

v.2, n.5, 2025 - Maio

# REVISTA O UNIVERSO OBSERVÁVEL

## VIGILÂNCIA ALGORÍTMICA E DIREITOS FUNDAMENTAIS: DESAFIOS JURÍDICOS NA ERA DA INTELIGÊNCIA ARTIFICIAL

Moisés de Moura Andrade<sup>1</sup>  
Thamires Silva Martins<sup>2</sup>  
Wallace Silva Bismark<sup>3</sup>  
Juliana Machado Romanoski<sup>4</sup>

Revista O Universo Observável  
DOI: 10.5281/zenodo.15477790  
[ISSN: 2966-0599](https://doi.org/10.5281/zenodo.15477790)

<sup>1</sup>Faculdades Londrina

E-mail: [assess.juridica.imobiliaria@gmail.com](mailto:assess.juridica.imobiliaria@gmail.com)

Lattes: <https://lattes.cnpq.br/6188681545521763>

<sup>2</sup>Universidade de São Paulo - USP

Lattes: <http://lattes.cnpq.br/7422474565097183>

<sup>3</sup>Instituto Federal de Mato Grosso - IFMT

E-mail: [wallacebismark@gmail.com](mailto:wallacebismark@gmail.com)

Lattes: <http://lattes.cnpq.br/4119834777860360>

<sup>4</sup> Universidade de Várzea Grande / MT (UNIVAG)

E-mail: [julianaharveyromanoski@hotmail.com](mailto:julianaharveyromanoski@hotmail.com)

Lattes: <https://lattes.cnpq.br/5813072057827405>



## VIGILÂNCIA ALGORÍTMICA E DIREITOS FUNDAMENTAIS: DESAFIOS JURÍDICOS NA ERA DA INTELIGÊNCIA ARTIFICIAL

Moisés de Moura Andrade, Thamires Silva Martins, Wallace Silva Bismark e  
Juliana Machado Romanoski



Fonte: <https://www.enriquedans.com/2017/10/cuando-la-vigilancia-se-vuelve-algoritmica.html>

**PERIÓDICO CIENTÍFICO INDEXADO INTERNACIONALMENTE**

ISSN  
International Standard Serial Number  
2966-0599

[www.ouniversoobservavel.com.br](http://www.ouniversoobservavel.com.br)

Editora e Revista  
O Universo Observável  
CNPJ: 57.199.688/0001-06  
Naviraí – Mato Grosso do Sul  
Rua: Botocudos, 365 – Centro  
CEP: 79950-000

## RESUMO

A incorporação de sistemas de vigilância algorítmica tem ampliado a capacidade de monitoramento estatal e privado, promovendo avanços significativos em segurança e eficiência administrativa. Contudo, essa mesma tecnologia impõe desafios complexos à proteção dos direitos fundamentais, especialmente no que se refere à privacidade e à igualdade dos cidadãos. Este artigo analisa, por meio de revisão bibliográfica, os impactos da utilização de inteligência artificial para vigilância, evidenciando as lacunas normativas existentes e a necessidade de uma regulação específica que harmonize a inovação tecnológica com a garantia dos direitos individuais.

**Palavras-chave:** Vigilância Algorítmica. Direitos Fundamentais. Inteligência Artificial.

## ABSTRACT

*The integration of algorithmic surveillance systems has significantly enhanced the monitoring capabilities of both state and private entities, contributing to improved security and administrative efficiency. However, this technology also presents complex challenges to the protection of fundamental rights, particularly regarding privacy and equality. This article analyzes, through a bibliographic review, the impacts of using artificial intelligence for surveillance, highlighting the regulatory gaps and the need for specific legislation that balances technological innovation with the protection of individual rights.*

**Keywords:** Algorithmic Surveillance. Fundamental Rights. Artificial Intelligence.

## 1 INTRODUÇÃO

A crescente incorporação de tecnologias baseadas em inteligência artificial (IA) nos sistemas de vigilância, tanto por instituições públicas quanto privadas, tem remodelado significativamente os mecanismos de controle social na sociedade contemporânea. Entre essas tecnologias, destacam-se os sistemas algorítmicos que operam por meio de análises preditivas, reconhecimento facial e monitoramento automatizado de dados em larga escala, o que tem sido amplamente denominado como vigilância algorítmica. Embora essas ferramentas sejam frequentemente justificadas com base em objetivos legítimos, como segurança pública, prevenção de crimes e eficiência administrativa, seus impactos sobre os direitos fundamentais dos indivíduos ainda são motivo de intensa preocupação e debate no meio jurídico.

A vigilância automatizada amplia o poder de observação do Estado e das corporações sobre os cidadãos, muitas vezes sem o devido controle, transparência ou possibilidade de contestação por parte dos afetados. Tal cenário levanta questões centrais relacionadas à privacidade, proteção de dados pessoais, liberdade de expressão, presunção de inocência e não discriminação. O uso indiscriminado e opaco de algoritmos de decisão pode resultar em perfis injustos, discriminações algorítmicas e violações à dignidade humana, especialmente quando essas ferramentas operam sem auditoria, supervisão jurídica adequada ou parâmetros éticos estabelecidos.

No Brasil, embora a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) represente um avanço normativo importante na tutela da privacidade e do tratamento de dados, ela ainda não contempla de forma específica os desafios trazidos pela inteligência artificial em sua dimensão preditiva e autônoma. Além disso, a ausência de uma legislação robusta e atualizada

que regulamente diretamente o uso de algoritmos de vigilância agrava os riscos de arbitrariedade, reforçando a necessidade de discussões jurídicas aprofundadas sobre os limites normativos, as garantias fundamentais e os mecanismos de responsabilização.

Diante disso, este artigo tem como propósito analisar criticamente os desafios jurídicos impostos pela vigilância algorítmica à luz dos direitos fundamentais, problematizando a atuação estatal e privada em contextos de monitoramento digital e indicando possíveis caminhos normativos para a construção de uma regulação equilibrada, que promova a inovação tecnológica sem comprometer as garantias constitucionais. A pesquisa se desenvolve por meio de uma revisão bibliográfica, a partir de estudos doutrinários, legislações correlatas e documentos jurídicos recentes, com enfoque qualitativo e abordagem dedutiva.

## 2 REVISÃO DE LITERATURA

### 2.1 A INTELIGÊNCIA ARTIFICIAL NO CONTEXTO DA SOCIEDADE DA INFORMAÇÃO

A inteligência artificial (IA) tem se consolidado como um dos pilares da chamada quarta revolução industrial, promovendo transformações profundas nas dinâmicas sociais, econômicas e institucionais. Seu desenvolvimento ocorre em um cenário marcado pela aceleração digital, alta conectividade e massiva coleta de dados (POLIDO, 2024).

No contexto da sociedade da informação, a IA opera como instrumento estratégico de poder, com impacto direto sobre decisões governamentais, estratégias de mercado e rotinas individuais. Ela permite o processamento automatizado de grandes volumes de dados, promovendo rapidez e precisão na geração de informações (VIGLIAR, 2023).

Conforme observa Polido (2024), a inteligência artificial integra um paradigma sociotécnico que combina conectividade global, automação e vigilância de dados, ampliando as capacidades analíticas dos sistemas de informação. Essa integração, contudo, carrega implicações significativas para os direitos fundamentais dos cidadãos.

No Brasil, o uso institucional da IA, especialmente por órgãos de segurança pública, cresce sem um debate regulatório proporcional. Tecnologias como reconhecimento facial e análise preditiva vêm sendo aplicadas em contextos sensíveis, sem garantias suficientes de proteção aos direitos individuais (ANDRÉA; DA SILVA; GUNDIM, 2022).

Tais práticas expandem os mecanismos tradicionais de vigilância estatal, muitas vezes sem transparência, consentimento ou avaliação crítica sobre seus riscos sociais. A ausência de auditoria e de controle social efetivo eleva a possibilidade de abusos e discriminações (TOBBIN; CARDIN, 2021).

Sarlet e Sarlet (2022) alertam para o fato de que o uso não regulado da IA, especialmente em ambientes públicos, pode ferir princípios constitucionais, como a privacidade, a liberdade de expressão e a igualdade. A opacidade dos algoritmos agrava esse risco, pois dificulta a compreensão e a contestação de decisões automatizadas.

De acordo com Barbosa e Pinheiro (2023), é essencial que o ordenamento jurídico acompanhe essas inovações tecnológicas por meio de mecanismos normativos que assegurem transparência, auditabilidade e responsabilidade no uso da IA. Sem isso, o avanço tecnológico pode caminhar em descompasso com a proteção dos direitos humanos.

Diante disso, faz-se necessária a elaboração de políticas públicas específicas, com enfoque na regulação ética e jurídica da inteligência artificial. Esse esforço deve envolver a academia, o poder público e a sociedade civil, de modo a garantir o equilíbrio entre inovação e salvaguardas constitucionais (ACIOLY; MENDES; NETO, 2023).

## 2.2 VIGILÂNCIA ALGORÍTMICA E CAPITALISMO DE DADOS

A vigilância algorítmica é caracterizada pelo uso de sistemas computacionais capazes de processar dados em larga escala, identificar padrões e produzir decisões automatizadas. Essa prática, embora tecnologicamente eficiente, levanta sérios questionamentos sobre sua legitimidade democrática e jurídica (TOBBIN; CARDIN, 2021).

Segundo os autores, o que diferencia a vigilância algorítmica das formas tradicionais é

sua capacidade de operar de modo invisível, contínuo e preditivo. Isso ocorre sem o conhecimento ou o consentimento efetivo dos indivíduos monitorados, o que compromete os princípios da autodeterminação informacional e da privacidade.

Esses sistemas são empregados em diferentes esferas: policiamento preditivo, triagens automatizadas em políticas públicas, monitoramento em tempo real e análise de comportamento. Tais aplicações indicam uma mudança de paradigma, onde o controle se torna silencioso e automatizado (DE TEFFÉ; MEDON, 2020).

No ambiente digital, essa lógica tem sido denominada como capitalismo de vigilância, conceito segundo o qual os dados pessoais são transformados em mercadorias e utilizados para fins comerciais e de controle social. Nesse cenário, os algoritmos assumem papel central na arquitetura do poder informacional (TOBBIN; CARDIN, 2021).

Além disso, sistemas algorítmicos frequentemente refletem e amplificam desigualdades sociais históricas. Como destaca Sarlet e Rodriguez (2022), algoritmos treinados com dados enviesados tendem a reproduzir discriminações raciais, de gênero e de classe, promovendo resultados injustos sob uma aparência de neutralidade técnica.

A ausência de regulação específica sobre o uso dessas ferramentas contribui para o agravamento desses riscos. A opacidade das decisões algorítmicas, combinada à dificuldade de auditoria, limita a responsabilização dos agentes envolvidos e dificulta o exercício de direitos pelos afetados (BARBOSA; PINHEIRO, 2023).

A utilização de algoritmos em ambientes públicos, especialmente por órgãos de segurança, exige transparência, critérios de proporcionalidade e a adoção de mecanismos de supervisão independentes. Isso é essencial para impedir abusos e garantir a proteção dos direitos fundamentais (ACIOLY; MENDES; NETO, 2023).

Portanto, é necessário repensar criticamente o uso da IA como ferramenta de vigilância, exigindo marcos regulatórios que assegurem justiça, equidade e responsabilidade. A vigilância algorítmica não pode operar à margem dos princípios do Estado Democrático de Direito (SARLET; SARLET, 2022).

## 2.3 DIREITOS FUNDAMENTAIS E DESAFIOS ÉTICO-JURÍDICOS DA VIGILÂNCIA AUTOMATIZADA

O uso de tecnologias de inteligência artificial para fins de vigilância impõe sérios desafios à proteção dos direitos fundamentais. A privacidade, a liberdade de expressão, a presunção

de inocência e a igualdade de tratamento são alguns dos direitos mais diretamente impactados pela vigilância algorítmica. Isso ocorre porque os sistemas automatizados tendem a operar com base em critérios estatísticos que, embora eficientes, nem sempre respeitam as nuances e os contextos sociais dos indivíduos monitorados (SARLET; SARLET, 2022).

A opacidade dos algoritmos utilizados por instituições públicas dificulta a compreensão sobre como decisões são tomadas, o que compromete o direito à informação e à ampla defesa. Quando cidadãos não conseguem identificar os critérios utilizados para classificações ou sanções automatizadas, há grave violação à transparência e à accountability. De acordo com Tobbin e Cardin (2021), a vigilância digital em larga escala transforma os indivíduos em objetos de análise e controle, corroendo a autonomia pessoal e enfraquecendo a cidadania.

Outro aspecto preocupante é a possibilidade de discriminação algorítmica, resultado da reprodução de preconceitos históricos nos conjuntos de dados utilizados para treinar os sistemas de IA. Como afirmam Sarlet e Rodriguez (2022), algoritmos podem reforçar desigualdades sociais ao operar com base em dados enviesados ou mal contextualizados, prejudicando grupos vulneráveis e aumentando a exclusão social. O ideal de neutralidade tecnológica, frequentemente defendido, se mostra ilusório diante dessas evidências.

Em contextos de segurança pública, a adoção de tecnologias como reconhecimento facial e análise comportamental preditiva tende a afetar desproporcionalmente comunidades racializadas e periféricas. Estudos apontam que tais ferramentas possuem maior margem de erro na identificação de pessoas negras e indígenas, o que agrava a seletividade penal e compromete o princípio da igualdade perante a lei (BARBOSA; PINHEIRO, 2023). Essa seletividade algorítmica deve ser tratada como um problema jurídico e não apenas técnico.

Além disso, o uso de inteligência artificial sem o devido respaldo jurídico viola o princípio da legalidade, previsto no artigo 5º, inciso II, da Constituição Federal. A ausência de norma clara que autorize e delimite o uso da IA em ambientes públicos compromete o Estado de Direito, pois permite a atuação tecnológica sem controle, sem motivação e sem possibilidade real de contestação. Isso é incompatível com uma sociedade democrática (SIEVERS, 2020).

A proteção contra decisões automatizadas exige mecanismos legais que garantam revisão humana qualificada, direito à explicação e possibilidade de contestação formal. Nesse sentido, Acioly, Mendes e Neto (2023) propõem as avaliações de impacto algorítmico como instrumento essencial para identificar riscos

e mitigar danos antes da implementação de sistemas decisórios baseados em IA. Essa ferramenta permite maior transparência e compatibilização com os direitos fundamentais.

A ausência de responsabilização clara em casos de violação de direitos por algoritmos agrava a vulnerabilidade dos cidadãos. Em muitos casos, nem mesmo os próprios agentes públicos compreendem o funcionamento interno dos sistemas utilizados, o que dificulta a identificação de culpados e o devido processo legal. Essa lacuna jurídica reforça a urgência de uma governança algorítmica participativa e orientada por princípios éticos (DE TEFFÉ; MEDON, 2020).

Em suma, a vigilância automatizada exige uma resposta jurídica robusta, capaz de equilibrar os benefícios da inovação tecnológica com os limites impostos pela Constituição. A defesa dos direitos fundamentais não deve ser relativizada diante do avanço técnico, mas reafirmada como eixo estruturante das políticas públicas digitais. É papel do direito construir limites claros, mecanismos de controle e espaços de participação social nesse novo cenário digital.

#### 2.4 A LEI GERAL DE PROTEÇÃO DE DADOS E SEUS LIMITES DIANTE DA INTELIGÊNCIA ARTIFICIAL

A promulgação da Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), representou um marco normativo no ordenamento jurídico brasileiro. Inspirada no Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, a LGPD estabeleceu princípios e diretrizes para o tratamento de dados pessoais no Brasil, buscando assegurar a privacidade e a autodeterminação informacional dos cidadãos (BARBOSA; PINHEIRO, 2023).

A LGPD parte de princípios fundamentais como a finalidade, a necessidade, a transparência, a segurança e a responsabilização, exigindo que o tratamento de dados ocorra com base legal clara e de maneira proporcional. Esses princípios se aplicam a agentes públicos e privados, sendo obrigatória a adoção de medidas técnicas e administrativas para proteger os dados pessoais contra acessos indevidos (SARLET; RODRIGUEZ, 2022).

Apesar dos avanços promovidos, a LGPD apresenta lacunas significativas no que se refere à regulação da inteligência artificial e da vigilância algorítmica. A lei não trata de forma específica as decisões automatizadas com base em algoritmos complexos, tampouco exige a explicabilidade dos sistemas de IA utilizados por entes públicos, o que compromete a efetividade do direito à informação (TOBBIN; CARDIN, 2021).

A ausência de obrigação expressa de fornecer justificativas compreensíveis sobre decisões automatizadas dificulta o exercício dos

direitos dos titulares, como o direito à revisão e à correção de dados. Isso é especialmente crítico em contextos em que decisões com grande impacto, como concessão de benefícios, aplicação de sanções ou ações de segurança, são tomadas por sistemas de IA (SIEVERS, 2020). Outro problema refere-se às exceções previstas no art. 4º da LGPD, que excluem de sua aplicação os tratamentos de dados realizados para fins de segurança pública, defesa nacional e investigação criminal. Tal exceção, embora compreensível em certos contextos, pode abrir margem para abusos quando utilizada como justificativa para implantações tecnológicas sem a devida regulamentação específica (BARBOSA; PINHEIRO, 2023).

A interpretação extensiva desse dispositivo pode resultar em um “limbo jurídico”, em que órgãos de segurança pública utilizam tecnologias de vigilância com

escasso controle normativo. Como apontam Sarlet e Sarlet (2022), é necessário um regime especial que contemple os riscos específicos da IA sem suprimir os direitos fundamentais assegurados constitucionalmente.

Ademais, a atuação da Autoridade Nacional de Proteção de Dados (ANPD) ainda é incipiente diante dos desafios impostos pelas tecnologias emergentes. A ANPD possui a atribuição de regulamentar e fiscalizar a aplicação da LGPD, mas carece de instrumentos normativos próprios que tratem da inteligência artificial e suas especificidades no contexto da administração pública (ACIOLY; MENDES; NETO, 2023).

A ausência de normativas secundárias voltadas à IA fragiliza a implementação efetiva da LGPD, dificultando a responsabilização por danos causados por algoritmos e sistemas preditivos. A falta de clareza sobre os deveres dos controladores e operadores de IA compromete a segurança jurídica dos usuários e a atuação do Poder Judiciário.

Para lidar com essas limitações, especialistas defendem a criação de uma legislação complementar ou específica para inteligência artificial. Tal norma deveria abordar critérios de desenvolvimento, testes de impacto, auditoria, explicabilidade e responsabilização, bem como direitos específicos dos cidadãos frente às decisões automatizadas (DE TEFFÉ; MEDON, 2020).

Nesse contexto, torna-se indispensável repensar o papel da LGPD como pilar normativo e alicerce inicial de uma regulação mais ampla e robusta sobre as tecnologias algorítmicas. A lei deve ser compreendida como ponto de partida, mas não como instrumento único, diante da complexidade e autonomia dos sistemas de IA.

Assim, a efetiva proteção dos dados pessoais e dos direitos fundamentais no cenário da inteligência artificial depende da combinação entre legislação geral, normativas específicas e políticas

públicas transparentes. Apenas com esse tripé normativo será possível compatibilizar inovação tecnológica e dignidade humana no espaço digital.

## 2.5 CAMINHOS REGULATÓRIOS PARA A RESPONSABILIZAÇÃO DE SISTEMAS ALGORÍTMICOS NO BRASIL

A crescente utilização de sistemas algorítmicos para tomada de decisões automatizadas impõe novos desafios ao modelo tradicional de responsabilização jurídica. O arcabouço normativo vigente ainda não contempla, de forma satisfatória, os riscos associados à autonomia técnica desses sistemas, o que exige a construção de mecanismos específicos de regulação e controle (DE TEFFÉ; MEDON, 2020).

Os modelos atuais de responsabilidade civil baseiam-se, em regra, na relação direta entre a ação ou omissão do agente e o dano causado. Contudo, na inteligência artificial, essa relação é muitas vezes indireta ou difícil de estabelecer, especialmente quando se trata de decisões geradas por sistemas de aprendizado de máquina que operam com baixa intervenção humana (BARBOSA; PINHEIRO, 2023).

Nesse cenário, é necessário avançar na formulação de critérios que permitam atribuir responsabilidade aos desenvolvedores, operadores e usuários de sistemas algorítmicos. Para isso, devem ser consideradas tanto a previsibilidade do dano quanto a obrigação de adoção de medidas preventivas, como testes, auditorias e avaliações de risco (ACIOLY; MENDES; NETO, 2023).

A literatura jurídica contemporânea aponta para a necessidade de adoção do dever de diligência tecnológica, que consiste na obrigação dos agentes envolvidos em prever, mitigar e responder por riscos advindos do uso da IA. Essa noção amplia o conceito de culpa, incluindo falhas no projeto, nos dados de treinamento ou na ausência de supervisão (TOBBIN; CARDIN, 2021).

A ausência de uma legislação específica dificulta a responsabilização objetiva por danos decorrentes de decisões automatizadas. Em muitos casos, a vítima sequer tem acesso às informações mínimas para identificar o erro, o que contraria os princípios da ampla defesa e do contraditório, pilares do devido processo legal (SARLET; SARLET, 2022).

A criação de um marco regulatório para a inteligência artificial no Brasil deve prever critérios claros de responsabilidade solidária entre os diversos agentes da cadeia tecnológica. Isso inclui empresas desenvolvedoras, contratantes públicos e operadores diretos dos sistemas, garantindo a proteção do usuário final (SARLET; RODRIGUEZ, 2022).

Outro caminho viável é a institucionalização de estruturas permanentes de governança algorítmica, com a participação de

especialistas, representantes da sociedade civil, entidades de fiscalização e órgãos públicos. Essas estruturas seriam responsáveis por aprovar normas técnicas, monitorar o uso da IA e avaliar impactos sociais (POLIDO, 2024).

As avaliações de impacto algorítmico, como propõem Acioly, Mendes e Neto (2023), devem ser obrigatórias antes da implantação de sistemas de IA em setores sensíveis como saúde, segurança pública e justiça. Essa avaliação deve considerar riscos de discriminação, violação de privacidade, opacidade e falhas sistêmicas.

Além disso, deve-se exigir que todos os sistemas utilizados pelo poder público sejam auditáveis, documentados e compatíveis com os princípios constitucionais. A opacidade tecnológica, quando adotada pelo Estado, compromete o controle social e fragiliza a democracia (VIGLIAR, 2023).

No campo judicial, o Judiciário precisa ser capacitado para lidar com litígios envolvendo IA compreendendo a lógica técnica dos algoritmos e os impactos jurídicos das decisões automatizadas. Sem isso, a responsabilização se torna ineficaz, e o acesso à justiça é comprometido.

Portanto, os caminhos regulatórios para a responsabilização da inteligência artificial no Brasil devem combinar instrumentos legais, técnicos e institucionais. Apenas um sistema integrado e multidisciplinar será capaz de garantir que a inovação tecnológica seja acompanhada de responsabilidade, justiça e segurança jurídica.

## 2.6 REGULAÇÃO PROPOSITIVA DA VIGILÂNCIA ALGORÍTMICA: DIRETRIZES PARA UMA SOLUÇÃO JURÍDICA

Diante dos riscos evidenciados pela vigilância algorítmica, torna-se urgente o desenvolvimento de uma regulação jurídica capaz de responder, de forma eficaz, aos impactos que tais tecnologias geram sobre os direitos fundamentais. A mera aplicação dos dispositivos gerais da LGPD mostra-se insuficiente para tutelar a complexidade dos sistemas autônomos, sendo necessário avançar para normativas específicas, focadas em decisões automatizadas e uso estatal da IA (SARLET; RODRIGUEZ, 2022).

A regulação proposta deve partir da premissa de que toda intervenção tecnológica que envolva coleta, cruzamento ou inferência de dados pessoais — sobretudo com fins de vigilância — deve respeitar os princípios constitucionais da legalidade, da proporcionalidade, da finalidade e da transparência. Para tanto, é imprescindível que se estabeleça uma base legal clara e detalhada, com previsões específicas sobre vigilância digital, inclusive no setor público (SIEVERS, 2020).

Uma das principais diretrizes regulatórias deve ser a obrigatoriedade da explicabilidade algorítmica, permitindo que os

indivíduos compreendam, em linguagem acessível, como decisões automatizadas são formuladas. Esse princípio viabiliza o controle democrático da tecnologia, impede o funcionamento opaco e fortalece o direito à informação e à ampla defesa (ACIOLY; MENDES; NETO, 2023).

Outro eixo central deve ser a institucionalização de auditorias obrigatórias para sistemas utilizados pelo poder público, especialmente aqueles que envolvam segurança, justiça e políticas sociais. Essas auditorias devem ser realizadas por entidades independentes, com participação da sociedade civil, e devem avaliar impactos discriminatórios, riscos de vazamento de dados e critérios técnicos de funcionamento (DE TEFFÉ; MEDON, 2020).

A regulação também precisa incluir a criação de uma autoridade técnica autônoma voltada à supervisão da inteligência artificial, que atue de forma complementar à ANPD. Essa autoridade teria a função de emitir pareceres técnicos, fiscalizar usos de IA sensíveis e propor atualizações normativas contínuas, conforme a evolução tecnológica (POLIDO, 2024).

É igualmente necessário que o ordenamento jurídico assegure direitos processuais específicos para decisões algorítmicas, como o direito à revisão humana qualificada, o direito à não discriminação automatizada e o direito à contestação. Esses direitos devem estar expressos em lei e garantir que qualquer cidadão possa reagir formalmente a decisões prejudiciais baseadas em IA (TOBBIN; CARDIN, 2021). No âmbito do setor privado, a legislação deve responsabilizar civilmente os desenvolvedores e fornecedores de tecnologias que causem danos por falhas estruturais nos algoritmos ou pelo uso indevido de dados. A adoção do princípio da responsabilidade solidária pode ser uma alternativa viável para garantir a reparação efetiva às vítimas de decisões injustas automatizadas (BARBOSA; PINHEIRO, 2023). Além disso, a regulação deve estabelecer como obrigatória a realização de avaliações de impacto algorítmico (AIA), especialmente em ambientes públicos. Tais instrumentos devem ser aplicados previamente à implementação dos sistemas, com relatórios públicos e auditáveis, visando identificar e mitigar eventuais riscos a direitos e liberdades (ACIOLY; MENDES; NETO, 2023).

A adoção de um marco regulatório progressivo e participativo, que envolva universidades, organizações da sociedade civil e o setor privado, permitirá uma construção coletiva e democrática das normas sobre inteligência artificial. Esse processo deve assegurar constante atualização e adaptação, diante da velocidade com que a tecnologia evolui (VIGLIAR, 2023).

Por fim, a resposta jurídica ao problema da vigilância algorítmica deve ir além da contenção

e avançar para uma cultura de uso ético e responsável da tecnologia, baseada na centralidade da dignidade humana. O Estado deve garantir que o avanço tecnológico seja acompanhado por salvaguardas robustas, garantindo que os algoritmos sirvam à justiça, e não ao controle abusivo dos cidadãos (SARLET; SARLET, 2022).

### 3 CONCLUSÃO

A presente pesquisa teve como objetivo analisar os impactos da vigilância algorítmica sobre os direitos fundamentais no Brasil, à luz do crescente uso de tecnologias de inteligência artificial em contextos públicos e privados. Constatou-se que, embora a IA represente uma inovação estratégica para diversos setores, sua aplicação sem o devido controle normativo compromete princípios essenciais do Estado Democrático de Direito.

A ausência de uma legislação específica que regule a atuação dos algoritmos de vigilância favorece práticas opacas, discriminatórias e incompatíveis com os direitos à privacidade, à igualdade e à liberdade. A atual LGPD, embora importante, mostra-se insuficiente para responder à complexidade técnica e ética da IA, sobretudo diante das exceções legais voltadas à segurança pública e à pouca efetividade da fiscalização.

Diante desse cenário, defende-se a criação de um marco regulatório próprio para inteligência artificial, que contemple a obrigatoriedade de avaliações de impacto algorítmico, a transparência dos processos decisórios automatizados, e a responsabilização objetiva de todos os agentes envolvidos. Além disso, é fundamental assegurar o direito à revisão humana, à explicação e à contestação das decisões automatizadas.

A regulação proposta deve ir além da repressão aos excessos, promovendo uma governança algorítmica baseada em valores constitucionais, participação social e fiscalização técnica qualificada. Para isso, é necessário integrar esforços entre o

Poder Legislativo, a ANPD, o sistema de justiça, universidades e organizações da sociedade civil.

A vigilância algorítmica, enquanto fenômeno estruturante da era digital, não pode se desenvolver à revelia dos direitos fundamentais. O uso da inteligência artificial pelo Estado e pelo mercado deve estar ancorado em um projeto jurídico que privilegie a dignidade da pessoa humana, a não discriminação e o devido processo legal.

Portanto, a resposta jurídica ao problema proposto não está apenas na contenção da tecnologia, mas na sua reorientação ética. Ao colocar o ser humano no centro das decisões e garantir o controle institucional das ferramentas digitais, o direito reafirma seu papel de equilíbrio

entre inovação e justiça social.

A construção de um modelo regulatório sólido e democrático é o caminho para assegurar que a inteligência artificial, em vez de agravar desigualdades e restringir liberdades, se torne uma aliada da cidadania, da transparência e da proteção dos direitos humanos.

### REFERÊNCIAS

ACIOLY, Luis Henrique; MENDES, Isabelle Brito Bezerra; NETO, João Araújo Monteiro. As avaliações de impacto como instrumentos de inteligibilidade algorítmica e garantia de direitos fundamentais na regulação de inteligência artificial. *Diké – Revista Jurídica*, v. 22, n. 24, p. 225-251, 2023.

BARBOSA, Leonardo Figueiredo; PINHEIRO, Caroline. Inteligência artificial no Brasil: avanços regulatórios. *Revista de Informação Legislativa*, v. 60, n. 240, p. 11-41, 2023.

DE TEFFÉ, Chiara Spadaccini; MEDON, Filipe. Responsabilidade civil e regulação de novas tecnologias: questões acerca da utilização de inteligência artificial na tomada de decisões empresariais. *REI – Revista Estudos Institucionais*, v. 6, n. 1, p. 301- 333, 2020.

POLIDO, Fabrício Bertini Pasquot. Estado, soberania digital e tecnologias emergentes: interações entre direito internacional, segurança cibernética e inteligência artificial. *Revista de Ciências do Estado*, v. 9, n. 1, p. 1-30, 2024.

SARLET, Ingo Wolfgang; SARLET, Grabielle Bezerra Sales. Algumas notas sobre a relação entre inteligência artificial, proteção de dados pessoais e os direitos fundamentais na ordem constitucional brasileira. *Revista Jurídica de Asturias*, n. 45, 2022.

SIEVERS, Fretz. Lei Geral de Proteção de Dados, Lei de Acesso à Informação e a Improbidade Administrativa: um novo cenário para o agente público na sociedade da informação. *Conhecimento Interativo*, v. 14, n. 2, 2020.

TOBBIN, Raíssa Arantes; CARDIN, Valéria Silva Galdino. Tecnologias vestíveis e capitalismo de vigilância: do compartilhamento de dados sobre saúde e a proteção dos direitos da personalidade. *Revista de Direito, Governança e Novas Tecnologias*, v. 7, n. 1, p. 126-147, 2021.

VIGLIAR, José Marcelo Menezes. *Inteligência Artificial: Aspectos Jurídicos*. São Paulo: Almedina Brasil, 2023.