2024).

A transparência também precisa ser compreensível. Informações técnicas excessivamente complexas podem ser inúteis para cidadãos. Por isso, devem existir diferentes camadas de explicação: linguagem simples para afetados, documentação técnica para auditores, relatórios regulatórios para autoridades e dados agregados para controle social (ANANNY; CRAWFORD, 2018; MENDES, 2020).

Sem transparência, explicabilidade e auditabilidade, a IA pode criar uma nova forma de poder invisível. O constitucionalismo tecnológico exige que sistemas decisórios sejam tecnicamente controláveis e juridicamente justificáveis.

11. RESPONSABILIZAÇÃO ALGORÍTMICA E DEVER DE PRESTAÇÃO DE CONTAS

A responsabilização é elemento indispensável da governança algorítmica. Sistemas de IA podem produzir danos, discriminações, exclusões, erros e violações de direitos. Quando isso ocorre, é

necessário identificar quem responde: desenvolvedor, fornecedor, operador, controlador de dados, órgão público, empresa contratante, gestor ou todos em diferentes graus (CITRON; PASQUALE, 2014; KROLL et al., 2017).

A complexidade técnica não pode gerar irresponsabilidade. O argumento de que o modelo é autônomo, complexo ou imprevisível não deve afastar o dever de cuidado. Quem desenvolve, adquire ou utiliza sistema algorítmico deve avaliar riscos, documentar decisões, monitorar resultados e reparar danos quando houver falha (UNIÃO EUROPEIA, 2024; FLORIDI; COWLS, 2019).

A responsabilização algorítmica exige governança ex ante e ex post. Ex ante, devem existir avaliação de impacto, análise de riscos, testes, validação, revisão jurídica, proteção de dados, segurança e documentação antes da implantação. Ex post, devem existir monitoramento, canais de reclamação, auditoria, correção, sanção e reparação (MENDES, 2020; BIONI, 2021).

A LGPD já incorpora lógica de accountability ao exigir responsabilização e prestação de contas. Esse princípio pode ser expandido para a IA: não basta cumprir regras formalmente; é necessário demonstrar conformidade, prevenir riscos e comprovar medidas de governança. O ônus de demonstrar segurança e legitimidade deve recair sobre quem controla o sistema, não sobre o cidadão afetado (DONEDA, 2021; BIONI, 2021).

Em sistemas públicos, a responsabilização deve ser ainda mais rigorosa. O Estado não pode terceirizar decisões algorítmicas sem manter controle sobre legalidade, finalidade, proporcionalidade e impactos. Contratar tecnologia privada não elimina

responsabilidade pública. A administração deve compreender o sistema que utiliza e responder por suas consequências (CITRON, 2008; HILDEBRANDT, 2015).

A cadeia de responsabilidade em IA pode ser complexa porque diferentes agentes participam do ciclo de vida do sistema. Um fornecedor desenvolve o modelo; outro fornece dados; uma empresa integra; um órgão público utiliza; um operador interpreta resultados. Por isso, contratos, documentação e normas devem delimitar deveres de cada agente (KROLL et al., 2017; UNIÃO EUROPEIA, 2024).

A responsabilização também deve incluir dever de reparação coletiva. Danos algorítmicos podem ser massivos e atingir grupos inteiros. Uma ferramenta discriminatória de crédito, seleção ou policiamento pode afetar milhares de pessoas. Nesses casos, mecanismos individuais de reparação são insuficientes; é necessário controle coletivo, atuação de órgãos reguladores, Ministério Público, defensorias, associações e ações coletivas (EUBANKS, 2018; BENJAMIN, 2019).

Portanto, a governança algorítmica responsável exige que todo sistema de IA tenha responsáveis identificáveis, deveres documentados, mecanismos de prevenção e canais efetivos de reparação.

12. REGULAÇÃO COMPARADA DA INTELIGÊNCIA ARTIFICIAL

A regulação internacional da inteligência artificial caminha para modelos baseados em risco, direitos humanos, segurança, transparência e responsabilização. A União Europeia tornou-se referência com o AI Act, que classifica sistemas de IA conforme

níveis de risco, proíbe determinadas práticas, regula sistemas de alto risco, estabelece deveres de transparência e impõe regras para modelos de propósito geral (UNIÃO EUROPEIA, 2024).

A abordagem europeia é relevante porque vincula inovação tecnológica à proteção de direitos fundamentais. Sistemas de alto risco, como aqueles utilizados em emprego, educação, crédito, migração, justiça, segurança e serviços essenciais, passam a exigir gestão de riscos, governança de dados, documentação técnica, transparência, supervisão humana, robustez e segurança. Essa lógica reconhece que nem toda IA possui o mesmo impacto jurídico (UNIÃO EUROPEIA, 2024; DE GREGORIO, 2022).

A OCDE formulou princípios para IA confiável, centrada no ser humano, respeitosa dos direitos humanos, democrática, transparente, robusta, segura e responsável. Esses princípios influenciaram políticas públicas em diversos países e funcionam como referência internacional para governança ética e regulatória (OCDE, 2024).

A UNESCO, por sua vez, aprovou recomendação global sobre ética da inteligência artificial, enfatizando direitos humanos, dignidade, diversidade, inclusão, sustentabilidade, transparência, responsabilidade e governança. A recomendação é importante porque desloca o debate para uma perspectiva global, considerando impactos sociais, culturais e ambientais da IA (UNESCO, 2021).

O Brasil discute seu marco legal por meio do PL nº 2.338/2023, que propõe normas gerais para desenvolvimento, fomento e uso ético e responsável da inteligência artificial com centralidade da pessoa humana. O projeto dialoga com abordagem baseada em risco,

direitos dos afetados, governança responsável e proteção de direitos fundamentais. Sua tramitação demonstra que o país busca construir regulação própria, em diálogo com experiências internacionais, mas adaptada à realidade constitucional brasileira.

A regulação comparada revela dilemas comuns. O primeiro é equilibrar inovação e proteção. Regulação excessivamente rígida pode dificultar desenvolvimento tecnológico; regulação fraca pode permitir danos massivos. O segundo é definir responsabilidades em cadeias complexas. O terceiro é criar órgãos fiscalizadores capazes de compreender tecnologia. O quarto é proteger direitos sem inviabilizar pesquisa e uso legítimo (FLORIDI; COWLS, 2019; CRAWFORD, 2021).

Outro desafio é a assimetria global. Países com maior capacidade tecnológica influenciam padrões, infraestrutura e mercado. Países em desenvolvimento podem tornar-se importadores de sistemas de IA sem capacidade plena de auditoria. Por isso, a soberania digital e a capacidade regulatória nacional são componentes importantes do constitucionalismo tecnológico (COHEN, 2019; CRAWFORD, 2021).

A regulação comparada indica que a IA exige instrumentos combinados: leis gerais, normas setoriais, padrões técnicos, certificações, avaliações de impacto, autoridades reguladoras, auditorias, códigos de conduta e controle judicial. Nenhum instrumento isolado é suficiente.

13. INTELIGÊNCIA ARTIFICIAL NA ADMINISTRAÇÃO PÚBLICA

O uso de inteligência artificial na administração pública pode melhorar eficiência, reduzir filas, detectar fraudes, aprimorar planejamento, organizar documentos, automatizar tarefas

repetitivas e apoiar políticas públicas. No entanto, quando o Estado utiliza IA, os riscos são constitucionalmente mais sensíveis porque decisões públicas possuem autoridade, coercibilidade e impacto direto sobre direitos (CITRON, 2008; KITCHIN, 2014).

A administração pública está vinculada aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência. A IA pode contribuir para eficiência, mas não pode sacrificar legalidade, publicidade e controle. Um sistema automatizado que decide sem base legal, sem transparência ou sem possibilidade de revisão viola o núcleo do regime jurídico-administrativo (DI PIETRO, 2023; CITRON, 2008).

A decisão administrativa automatizada exige motivação. O cidadão deve compreender por que recebeu ou perdeu benefício, por que foi classificado como risco, por que foi selecionado para fiscalização ou por que teve requerimento negado. A motivação não pode ser substituída por referência genérica ao sistema (HILDEBRANDT, 2015; WACHTER; MITTELSTADT; FLORIDI, 2017).

A impessoalidade administrativa não significa automatização cega. Um algoritmo pode parecer impessoal, mas reproduzir vieses dos dados. A impessoalidade exige tratamento igualitário e juridicamente justificado, não apenas ausência de decisão humana direta (BAROCAS; SELBST, 2016; EUBANKS, 2018).

A publicidade deve ser reinterpretada. Não basta publicar o resultado de uma política; é necessário informar o uso de IA, a finalidade, os critérios gerais, os dados utilizados, os riscos, os mecanismos de revisão e os responsáveis. A opacidade tecnológica é

incompatível com administração democrática (KROLL et al., 2017; MENDES, 2020).

Em políticas sociais, o cuidado deve ser redobrado. Sistemas automatizados podem excluir pessoas vulneráveis por inconsistências cadastrais, dados desatualizados ou critérios inadequados. O Estado não pode transformar eficiência administrativa em barreira de acesso a direitos sociais. A tecnologia deve facilitar inclusão, e não automatizar indeferimentos (EUBANKS, 2018; SEN, 2000).

Em segurança pública, sistemas preditivos, reconhecimento facial e análise de risco podem intensificar seletividade penal. A adoção dessas tecnologias deve ser excepcional, proporcional, legalmente autorizada, auditável e submetida a controle externo. A promessa de segurança não pode justificar vigilância generalizada ou discriminação automatizada (BENJAMIN, 2019; LYON, 2018).

A administração pública algorítmica também exige capacitação institucional. Órgãos públicos não podem adquirir sistemas de IA sem equipe capaz de avaliar riscos, contratos, dados, segurança, vieses, documentação e impactos. A dependência acrítica de fornecedores privados pode fragilizar soberania administrativa e controle público (COHEN, 2019; CRAWFORD, 2021).

Portanto, a IA no setor público deve ser orientada por governança reforçada: legalidade, avaliação de impacto, transparência, revisão humana, auditoria, controle social e responsabilização.

14. RESULTADOS DA ANÁLISE

A análise desenvolvida permite identificar dez resultados principais.

O primeiro resultado é que a inteligência artificial desloca parte do poder decisório para sistemas técnicos capazes de classificar, prever, recomendar e automatizar decisões em escala, afetando diretamente direitos fundamentais.

O segundo resultado é que a governança algorítmica não é neutra. Ela incorpora escolhas sobre dados, objetivos, métricas, categorias, riscos e valores, razão pela qual deve ser submetida a controle jurídico e democrático.

O terceiro resultado é que o constitucionalismo tecnológico emerge como resposta à expansão do poder digital, buscando aplicar princípios constitucionais à regulação de plataformas, algoritmos, dados e sistemas de IA.

O quarto resultado é que privacidade e proteção de dados são fundamentos centrais da regulação da IA, pois sistemas algorítmicos dependem de coleta, cruzamento e inferência massiva de informações pessoais.

O quinto resultado é que a igualdade é ameaçada por vieses algorítmicos capazes de reproduzir discriminações históricas sob aparência de neutralidade estatística.

O sexto resultado é que a liberdade de expressão é afetada por algoritmos de recomendação e moderação, que influenciam visibilidade, circulação e remoção de conteúdos na esfera pública digital.

O sétimo resultado é que o devido processo legal precisa ser reinterpretado para ambientes automatizados, exigindo informação, explicação, contestação, revisão humana e auditoria.

O oitavo resultado é que transparência, explicabilidade e auditabilidade são condições mínimas para legitimidade jurídica de sistemas algorítmicos de alto impacto.

O nono resultado é que a responsabilização algorítmica deve alcançar todo o ciclo de vida da IA, desde desenvolvimento e treinamento até implantação, monitoramento e reparação de danos.

O décimo resultado é que a regulação da IA deve equilibrar inovação, segurança jurídica e proteção de direitos fundamentais, evitando tanto o tecnossolucionismo desregulado quanto bloqueios normativos incompatíveis com desenvolvimento científico e econômico responsável.

15. DISCUSSÃO

A discussão central deste artigo é que a inteligência artificial desafia a arquitetura clássica do constitucionalismo porque cria formas de poder que não se encaixam integralmente nos modelos tradicionais de controle estatal. O poder algorítmico é distribuído, técnico, opaco, público-privado e frequentemente transnacional. Ele pode afetar direitos sem se apresentar como decisão política explícita (PASQUALE, 2015; DE GREGORIO, 2022).

O primeiro ponto crítico é a insuficiência da neutralidade técnica. Sistemas de IA são frequentemente apresentados como objetivos, racionais e superiores ao julgamento humano. No entanto, algoritmos operam com dados, categorias e funções de otimização definidas por pessoas e instituições. A técnica pode reduzir algumas arbitrariedades humanas, mas também pode automatizar preconceitos e ocultar decisões políticas (BAROCAS; SELBST, 2016; CRAWFORD, 2021).

O segundo ponto é a assimetria informacional. Cidadãos e consumidores frequentemente não sabem quando estão sendo avaliados por algoritmos, quais dados foram utilizados, quais critérios foram aplicados e como contestar o resultado. Essa assimetria compromete autonomia, devido processo e igualdade de armas (PASQUALE, 2015; WACHTER; MITTELSTADT; FLORIDI, 2017).

O terceiro ponto refere-se à escala. Sistemas algorítmicos podem produzir erros massivos. Uma política pública automatizada pode negar benefícios a milhares de pessoas; uma ferramenta de crédito pode excluir grupos inteiros; um sistema de moderação pode silenciar discursos legítimos; um sistema biométrico pode produzir identificações falsas. O risco constitucional é ampliado pela velocidade e pela reprodução automatizada (O'NEIL, 2016; EUBANKS, 2018).

O quarto ponto é a necessidade de regulação baseada em risco. Nem todo sistema de IA exige o mesmo grau de controle. Um filtro de spam não possui o mesmo impacto que um sistema usado em justiça criminal, saúde, crédito, emprego ou segurança pública. A proporcionalidade regulatória exige calibrar obrigações conforme risco e impacto sobre direitos (UNIÃO EUROPEIA, 2024; OCDE, 2024).

O quinto ponto é a relevância da avaliação de impacto algorítmico. Antes de implantar sistemas de alto risco, deve-se avaliar finalidade, necessidade, dados, vieses, segurança, explicabilidade, impacto sobre grupos vulneráveis e alternativas menos lesivas. Essa avaliação deve ser documentada e passível de fiscalização (MENDES, 2020; KROLL et al., 2017).

O sexto ponto é o papel da supervisão humana. A IA deve apoiar decisões, não substituir integralmente responsabilidade humana em contextos sensíveis. Contudo, a supervisão humana precisa ser real. Um humano que apenas confirma automaticamente o sistema não exerce controle democrático. É necessário poder efetivo de revisão, correção e responsabilização (CITRON; PASQUALE, 2014; RUDIN, 2019).

O sétimo ponto é a proteção de grupos vulneráveis. A IA pode aprofundar desigualdades quando aplicada sem sensibilidade social. Sistemas treinados com dados históricos podem penalizar justamente aqueles que já sofreram discriminação. O constitucionalismo tecnológico deve incorporar justiça social, e não apenas eficiência técnica (BENJAMIN, 2019; EUBANKS, 2018).

O oitavo ponto envolve a soberania regulatória. Países que importam tecnologias sem capacidade de auditoria tornam-se dependentes de modelos desenvolvidos segundo realidades sociais, jurídicas e culturais distintas. O Brasil precisa desenvolver capacidade institucional para avaliar, regular e auditar sistemas de IA conforme sua Constituição e suas desigualdades específicas (DONEDA, 2021; COHEN, 2019).

O nono ponto é que a autorregulação é insuficiente. Códigos éticos empresariais são úteis, mas não substituem direitos, deveres, fiscalização e sanções. A experiência internacional demonstra que princípios voluntários precisam ser convertidos em mecanismos jurídicos concretos quando há risco relevante a direitos fundamentais (UNESCO, 2021; UNIÃO EUROPEIA, 2024).

O décimo ponto é que inovação e direitos fundamentais não são inimigos. A ausência de regulação pode gerar insegurança jurídica, desconfiança social e danos. Uma regulação bem desenhada pode estimular inovação responsável, criar padrões de confiança e proteger cidadãos. O desafio é construir ambiente normativo capaz de promover tecnologia sem abdicar da Constituição (FLORIDI; COWLS, 2019; OCDE, 2024).

Assim, a governança algorítmica exige novo pacto constitucional com a tecnologia. A IA deve ser integrada ao Estado Democrático de Direito como instrumento submetido à dignidade humana, e não como instância autônoma de decisão.

16. DIRETRIZES PARA UMA GOVERNANÇA ALGORÍTMICA CONSTITUCIONAL

A partir da análise realizada, propõem-se diretrizes para uma governança algorítmica compatível com o Estado Democrático de Direito.

Primeiro, reconhecer que sistemas de IA de alto impacto devem ser submetidos a controle jurídico reforçado, especialmente quando afetarem direitos fundamentais, acesso a serviços essenciais, liberdade, igualdade, saúde, trabalho, crédito, educação, segurança ou justiça.

Segundo, adotar avaliação de impacto algorítmico antes da implantação de sistemas sensíveis, contemplando finalidade, necessidade, proporcionalidade, dados utilizados, riscos discriminatórios, segurança, explicabilidade e alternativas menos lesivas.

Terceiro, garantir transparência em camadas: informações simples para cidadãos, documentação técnica para auditores, relatórios regulatórios para autoridades e dados agregados para controle social.

Quarto, assegurar explicabilidade suficiente das decisões automatizadas, especialmente quando produzirem efeitos jurídicos, econômicos ou sociais relevantes sobre indivíduos ou grupos.

Quinto, estabelecer direito à contestação e à revisão humana efetiva, impedindo que decisões automatizadas de alto impacto sejam imunes a controle.

Sexto, implementar auditorias independentes em sistemas de alto risco, com verificação de vieses, segurança, robustez, qualidade dos dados, desempenho por grupos e conformidade jurídica.

Sétimo, proteger dados pessoais segundo princípios de finalidade, necessidade, adequação, transparência, segurança, prevenção e responsabilização.

Oitavo, vedar ou restringir usos incompatíveis com direitos fundamentais, como vigilância biométrica massiva sem base legal estrita, manipulação comportamental abusiva, social scoring discriminatório e sistemas que explorem vulnerabilidades.

Nono, exigir supervisão humana qualificada, com poder real de modificar decisões, suspender sistemas e corrigir danos.

Décimo, responsabilizar agentes em toda a cadeia de IA: desenvolvedores, fornecedores, operadores, controladores de dados, gestores públicos e empresas usuárias.

Décimo primeiro, assegurar participação social na governança de tecnologias públicas de alto impacto, especialmente quando afetarem grupos vulneráveis.

Décimo segundo, garantir controle judicial efetivo sobre decisões automatizadas, com acesso à prova técnica, documentação, logs, critérios e informações necessárias à defesa de direitos.

Décimo terceiro, promover capacitação técnica de órgãos públicos, tribunais, agências reguladoras, Ministério Público, defensorias e autoridades de proteção de dados.

Décimo quarto, estimular inovação responsável, com ambientes regulatórios seguros, pesquisa pública, transparência, proteção de direitos e desenvolvimento tecnológico soberano.

Décimo quinto, consolidar o constitucionalismo tecnológico como paradigma de interpretação jurídica, afirmando que nenhuma inovação pode se sobrepor à dignidade humana e aos direitos fundamentais.

17. CONSIDERAÇÕES FINAIS

A inteligência artificial tornou-se infraestrutura decisória da sociedade contemporânea. Sua expansão modifica a forma como decisões públicas e privadas são tomadas, ampliando eficiência e capacidade analítica, mas também criando riscos à privacidade, igualdade, liberdade, devido processo, proteção de dados e controle democrático.

O artigo demonstrou que a governança algorítmica não é mero fenômeno técnico. Ela representa nova forma de exercício de poder,

capaz de classificar pessoas, prever comportamentos, distribuir oportunidades, restringir direitos e influenciar escolhas. Por isso, deve ser submetida aos princípios do Estado Democrático de Direito.

O constitucionalismo tecnológico surge como resposta jurídica à expansão do poder digital. Seu objetivo é aplicar a força normativa da Constituição aos sistemas tecnológicos que organizam a vida social. Isso significa reconhecer que algoritmos, plataformas, bancos de dados e modelos de IA precisam respeitar dignidade humana, igualdade, liberdade, privacidade, devido processo e responsabilização.

A análise evidenciou que a proteção de dados pessoais é elemento central desse novo paradigma. Sem controle sobre dados e inferências, indivíduos tornam-se vulneráveis à vigilância, manipulação e discriminação. A LGPD, o Marco Civil da Internet e a Constituição Federal fornecem bases importantes, mas a inteligência artificial exige mecanismos adicionais de transparência, auditoria e avaliação de impacto.

A igualdade também se revelou eixo fundamental. Sistemas de IA podem reproduzir vieses históricos e automatizar discriminações sob aparência de neutralidade. A não discriminação algorítmica exige testes, auditorias, diversidade de dados, participação social e monitoramento contínuo.

O devido processo legal precisa ser reinterpretado para decisões automatizadas. A pessoa afetada deve ter direito à informação, explicação, contestação, revisão humana e acesso a mecanismos de reparação. A decisão algorítmica não pode tornar-se uma caixa-preta incontestável.

As experiências internacionais, especialmente o AI Act europeu, os princípios da OCDE e a Recomendação da UNESCO, indicam tendência de regulação baseada em risco, centralidade humana, transparência e responsabilização. O Brasil, ao discutir seu marco legal de IA, tem oportunidade de construir modelo regulatório alinhado à Constituição de 1988 e às particularidades sociais do país.

Conclui-se que a efetividade dos direitos fundamentais na era da inteligência artificial depende da consolidação de uma governança algorítmica constitucional. A inovação deve ser incentivada, mas não pode operar fora do controle democrático. A tecnologia deve servir à pessoa humana, à justiça social e à democracia. O desafio jurídico do século XXI é assegurar que o poder computacional permaneça subordinado à Constituição.

REFERÊNCIAS BIBLIOGRÁFICAS

AJUNWA, Ifeoma. **The quantified worker: law and technology in the modern workplace.** Cambridge: Cambridge University Press, 2023.

ALEXY, Robert. **Teoria dos direitos fundamentais.** São Paulo: Malheiros, 2008.

ANANNY, Mike; CRAWFORD, Kate. Seeing without knowing: limitations of the transparency ideal and its application to algorithmic accountability. **New Media & Society,** v. 20, n. 3, p. 973-989, 2018.

BAROCAS, Solon; SELBST, Andrew D. Big data's disparate impact. **California Law Review,** v. 104, n. 3, p. 671-732, 2016.

BENDER, Emily M.; GEBRU, Timnit; MCMILLAN-MAJOR, Angelina; SHMITCHELL, Shmargaret. On the dangers of stochastic parrots: can language models be too big? In: **Proceedings of the ACM Conference on Fairness, Accountability, and Transparency.** New York: ACM, 2021. p. 610-623.

BENJAMIN, Ruha. **Race after technology: abolitionist tools for the new Jim Code.** Cambridge: Polity Press, 2019.

BENKLER, Yochai; FARIS, Robert; ROBERTS, Hal. **Network propaganda: manipulation, disinformation, and radicalization in American politics.** Oxford: Oxford University Press, 2018.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.** 3. ed. Rio de Janeiro: Forense, 2021.

BOBBIO, Norberto. **A era dos direitos.** Rio de Janeiro: Campus, 1992.

BOMMASANI, Rishi et al. On the opportunities and risks of foundation models. **arXiv preprint arXiv:2108.07258,** 2021.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília: Senado Federal, 1988.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília: Presidência da República, 2014.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais. Brasília: Presidência da República, 2018.

BRASIL. **Projeto de Lei nº 2.338, de 2023.** Dispõe sobre o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana. Brasília: Congresso Nacional, 2023.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender shades: intersectional accuracy disparities in commercial gender classification. In: **Proceedings of Machine Learning Research,** v. 81, p. 1-15, 2018.

CANOTILHO, José Joaquim Gomes. **Direito constitucional e teoria da Constituição.** 7. ed. Coimbra: Almedina, 2003.

CAVOUKIAN, Ann. **Privacy by design: the 7 foundational principles.** Toronto: Information and Privacy Commissioner of Ontario, 2011.

CELESTE, Edoardo. Digital constitutionalism: a new systematic theorisation. **International Review of Law, Computers & Technology,** v. 33, n. 1, p. 76-99, 2019.

CITRON, Danielle Keats; PASQUALE, Frank. The scored society: due process for automated predictions. **Washington Law Review,** v. 89, n. 1, p. 1-33, 2014.

CITRON, Danielle Keats. Technological due process. **Washington University Law Review,** v. 85, n. 6, p. 1249-1313, 2008.

COHEN, Julie E. **Between truth and power: the legal constructions of informational capitalism.** Oxford: Oxford University Press, 2019.

COHEN, Julie E. **Configuring the networked self: law, code, and the play of everyday practice.** New Haven: Yale University Press, 2012.

CRAWFORD, Kate. **Atlas of AI: power, politics, and the planetary costs of artificial intelligence.** New Haven: Yale University Press, 2021.

DE GREGORIO, Giovanni. **Digital constitutionalism in Europe: reframing rights and powers in the algorithmic society.** Cambridge: Cambridge University Press, 2022.

DENARDIS, Laura. **The internet in everything: freedom and security in a world with no off switch.** New Haven: Yale University Press, 2020.

DI PIETRO, Maria Sylvia Zanella. **Direito administrativo.** 36. ed. Rio de Janeiro: Forense, 2023.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

DWORKIN, Ronald. **Levando os direitos a sério.** São Paulo: Martins Fontes, 2002.

EUBANKS, Virginia. **Automating inequality: how high-tech tools profile, police, and punish the poor.** New York: St. Martin's Press, 2018.

FLORIDI, Luciano; COWLS, Josh. A unified framework of five principles for AI in society. **Harvard Data Science Review,** v. 1, n. 1, 2019.

GEBRU, Timnit et al. Datasheets for datasets. **Communications of the ACM,** v. 64, n. 12, p. 86-92, 2021.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social.** 7. ed. São Paulo: Atlas, 2019.

GILLESPIE, Tarleton. **Custodians of the internet: platforms, content moderation, and the hidden decisions that shape social media.** New Haven: Yale University Press, 2018.

HABERMAS, Jürgen. **Direito e democracia: entre facticidade e validade.** Rio de Janeiro: Tempo Brasileiro, 1997.

HILDEBRANDT, Mireille. **Smart technologies and the end(s) of law: novel entanglements of law and technology.** Cheltenham: Edward Elgar, 2015.

KITCHIN, Rob. Thinking critically about and researching algorithms. **Information, Communication & Society,** v. 20, n. 1, p. 14-29, 2017.

KLONICK, Kate. The new governors: the people, rules, and processes governing online speech. **Harvard Law Review,** v. 131, n. 6, p. 1598-1670, 2018.

KROLL, Joshua A.; HUEY, Joanna; BAROCAS, Solon; FELTEN, Edward W.; REIDENBERG, Joel R.; ROBINSON, David G.; YU, Harlan. Accountable algorithms. **University of Pennsylvania Law Review,** v. 165, n. 3, p. 633-705, 2017.

LESSIG, Lawrence. **Code and other laws of cyberspace.** New York: Basic Books, 1999.

LESSIG, Lawrence. **Code: version 2.0.** New York: Basic Books, 2006.

LYON, David. **The culture of surveillance: watching as a way of life.** Cambridge: Polity Press, 2018.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor.** São Paulo: Saraiva, 2020.

MINAYO, Maria Cecília de Souza. **O desafio do conhecimento: pesquisa qualitativa em saúde.** 14. ed. São Paulo: Hucitec, 2014.

MITCHELL, Margaret et al. Model cards for model reporting. In: **Proceedings of the Conference on Fairness, Accountability, and Transparency.** New York: ACM, 2019. p. 220-229.

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

OCDE. **Recommendation of the Council on Artificial Intelligence.** Paris: OECD, 2024.

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

RAGHAVAN, Manish; BAROCAS, Solon; KLEINBERG, Jon; LEVY, Karen. Mitigating bias in algorithmic hiring: evaluating claims and practices. In: **Proceedings of the Conference on Fairness, Accountability, and Transparency.** New York: ACM, 2020. p. 469-481.

RUDIN, Cynthia. Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. **Nature Machine Intelligence,** v. 1, p. 206-215, 2019.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais.** 13. ed. Porto Alegre: Livraria do Advogado, 2022.

SEN, Amartya. **Desenvolvimento como liberdade.** São Paulo: Companhia das Letras, 2000.

SUNSTEIN, Cass R. **#Republic: divided democracy in the age of social media.** Princeton: Princeton University Press, 2017.

SUZOR, Nicolas. **Lawless: the secret rules that govern our digital lives.** Cambridge: Cambridge University Press, 2019.

UNESCO. **Recommendation on the Ethics of Artificial Intelligence.** Paris: United Nations Educational, Scientific and Cultural Organization, 2021.

UNIÃO EUROPEIA. **Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence.** Official Journal of the European Union, 2024.

WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. **International Data Privacy Law,** v. 7, n. 2, p. 76-99, 2017.

YEUNG, Karen. Algorithmic regulation: a critical interrogation. **Regulation & Governance,** v. 12, n. 4, p. 505-523, 2018.

ZUBOFF, Shoshana. **The age of surveillance capitalism: the fight for a human future at the new frontier of power.** New York: PublicAffairs, 2019.

[1] Especialista em Inteligência Artificial e Computacional pela Universidade Federal de Viçosa, vinculado à Universidade Federal do Ceará (UFC). E-mail: acesse o artigo original para visualizar o e-mail

[2] Graduanda em Direito pelo Centro Universitário do Norte (UNINORTE). E-mail: acesse o artigo original para visualizar o e-mail

[3] Bacharela em Direito pela Universidade de Uberaba (UNIUBE). E-mail: acesse o artigo original para visualizar o e-mail

[4] Mestra em Direito pela Universidade de Marília (UNIMAR) e Professora Assistente da Universidade Estadual Vale do Acaraú (UVA). E-mail: acesse o artigo original para visualizar o e-mail

[5] Mestrando em Direito e Desenvolvimento no Semiárido pelo Centro Universitário INTA (UNINTA) e Bacharel em Direito pela Universidade Federal de Goiás (UFG). E-mail: acesse o artigo original para visualizar o e-mail

[6] Especialista (MBA) em Planejamento Tributário pela Faculdade Luciano Feijão (FLF). E-mail: acesse o artigo original para visualizar o e-mail

[7] Mestre em Direito pela Universidade Christus (Unichristus). E-mail: acesse o artigo original para visualizar o e-mail

[8] Especialista em Direito Processual Civil pela Universidade Estadual Vale do Acaraú (UEVA). E-mail: acesse o artigo original para visualizar o e-mail

[9] Mestre em Economia pela Universidade Federal do Ceará (UFC) e Especialista em Direito Tributário pela Pontifícia Universidade Católica de Minas Gerais (PUC Minas). E-mail: acesse o artigo original para visualizar o e-mail

[10] Mestra em Ciências e Meio Ambiente pela Universidade Federal do Pará (UFPA), Advogada e Professora. E-mail: acesse o artigo original para visualizar o e-mail