

INTELIGÊNCIA ARTIFICIAL E RESPONSABILIDADE JURÍDICA: DESAFIOS PARA A PROTEÇÃO DOS DIREITOS FUNDAMENTAIS

ARTIFICIAL INTELLIGENCE AND LEGAL LIABILITY: CHALLENGES FOR THE
PROTECTION OF FUNDAMENTAL RIGHTS

INTELIGENCIA ARTIFICIAL Y RESPONSABILIDAD JURÍDICA: DESAFÍOS PARA
LA PROTECCIÓN DE LOS DERECHOS FUNDAMENTALES

Rennan Christian Silva Lins de Oliveira¹, William Carvalho Guimarães², Rosa Caroline Teixeira³,
Juliana de Macedo Ferreira Carelle⁴, Sandra Cavalcante Sousa da Silva⁵, Luciane Santos Roque⁶

DOI: 10.54899/dcs.v23i93.6473

Recibido: 01/07/2026 | Aceptado: 27/07/2026 | Publicación en línea: 04/08/2026.

RESUMO

O presente artigo analisou os desafios jurídicos decorrentes do desenvolvimento e da utilização da inteligência artificial, com ênfase na proteção dos direitos fundamentais e na responsabilização pelos danos produzidos por sistemas automatizados. A pesquisa adotou abordagem qualitativa, de caráter bibliográfico e documental, fundamentada em livros, artigos científicos, normas jurídicas e documentos institucionais nacionais e internacionais. Os resultados demonstraram que a inteligência artificial pode contribuir para a eficiência de serviços públicos e privados, mas também pode ampliar riscos relacionados à privacidade, à proteção de dados pessoais, à discriminação algorítmica, à opacidade das decisões e à dificuldade de identificação dos responsáveis. Verificou-se que a responsabilização jurídica não deve ocorrer apenas após o dano, sendo necessária a adoção de medidas preventivas, como avaliação de riscos, transparência, supervisão humana, auditoria, segurança e possibilidade de contestação. Concluiu-se que o ordenamento jurídico brasileiro já oferece instrumentos relevantes para a proteção da pessoa, embora ainda existam lacunas diante das particularidades dos sistemas inteligentes. Assim, a regulamentação da inteligência artificial deve equilibrar inovação, segurança jurídica e respeito à dignidade humana, garantindo que o avanço tecnológico permaneça submetido aos valores democráticos e aos direitos fundamentais.

Palavras-chave: Inteligência Artificial. Responsabilidade Jurídica. Direitos Fundamentais. Proteção de Dados. Regulação.

¹Mestrando em Estudos Jurídicos com Ênfase em Direito Internacional, MUST University, Deerfield Beach, Flórida, Estados Unidos. E-mail: rennanlins2@hotmail.com

²Especialista em Direito Penal e Processo Penal com capacitação para o Magistério Superior, Universidade de Fortaleza (UNIFOR), Fortaleza, Ceará, Brasil. E-mail: wilcguimaraes@gmail.com

³Pós-Graduação Lato Sensu em Direito Público, Faculdade Educamais, São Paulo, São Paulo, Brasil.

E-mail: rcaroline@id.uff.br

⁴Pós-Graduação em Licitações e Contratos Administrativos, Universidade Unopar, Londrina, Paraná, Brasil.

E-mail: julianamf@id.uff.br

⁵Mestranda em Direito, Governança e Políticas Públicas, Universidade de Salvador (UNIFACS), Salvador, Bahia, Brasil. E-mail: sandracavalsousa@gmail.com

⁶Pós-Graduação em Direito Educacional, Faculdade Unina, Curitiba Paraná, Brasil. E-mail: luasroque@gmail.com

ABSTRACT

This article analyzed the legal challenges arising from the development and use of artificial intelligence, with emphasis on the protection of fundamental rights and liability for damages caused by automated systems. The research adopted a qualitative, bibliographic, and documentary approach, based on books, scientific articles, legal standards, and national and international institutional documents. The results showed that artificial intelligence can contribute to the efficiency of public and private services, but it can also increase risks related to privacy, personal data protection, algorithmic discrimination, decision-making opacity, and difficulties in identifying responsible parties. It was found that legal liability should not occur only after damage has been caused, making it necessary to adopt preventive measures such as risk assessment, transparency, human oversight, auditing, security, and the possibility of contesting decisions. It was concluded that the Brazilian legal system already provides relevant instruments for the protection of individuals, although gaps remain regarding the specific characteristics of intelligent systems. Therefore, artificial intelligence regulation must balance innovation, legal certainty, and respect for human dignity, ensuring that technological development remains subject to democratic values and fundamental rights.

Keywords: Artificial Intelligence. Legal Liability. Fundamental Rights. Data Protection. Regulation.

RESUMEN

El presente artículo analizó los desafíos jurídicos derivados del desarrollo y uso de la inteligencia artificial, con énfasis en la protección de los derechos fundamentales y en la responsabilidad por los daños producidos por sistemas automatizados. La investigación adoptó un enfoque cualitativo, bibliográfico y documental, fundamentado en libros, artículos científicos, normas jurídicas y documentos institucionales nacionales e internacionales. Los resultados demostraron que la inteligencia artificial puede contribuir a la eficiencia de los servicios públicos y privados, pero también puede ampliar los riesgos relacionados con la privacidad, la protección de datos personales, la discriminación algorítmica, la opacidad de las decisiones y la dificultad para identificar a los responsables. Se verificó que la responsabilidad jurídica no debe producirse únicamente después del daño, siendo necesaria la adopción de medidas preventivas, como evaluación de riesgos, transparencia, supervisión humana, auditoría, seguridad y posibilidad de impugnación. Se concluyó que el ordenamiento jurídico brasileño ya ofrece instrumentos relevantes para la protección de las personas, aunque todavía existen vacíos frente a las particularidades de los sistemas inteligentes. Por lo tanto, la regulación de la inteligencia artificial debe equilibrar innovación, seguridad jurídica y respeto a la dignidad humana, garantizando que el avance tecnológico permanezca sometido a los valores democráticos y a los derechos fundamentales.

Palabras clave: Inteligencia Artificial. Responsabilidad Jurídica. Derechos Fundamentales. Protección de Datos. Regulación.



Esta obra está bajo una [Licencia Creative Commons Atribución- NoComercial 4.0 Internacional](https://creativecommons.org/licenses/by-nc/4.0/)

INTRODUÇÃO

A inteligência artificial tem ocupado um espaço cada vez mais expressivo nas relações sociais, econômicas e institucionais, deixando de ser uma tecnologia restrita aos ambientes científicos para integrar decisões que afetam diretamente a vida das pessoas. Sistemas algorítmicos já são utilizados na seleção de trabalhadores, concessão de crédito, definição de perfis de consumo, reconhecimento facial, diagnósticos médicos, segurança pública e prestação de serviços estatais. Embora essas aplicações ofereçam benefícios relacionados à rapidez, à eficiência e à capacidade de processamento de grandes volumes de informações, também produzem questionamentos jurídicos importantes. Isso ocorre porque decisões tomadas ou influenciadas por sistemas automatizados podem atingir direitos individuais e coletivos, especialmente quando não são acompanhadas de transparência, critérios compreensíveis e mecanismos adequados de controle humano.

No ordenamento jurídico brasileiro, a utilização dessas tecnologias deve ser interpretada a partir da centralidade da pessoa humana e da proteção dos direitos fundamentais. A Constituição Federal assegura, entre outros direitos, a vida, a liberdade, a igualdade, a segurança, a intimidade, a vida privada, a honra e a imagem, estabelecendo limites para práticas públicas e privadas que possam violar essas garantias. Além disso, a Emenda Constitucional nº 115, de 2022, incluiu expressamente a proteção dos dados pessoais entre os direitos e garantias fundamentais. Desse modo, a inovação tecnológica não pode ser compreendida como um campo separado da ordem constitucional, pois o desenvolvimento e a aplicação da inteligência artificial devem respeitar a dignidade humana, a não discriminação, a autonomia individual e o livre desenvolvimento da personalidade.

Entre os principais desafios jurídicos relacionados à inteligência artificial encontra-se a identificação dos responsáveis pelos danos produzidos por decisões algorítmicas. A complexidade aumenta quando participam do funcionamento de um sistema diferentes agentes, como desenvolvedores, fornecedores, empresas contratantes, operadores de dados, plataformas digitais e usuários profissionais. Em determinadas situações, torna-se difícil estabelecer se o dano decorreu de uma falha na programação, da baixa qualidade dos dados utilizados, da ausência de supervisão humana, do uso inadequado da ferramenta ou de uma combinação desses fatores. Essa fragmentação da cadeia tecnológica pode dificultar a demonstração do nexo causal e o acesso da vítima à reparação, especialmente quando o funcionamento interno do sistema não é

suficientemente explicado. Por essa razão, a responsabilidade jurídica precisa considerar não apenas o resultado prejudicial, mas também os deveres de prevenção, segurança, transparência, fiscalização e governança assumidos por cada agente envolvido.

A Lei Geral de Proteção de Dados Pessoais representa uma das principais bases normativas brasileiras para enfrentar parte desses problemas, uma vez que estabelece princípios como finalidade, adequação, necessidade, transparência, segurança, prevenção, não discriminação e responsabilização. A norma também assegura ao titular o direito de solicitar a revisão de decisões tomadas unicamente com base no tratamento automatizado de dados pessoais que afetem seus interesses, inclusive decisões relacionadas aos seus perfis profissional, pessoal, de consumo e de crédito. Entretanto, a proteção jurídica não se encerra na tutela dos dados pessoais, pois sistemas de inteligência artificial podem gerar danos mesmo quando não utilizam diretamente informações identificáveis. Assim, a responsabilidade relacionada à inteligência artificial deve dialogar com a Constituição Federal, o Código Civil, o Código de Defesa do Consumidor, o Marco Civil da Internet e as normas aplicáveis à Administração Pública, conforme a natureza da relação jurídica analisada.

No cenário internacional, o Regulamento Europeu de Inteligência Artificial consolidou uma abordagem baseada na classificação dos sistemas conforme os níveis de risco, estabelecendo obrigações mais rigorosas para aplicações capazes de afetar a saúde, a segurança e os direitos fundamentais. Entre as medidas previstas estão a gestão de riscos, a transparência, a qualidade dos dados, a documentação técnica, a supervisão humana e a avaliação de impacto sobre direitos fundamentais em determinadas utilizações de alto risco. No Brasil, o debate regulatório permanece em construção. O Projeto de Lei nº 2.338/2023, aprovado pelo Senado e encaminhado à Câmara dos Deputados em março de 2025, encontrava-se, em agosto de 2026, aguardando parecer na comissão especial responsável por sua análise. A proposta busca estabelecer normas para o desenvolvimento e o uso ético e responsável da inteligência artificial, demonstrando a necessidade de uma legislação capaz de conciliar inovação, segurança jurídica e proteção da pessoa humana.

Diante desse contexto, o presente artigo parte do seguinte questionamento: de que maneira a responsabilidade jurídica relacionada ao desenvolvimento e ao uso da inteligência artificial pode contribuir para a proteção efetiva dos direitos fundamentais? O objetivo geral consiste em analisar os principais desafios jurídicos decorrentes da utilização de sistemas de inteligência artificial, com ênfase na atribuição de responsabilidades, na prevenção de danos e na garantia dos

direitos das pessoas afetadas por decisões automatizadas. A relevância da discussão está na necessidade de impedir que a complexidade tecnológica seja utilizada como justificativa para a ausência de responsabilização ou para a redução das garantias constitucionais. Defende-se, portanto, que a inteligência artificial deve ser desenvolvida e utilizada a partir de uma perspectiva centrada no ser humano, na qual inovação e responsabilidade caminhem juntas, assegurando transparência, supervisão, possibilidade de contestação e reparação adequada diante de eventuais violações.

DESENVOLVIMENTO

A Proteção dos Direitos Fundamentais Diante das Decisões Algorítmicas

A análise jurídica da inteligência artificial deve partir da compreensão de que a tecnologia não constitui um fim em si mesma, mas um instrumento criado para atender necessidades humanas. Por essa razão, sua utilização precisa estar subordinada aos valores estabelecidos pela Constituição Federal, especialmente à dignidade da pessoa humana, à cidadania, à igualdade e à liberdade. A eficiência oferecida pelos sistemas automatizados não autoriza que pessoas sejam reduzidas a dados, padrões estatísticos ou classificações produzidas sem consideração pelas particularidades de cada situação. Quando uma decisão algorítmica interfere no acesso ao trabalho, à educação, à saúde, à justiça ou a um serviço essencial, seus efeitos deixam de ser apenas tecnológicos e passam a exigir uma leitura constitucional. Conforme dispõe a Constituição Federal, a dignidade humana representa um dos fundamentos do Estado Democrático de Direito e deve orientar tanto a atuação estatal quanto as relações privadas (Brasil, 1988).

Entre os direitos mais diretamente afetados pelo avanço da inteligência artificial encontram-se a privacidade e a proteção dos dados pessoais. A Emenda Constitucional nº 115, de 2022, reconheceu expressamente a proteção de dados pessoais, inclusive nos meios digitais, como um direito fundamental. Essa inclusão reforçou a necessidade de controle sobre a coleta, o armazenamento, o compartilhamento e a utilização de informações capazes de identificar ou caracterizar uma pessoa. A Lei Geral de Proteção de Dados Pessoais complementa essa proteção ao estabelecer que o tratamento de dados deve respeitar a liberdade, a privacidade e o livre desenvolvimento da personalidade. Portanto, sistemas de inteligência artificial que dependem de grandes bases de dados não podem utilizar informações pessoais sem finalidade legítima,

necessidade demonstrada e medidas adequadas de segurança (Brasil, 2018; Brasil, 2022).

A igualdade e a não discriminação também ocupam posição central nesse debate, pois os resultados produzidos pela inteligência artificial dependem da forma como os sistemas são desenvolvidos e dos dados utilizados em seu treinamento. Quando uma base de dados reproduz desigualdades históricas, exclusões sociais ou representações desequilibradas de determinados grupos, o sistema pode repetir essas distorções em suas respostas. Isso pode ocorrer, por exemplo, em processos de recrutamento, análise de crédito, reconhecimento facial ou avaliação de riscos. A LGPD estabelece a não discriminação como um dos princípios do tratamento de dados pessoais, impedindo sua utilização para fins ilícitos ou abusivos. A UNESCO também destaca que o desenvolvimento da inteligência artificial deve respeitar a equidade, a dignidade humana, a transparência e os direitos fundamentais, evitando que a inovação aprofunde desigualdades já existentes (Brasil, 2018; UNESCO, 2021).

Outro aspecto relevante está relacionado à autonomia das pessoas diante de decisões automatizadas. Em muitos casos, o indivíduo não sabe que está sendo avaliado por um sistema algorítmico, não conhece as informações utilizadas nem compreende os critérios que determinaram determinado resultado. Esse cenário compromete a possibilidade de contestação e pode fazer com que uma decisão tecnológica seja recebida como definitiva ou incontestável. O artigo 20 da LGPD assegura ao titular dos dados o direito de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado que afetem seus interesses. A norma também determina que o controlador forneça informações claras e adequadas sobre os critérios e procedimentos empregados, ainda que sejam preservados os segredos comercial e industrial. Dessa forma, a proteção jurídica exige que a pessoa tenha condições reais de compreender, questionar e buscar a revisão do resultado produzido pelo sistema (Brasil, 2018).

No âmbito do Poder Público, a utilização de inteligência artificial precisa observar, além dos direitos individuais, os princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência. A automatização de decisões administrativas ou judiciais não pode afastar o dever de fundamentação nem impedir que o cidadão conheça os motivos de uma medida que afete sua esfera jurídica. No Poder Judiciário brasileiro, a Resolução nº 615/2025 do Conselho Nacional de Justiça determina que as soluções de inteligência artificial sejam avaliadas de acordo com seu nível de risco e com o impacto que possam produzir sobre os direitos fundamentais. A norma prevê ainda mecanismos de governança, auditoria, monitoramento, transparência e supervisão, demonstrando que a adoção dessas ferramentas deve fortalecer a prestação jurisdicional, e não

substituir a responsabilidade de magistrados e servidores (Brasil, 1988; CNJ, 2025).

A proteção dos direitos fundamentais também envolve a preservação da liberdade de expressão, da honra, da imagem e da identidade pessoal. Ferramentas capazes de produzir textos, vozes, imagens e vídeos sintéticos ampliam as possibilidades de criação, mas também podem ser utilizadas para manipular informações, imitar pessoas e disseminar conteúdos falsos. Nessas situações, o dano pode alcançar não apenas a privacidade, mas a reputação, a segurança e a liberdade de formação da opinião. O Alto Comissariado das Nações Unidas para os Direitos Humanos alerta que o uso crescente de sistemas baseados em dados pode produzir impactos discriminatórios, interferências na privacidade e limitações ao exercício de direitos. A UNESCO acrescenta que a responsabilidade final pelas decisões e pelos resultados da inteligência artificial deve permanecer atribuída a pessoas ou instituições, não sendo adequado reconhecer autonomia jurídica aos próprios sistemas (OHCHR, 2021; UNESCO, 2021).

Responsabilidade Civil e Identificação dos Agentes Envolvidos

A responsabilidade civil representa um dos principais instrumentos utilizados para reparar os prejuízos decorrentes do uso inadequado da inteligência artificial. O Código Civil estabelece que aquele que, por ação ou omissão voluntária, negligência ou imprudência, viola um direito e causa dano a outra pessoa pratica ato ilícito. A legislação também determina que quem causar dano fica obrigado a repará-lo, admitindo a responsabilidade independentemente da existência de culpa quando a atividade desenvolvida implicar risco para os direitos de terceiros. Essas disposições podem ser aplicadas aos danos algorítmicos, mas a complexidade dos sistemas tecnológicos exige uma análise cuidadosa da conduta, do dano, do nexo causal e do grau de participação de cada agente. Assim, a novidade tecnológica não elimina os fundamentos tradicionais da responsabilidade civil, embora demande sua interpretação de acordo com as características do ambiente digital (Brasil, 2002).

Uma das dificuldades está na existência de uma cadeia formada por diversos participantes. O desenvolvimento de um sistema de inteligência artificial pode envolver empresas que produzem o modelo, profissionais que realizam sua programação, organizações que fornecem dados, plataformas que disponibilizam a tecnologia e instituições que a utilizam em suas atividades. Em razão dessa divisão, nem sempre o agente que apresenta o sistema ao público é o mesmo que controla seu funcionamento ou define a finalidade de uso. A LGPD diferencia as

funções do controlador, responsável pelas decisões relacionadas ao tratamento dos dados, e do operador, que realiza o tratamento conforme as instruções recebidas. Essa distinção pode contribuir para identificar responsabilidades, mas não afasta a necessidade de examinar concretamente quem possuía capacidade de prevenir, corrigir ou interromper a prática causadora do dano (Brasil, 2018).

Nos casos que envolvem tratamento de dados pessoais, a LGPD estabelece regras específicas de responsabilidade e reparação. De acordo com seu artigo 42, o controlador ou o operador que causar dano patrimonial, moral, individual ou coletivo em violação à legislação de proteção de dados deve repará-lo. A lei admite responsabilidade solidária quando o operador descumpre suas obrigações legais ou não segue as instruções lícitas do controlador, bem como quando mais de um controlador participa diretamente da operação que causou o prejuízo. O tratamento também é considerado irregular quando não oferece a segurança que o titular legitimamente poderia esperar. Essas regras são importantes para impedir que a divisão técnica das tarefas seja utilizada como argumento para afastar a reparação devida à pessoa prejudicada (Brasil, 2018).

Quando a inteligência artificial é utilizada no fornecimento de produtos ou serviços, também podem ser aplicadas as disposições do Código de Defesa do Consumidor. O CDC estabelece que fabricantes e fornecedores respondem, independentemente de culpa, pelos danos causados por defeitos do produto ou do serviço, inclusive quando as informações sobre sua utilização e seus riscos são insuficientes ou inadequadas. Um sistema pode ser considerado defeituoso quando não oferece a segurança que o consumidor legitimamente espera, considerando seu modo de fornecimento, os riscos previsíveis e o contexto em que foi colocado no mercado. Desse modo, uma empresa não deve ser afastada de sua responsabilidade apenas por afirmar que o resultado prejudicial foi produzido automaticamente pelo sistema. A decisão de empregar a ferramenta, definir sua finalidade e oferecê-la ao consumidor continua sendo uma atividade humana e empresarial (Brasil, 1990).

A responsabilidade também alcança o Poder Público quando sistemas automatizados são utilizados para prestar serviços ou tomar decisões administrativas. A Constituição Federal determina que as pessoas jurídicas de direito público e as entidades privadas prestadoras de serviços públicos respondam pelos danos que seus agentes causarem a terceiros no exercício de suas funções. Embora a inteligência artificial não seja um agente público, sua utilização integra a atividade administrativa quando adotada por um órgão estatal. Assim, uma decisão

automatizada que negue injustamente um benefício, classifique incorretamente um cidadão ou produza tratamento discriminatório pode gerar responsabilidade do Estado. A contratação de uma empresa desenvolvedora não deve transferir integralmente ao particular o dever estatal de garantir legalidade, segurança, transparência e respeito aos direitos fundamentais (Brasil, 1988).

A produção da prova constitui outro desafio importante, pois as vítimas geralmente não possuem acesso ao código, à base de dados, às instruções fornecidas ao sistema ou aos registros de funcionamento da ferramenta. Essa desigualdade informacional pode dificultar a demonstração do nexo entre o uso da inteligência artificial e o dano sofrido. Para reduzir esse desequilíbrio, a LGPD permite que o juiz inverta o ônus da prova quando houver verossimilhança, hipossuficiência ou excessiva dificuldade para o titular produzir a prova. O Código de Defesa do Consumidor também prevê a facilitação da defesa do consumidor, inclusive por meio da inversão do ônus probatório. Em litígios algorítmicos, esses mecanismos são fundamentais para evitar que a opacidade tecnológica inviabilize o acesso à justiça e transforme a complexidade do sistema em uma forma de proteção indevida para quem o desenvolveu ou utilizou (Brasil, 1990; Brasil, 2018).

Regulação, Governança e Prevenção dos Riscos da Inteligência Artificial

A proteção dos direitos fundamentais não pode depender apenas da reparação posterior dos danos. Em razão da velocidade, da escala e da capacidade de reprodução das decisões algorítmicas, torna-se necessário adotar uma abordagem preventiva, capaz de identificar e reduzir os riscos antes que o sistema seja disponibilizado ou utilizado. Uma das principais referências internacionais nesse sentido é o Regulamento Europeu de Inteligência Artificial, que organiza as obrigações de acordo com o nível de risco das aplicações. Quanto maior a possibilidade de impacto sobre a saúde, a segurança ou os direitos fundamentais, mais rigorosos são os deveres impostos aos fornecedores e utilizadores. Essa lógica demonstra que nem todos os sistemas precisam receber o mesmo tratamento jurídico, mas aqueles empregados em áreas sensíveis devem estar sujeitos a controles mais intensos (União Europeia, 2024).

No Brasil, a construção de um marco geral para a inteligência artificial ainda se encontra em andamento. O Projeto de Lei nº 2.338/2023 busca regulamentar o desenvolvimento, o fomento e o uso ético e responsável da tecnologia, adotando como fundamento a centralidade da pessoa humana e a proteção dos direitos fundamentais. A proposta trabalha com a classificação dos sistemas conforme os riscos envolvidos e prevê obrigações relacionadas à governança, à

transparência e à responsabilização. Em 4 de agosto de 2026, o projeto permanecia na Câmara dos Deputados, aguardando parecer do relator na comissão especial constituída para sua análise. A quantidade de projetos apensados revela a amplitude e a complexidade do tema, que envolve desde decisões automatizadas até conteúdos sintéticos, auditoria de vieses e proteção da identidade pessoal (Brasil, 2023).

Mesmo antes da aprovação de uma legislação específica, as organizações que utilizam inteligência artificial devem adotar programas internos de governança e gestão de riscos. A LGPD determina que medidas técnicas e administrativas de segurança sejam implementadas desde a fase de concepção do produto ou serviço até sua execução. A norma também recomenda a criação de regras de boas práticas, mecanismos internos de supervisão, procedimentos de atendimento aos titulares e medidas de mitigação de riscos. Aplicada à inteligência artificial, essa orientação significa que a proteção dos direitos não deve ser acrescentada somente após a ocorrência de um problema. Privacidade, segurança, explicabilidade e controle humano precisam integrar o planejamento, o treinamento, a implantação e o monitoramento contínuo do sistema (Brasil, 2018).

A avaliação de impacto constitui um instrumento essencial para concretizar essa prevenção. Antes de utilizar uma solução de alto risco, a organização deve identificar sua finalidade, os grupos que poderão ser afetados, os tipos de dados utilizados, os possíveis erros e as medidas disponíveis para evitar ou corrigir consequências negativas. O Regulamento Europeu prevê avaliação de impacto sobre os direitos fundamentais para determinadas utilizações de inteligência artificial de alto risco, especialmente quando adotadas por órgãos públicos ou prestadores de serviços públicos. No Brasil, a Resolução nº 615/2025 do CNJ determina que os tribunais classifiquem os sistemas conforme seu nível de risco e adotem medidas específicas de governança antes de colocar soluções de alto risco em funcionamento. Esses modelos podem orientar outros setores que utilizam a tecnologia em atividades capazes de afetar direitos relevantes (União Europeia, 2024; CNJ, 2025).

A supervisão humana deve permanecer presente durante todo o ciclo de vida da inteligência artificial. Não basta permitir que uma pessoa confirme formalmente uma resposta produzida pelo sistema; é necessário que ela tenha competência, informações e autonomia para compreender o resultado, discordar dele e impedir sua aplicação quando houver risco de injustiça. A UNESCO estabelece que a responsabilidade e a prestação de contas devem permanecer vinculadas a pessoas físicas ou jurídicas, pois os sistemas de inteligência artificial não possuem

consciência, vontade ou personalidade jurídica própria. A supervisão humana, portanto, não representa uma oposição à inovação, mas uma garantia de que a tecnologia continuará submetida a decisões responsáveis, especialmente nos contextos em que erros podem comprometer a dignidade, a liberdade ou a igualdade das pessoas (UNESCO, 2021).

A construção de uma regulação adequada exige equilíbrio entre o incentivo à inovação e a proteção efetiva da pessoa humana. Regras excessivamente genéricas podem ser insuficientes para controlar sistemas de alto impacto, enquanto exigências desproporcionais podem dificultar pesquisas e aplicações socialmente benéficas. O caminho mais adequado está na adoção de deveres proporcionais ao risco, acompanhados de transparência, documentação técnica, auditorias, segurança, canais de contestação, reparação de danos e fiscalização independente. A inteligência artificial deve contribuir para ampliar oportunidades e melhorar serviços, mas sua eficiência não pode ser alcançada mediante a redução de direitos. A responsabilidade jurídica cumpre, nesse cenário, uma função reparadora e preventiva, orientando empresas e instituições públicas a desenvolverem tecnologias confiáveis, humanamente supervisionadas e compatíveis com os valores democráticos (Brasil, 2018; CNJ, 2025; UNESCO, 2021; União Europeia, 2024).

METODOLOGIA

A presente pesquisa caracterizou-se como bibliográfica, de abordagem qualitativa e natureza exploratória e descritiva. Essa escolha metodológica mostrou-se adequada ao objetivo de analisar os desafios relacionados à responsabilidade jurídica decorrente do desenvolvimento e da utilização da inteligência artificial, especialmente no que se refere à proteção dos direitos fundamentais. A abordagem qualitativa possibilitou interpretar conceitos, normas jurídicas e posicionamentos teóricos, considerando a complexidade das relações entre tecnologia, sociedade e Direito.

A pesquisa bibliográfica foi desenvolvida por meio da análise de livros, artigos científicos, trabalhos acadêmicos e publicações especializadas relacionadas à inteligência artificial, à responsabilidade civil, à proteção de dados pessoais e aos direitos fundamentais. De acordo com Gil (2022), a pesquisa bibliográfica é elaborada com base em materiais já publicados e permite ao pesquisador conhecer e analisar diferentes contribuições existentes sobre determinado problema. Dessa maneira, o levantamento das fontes possibilitou construir uma base teórica consistente para a compreensão do tema estudado.

Além das produções acadêmicas, foram examinados documentos jurídicos e institucionais relacionados à regulamentação e ao uso responsável da inteligência artificial. Entre os documentos analisados estiveram a Constituição Federal de 1988, o Código Civil, o Código de Defesa do Consumidor, a Lei Geral de Proteção de Dados Pessoais, a Emenda Constitucional nº 115/2022 e o Projeto de Lei nº 2.338/2023. Também foram considerados documentos internacionais, como o Regulamento Europeu de Inteligência Artificial e a Recomendação da UNESCO sobre a Ética da Inteligência Artificial.

A seleção dos materiais ocorreu de acordo com sua relação direta com o problema e os objetivos da pesquisa. Para a localização das produções, foram utilizados descritores como “inteligência artificial”, “responsabilidade jurídica”, “direitos fundamentais”, “responsabilidade civil”, “proteção de dados”, “decisões automatizadas” e “discriminação algorítmica”. Foram priorizadas publicações recentes, documentos oficiais e estudos que apresentassem fundamentação jurídica consistente, sendo excluídos os materiais repetidos ou que não contribuíam diretamente para a análise proposta.

A análise das informações ocorreu por meio de leitura exploratória, seletiva, analítica e interpretativa. Segundo Marconi e Lakatos (2021), a pesquisa científica exige procedimentos sistemáticos de levantamento, organização e interpretação das informações, permitindo que os dados encontrados contribuam para responder ao problema investigado. A partir dessa orientação, os conteúdos selecionados foram organizados em três eixos principais: proteção dos direitos fundamentais, responsabilidade jurídica pelos danos algorítmicos e mecanismos de regulação, governança e prevenção.

Por fim, as informações foram analisadas de forma crítica e articuladas com as normas jurídicas aplicáveis ao tema. A pesquisa não envolveu participantes, entrevistas, questionários ou coleta de dados em campo, uma vez que se concentrou exclusivamente em fontes bibliográficas e documentais de acesso público. O percurso metodológico adotado permitiu compreender os principais desafios jurídicos relacionados à inteligência artificial e identificar caminhos para a prevenção de danos, a responsabilização dos agentes envolvidos e a proteção efetiva dos direitos fundamentais.

RESULTADOS E DISCUSSÃO

A análise das fontes bibliográficas e documentais demonstrou que a inteligência artificial

vem modificando a maneira como decisões são produzidas em diferentes setores da sociedade. Os sistemas automatizados podem ampliar a eficiência, reduzir tarefas repetitivas e apoiar atividades complexas, mas também podem provocar danos materiais, morais e coletivos quando utilizados sem critérios adequados de segurança e supervisão. Os resultados indicaram que os riscos da inteligência artificial não se limitam a falhas técnicas, pois envolvem privacidade, discriminação, liberdade, igualdade, reputação e acesso a serviços essenciais. Estudo publicado pela Organização para a Cooperação e Desenvolvimento Econômico identificou incidentes relacionados a conteúdos sintéticos, segurança infantil, ataques cibernéticos, privacidade e saúde, confirmando que os impactos da tecnologia já alcançam diferentes dimensões da vida social (OECD, 2026).

Um dos principais resultados encontrados refere-se à relação entre inteligência artificial e proteção de dados pessoais. Muitos sistemas dependem da coleta e do processamento de grandes volumes de informações para treinamento, classificação de perfis e produção de recomendações. Entretanto, a existência de dados disponíveis em plataformas digitais não significa que possam ser utilizados livremente para qualquer finalidade. A Lei Geral de Proteção de Dados Pessoais exige que o tratamento observe princípios como finalidade, adequação, necessidade, transparência, segurança, prevenção e não discriminação. Dessa forma, empresas e instituições devem demonstrar a legitimidade do uso dos dados, limitar a coleta ao necessário e informar de maneira compreensível como as informações serão utilizadas (Brasil, 2018).

A atuação da Autoridade Nacional de Proteção de Dados evidencia que os conflitos relacionados à inteligência artificial já ultrapassaram o campo teórico. Em 2024, a ANPD determinou a suspensão cautelar do tratamento de dados pessoais realizado pela Meta para treinamento de sistemas de inteligência artificial, considerando, entre outros aspectos, a ausência de informações suficientes para que os titulares compreendessem as consequências desse tratamento. Posteriormente, a retomada ocorreu com restrições e exigências de maior transparência. O caso demonstrou que a inovação tecnológica não afasta a obrigação de respeitar os direitos dos titulares e de fornecer mecanismos acessíveis de oposição ao uso de seus dados (ANPD, 2024).

Outro aspecto relevante está relacionado às decisões automatizadas que afetam interesses individuais. O artigo 20 da LGPD assegura ao titular o direito de solicitar a revisão de decisões tomadas unicamente com base no tratamento automatizado de dados pessoais, especialmente quando envolvem perfis profissionais, pessoais, de consumo ou de crédito. Contudo, a efetividade

desse direito depende de a pessoa saber que foi submetida a uma decisão automatizada e receber informações sobre os critérios utilizados. A própria ANPD tem aprofundado o debate regulatório sobre inteligência artificial e revisão de decisões automatizadas, reconhecendo que a possibilidade de contestação representa uma condição necessária para a proteção da autonomia e do devido processo informacional (Brasil, 2018; ANPD, 2025).

Os resultados também apontaram que os vieses algorítmicos constituem uma das ameaças mais significativas à igualdade. Sistemas de inteligência artificial aprendem a partir de dados históricos que podem conter desigualdades sociais, raciais, econômicas e de gênero. Quando essas distorções não são identificadas durante o desenvolvimento e a avaliação do sistema, a tecnologia pode reproduzir tratamentos discriminatórios em processos de contratação, concessão de crédito, reconhecimento facial e acesso a políticas públicas. Lendvai (2025) considera o viés algorítmico um problema jurídico central da governança da inteligência artificial, pois decisões aparentemente neutras podem produzir efeitos desproporcionais sobre grupos socialmente vulneráveis.

A discussão demonstrou, ainda, que a ausência de intenção discriminatória não elimina a responsabilidade jurídica. Um sistema pode gerar consequências injustas mesmo quando seus desenvolvedores não programaram expressamente uma diferenciação entre grupos. A discriminação pode surgir da escolha das variáveis, da qualidade dos dados, da definição dos objetivos ou da forma como os resultados são utilizados. Por essa razão, a avaliação jurídica não deve se limitar ao código do programa, mas precisa considerar todo o ciclo de vida da tecnologia. A Resolução nº 615/2025 do Conselho Nacional de Justiça determina que as soluções de inteligência artificial observem justiça, equidade, inclusão, não discriminação, explicabilidade, contestabilidade e supervisão humana, reconhecendo que a prevenção dos vieses exige acompanhamento contínuo (CNJ, 2025).

A opacidade dos sistemas apareceu como outro obstáculo à proteção dos direitos fundamentais. Em determinados modelos, mesmo profissionais especializados podem encontrar dificuldades para explicar detalhadamente como uma resposta foi produzida. Entretanto, essa complexidade não pode servir como justificativa para impedir que o indivíduo compreenda os elementos essenciais de uma decisão que o prejudicou. A transparência juridicamente relevante não exige necessariamente a divulgação irrestrita do código-fonte, mas requer informações suficientes sobre a finalidade do sistema, os dados considerados, os critérios gerais utilizados, suas limitações e as possibilidades de contestação. Nesse sentido, o dever de explicação deve ser

proporcional à importância da decisão e à gravidade dos efeitos produzidos sobre a pessoa.

A identificação dos responsáveis pelos danos também se mostrou complexa em razão da quantidade de agentes envolvidos no funcionamento da inteligência artificial. Desenvolvedores, fornecedores, empresas contratantes, operadores, gestores e usuários profissionais podem participar de etapas diferentes do processo. A responsabilidade deve ser analisada considerando quem definiu a finalidade da tecnologia, selecionou os dados, controlou sua aplicação e possuía condições de evitar ou corrigir o dano. A simples afirmação de que o resultado foi produzido pelo algoritmo não rompe o nexo causal nem transforma o sistema em sujeito responsável. A inteligência artificial não possui personalidade jurídica própria, razão pela qual a obrigação de responder permanece vinculada às pessoas físicas ou jurídicas que participam de seu desenvolvimento e utilização.

Nas relações de consumo, os resultados indicaram que o Código de Defesa do Consumidor oferece instrumentos relevantes para a proteção das pessoas afetadas. O fornecedor responde objetivamente pelos danos causados por defeitos de produtos ou serviços, independentemente da comprovação de culpa. Uma ferramenta de inteligência artificial pode ser considerada defeituosa quando não oferece a segurança esperada, apresenta resultados incompatíveis com sua finalidade ou é disponibilizada sem informações adequadas sobre seus riscos e limitações. A responsabilidade também pode decorrer da publicidade que atribui à tecnologia capacidades superiores às que realmente possui. Portanto, as empresas devem evitar apresentar sistemas probabilísticos como ferramentas infalíveis, principalmente quando seus resultados influenciam decisões financeiras, profissionais ou relacionadas à saúde.

No setor público, a utilização da inteligência artificial demanda cautela ainda maior, pois as decisões administrativas podem interferir diretamente no acesso a benefícios, serviços e políticas públicas. A automatização não elimina os deveres de legalidade, motivação, impessoalidade, publicidade e possibilidade de recurso. Quando um sistema classifica incorretamente um cidadão, nega um direito ou direciona fiscalizações de maneira discriminatória, a Administração Pública continua responsável pela decisão. A OECD (2024) reconhece que a inteligência artificial pode aumentar a produtividade e a capacidade de resposta dos governos, mas ressalta que sua utilização precisa estar acompanhada de mecanismos de prestação de contas, avaliação de riscos e proteção dos cidadãos.

No âmbito judicial, verificou-se um avanço mais concreto na construção de regras específicas. A Resolução nº 615/2025 do CNJ estabelece diretrizes para desenvolvimento,

auditoria, monitoramento e uso responsável de soluções de inteligência artificial, exigindo respeito aos direitos fundamentais, supervisão humana, transparência e avaliação proporcional ao impacto do sistema. A norma também impede aplicações incompatíveis com garantias processuais, como aquelas que não permitam revisão humana ou que produzam discriminação abusiva. Em março de 2026, a Resolução nº 674 atualizou parte desse regime, demonstrando que a governança da inteligência artificial precisa ser periodicamente revisada para acompanhar a evolução tecnológica (CNJ, 2025; CNJ, 2026).

A inteligência artificial generativa acrescentou novos desafios à responsabilidade jurídica, sobretudo pela capacidade de produzir textos, imagens, áudios e vídeos que aparentam autenticidade. Esses conteúdos podem ser empregados para difamação, fraude, manipulação política, falsificação da identidade e disseminação de informações incorretas. Além disso, modelos generativos podem apresentar respostas inventadas, imprecisas ou descontextualizadas, criando riscos quando utilizados em áreas que exigem elevado grau de confiabilidade. O perfil de gerenciamento de riscos publicado pelo NIST em 2024 orienta que os riscos da inteligência artificial generativa sejam avaliados durante todo o ciclo de vida do sistema, desde a concepção e o treinamento até o monitoramento de sua utilização (AUTIO et al., 2024).

Diante desses riscos, a pesquisa demonstrou que a responsabilização posterior, embora necessária, não é suficiente para proteger os direitos fundamentais. Certos danos causados por inteligência artificial podem atingir milhares de pessoas em pouco tempo e produzir consequências difíceis de reverter. Por isso, a governança preventiva deve incluir avaliação de impacto algorítmico, testes de segurança, documentação das decisões técnicas, definição clara das responsabilidades, registro de incidentes, auditorias independentes e canais de reclamação. Também é necessário capacitar os profissionais que utilizam a tecnologia, pois a supervisão humana somente será efetiva quando o responsável tiver conhecimento e autonomia para questionar o resultado apresentado pelo sistema.

A abordagem baseada em riscos adotada pelo Regulamento Europeu de Inteligência Artificial oferece uma referência importante para esse modelo preventivo. O regulamento estabelece obrigações proporcionais ao potencial de dano das aplicações, diferenciando sistemas de risco limitado, alto risco e práticas consideradas incompatíveis com os valores da União Europeia. Para aplicações de alto risco, são previstos requisitos relacionados à governança dos dados, documentação técnica, registros de funcionamento, transparência, supervisão humana, precisão e segurança. Esse modelo evidencia que o nível de controle jurídico deve aumentar

conforme a possibilidade de a tecnologia afetar a saúde, a segurança e os direitos fundamentais (União Europeia, 2024).

No Brasil, observou-se que ainda não existe uma lei geral de inteligência artificial plenamente aprovada e vigente. O Projeto de Lei nº 2.338/2023 propõe uma regulamentação fundamentada na centralidade da pessoa humana, na classificação dos sistemas conforme o risco e na definição de direitos e obrigações para os agentes envolvidos. Em 4 de agosto de 2026, a proposta permanecia aguardando parecer do relator na comissão especial da Câmara dos Deputados. Essa situação mostra que o país ainda depende da aplicação conjunta da Constituição Federal, da LGPD, do Código Civil, do Código de Defesa do Consumidor e de normas setoriais. Embora esse conjunto normativo permita enfrentar diversas violações, uma legislação geral pode reduzir incertezas e estabelecer deveres preventivos mais específicos (Brasil, 2023).

Em síntese, os resultados confirmaram que a responsabilidade jurídica relacionada à inteligência artificial deve ser compreendida de forma ampla, abrangendo prevenção, transparência, supervisão, contestação e reparação. A proteção dos direitos fundamentais não depende apenas de descobrir quem deve pagar pelo dano depois que ele ocorre, mas de identificar quem tinha o dever e a capacidade de evitá-lo. A inovação responsável exige que os agentes mantenham registros, avaliem impactos, corrijam vieses e informem claramente as pessoas afetadas. Dessa maneira, a inteligência artificial poderá contribuir para o desenvolvimento social sem transformar sua complexidade em um espaço de ausência de controle, impunidade ou redução das garantias asseguradas pelo Estado Democrático de Direito.

CONSIDERAÇÕES FINAIS

A análise desenvolvida ao longo deste artigo permitiu compreender que a inteligência artificial representa uma importante ferramenta de inovação, mas também cria desafios jurídicos que não podem ser ignorados. Sua utilização em decisões que afetam a vida das pessoas exige cuidado, responsabilidade e respeito aos direitos fundamentais. Assim, a tecnologia não deve ser vista apenas pela capacidade de gerar rapidez e eficiência, mas também pelos impactos que pode produzir sobre a dignidade humana, a privacidade, a igualdade, a liberdade e a segurança.

O objetivo de analisar os principais desafios relacionados à responsabilidade jurídica no uso da inteligência artificial foi alcançado, uma vez que o estudo evidenciou as dificuldades existentes na identificação dos agentes responsáveis, na comprovação do nexo causal e na

reparação dos danos causados por decisões automatizadas. A participação de desenvolvedores, fornecedores, empresas, plataformas e instituições públicas torna a cadeia de responsabilidades mais complexa, mas não pode servir como justificativa para impedir que a vítima tenha acesso à reparação adequada.

Também foi possível perceber que a proteção dos direitos fundamentais não deve acontecer somente depois da ocorrência do dano. A prevenção precisa ocupar um lugar central na utilização da inteligência artificial, por meio de avaliações de risco, transparência, supervisão humana, controle dos dados, correção de vieses e criação de mecanismos de contestação. Quanto maior for o impacto de uma decisão automatizada sobre a vida de uma pessoa, maior deverá ser o nível de cuidado, fiscalização e responsabilidade dos agentes envolvidos.

Embora o ordenamento jurídico brasileiro já possua normas capazes de oferecer proteção em diferentes situações, ainda existem lacunas relacionadas às características específicas da inteligência artificial. Por isso, a construção de uma legislação própria e atualizada mostra-se necessária para estabelecer deveres mais claros, fortalecer a segurança jurídica e garantir uma atuação preventiva. Essa regulamentação, entretanto, deve equilibrar o incentivo à inovação com a proteção da pessoa humana, evitando tanto a ausência de controle quanto a criação de obstáculos desnecessários ao desenvolvimento tecnológico.

Conclui-se, portanto, que a inteligência artificial deve permanecer como um instrumento a serviço da sociedade e não como uma justificativa para a redução de direitos ou para a ausência de responsabilização. O avanço tecnológico somente poderá ser considerado verdadeiramente positivo quando estiver acompanhado de ética, transparência, controle humano e compromisso com a justiça. Dessa forma, a responsabilidade jurídica torna-se essencial para assegurar que a inovação aconteça de maneira segura, democrática e compatível com os valores fundamentais do Estado de Direito.

REFERÊNCIAS

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **ANPD determina suspensão cautelar do tratamento de dados pessoais para treinamento da IA da Meta**. Brasília, DF: ANPD, 2024.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **ANPD apresenta resultados da Tomada de Subsídios sobre Inteligência Artificial e Revisão de Decisões Automatizadas**. Brasília, DF: ANPD, 2025.

AUTIO, Chloe et al. **Artificial Intelligence Risk Management Framework: Generative**

Artificial Intelligence Profile. Gaithersburg: National Institute of Standards and Technology, 2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, 1988.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Dispõe sobre a proteção do consumidor e dá outras providências.** Brasília, DF: Presidência da República, 1990.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. **Institui o Código Civil.** Brasília, DF: Presidência da República, 2002.

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

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

BRASIL. Senado Federal. Projeto de Lei nº 2.338, de 2023. **Dispõe sobre o uso da inteligência artificial.** Brasília, DF: Senado Federal, 2023.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). Resolução nº 615, de 11 de março de 2025. **Estabelece diretrizes para o desenvolvimento, a utilização e a governança de soluções desenvolvidas com recursos de inteligência artificial no Poder Judiciário.** Brasília, DF: CNJ, 2025.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). Resolução nº 674, de 25 de março de 2026. **Altera a Resolução CNJ nº 615/2025, que estabelece diretrizes para o desenvolvimento, a utilização e a governança de soluções de inteligência artificial no Poder Judiciário.** Brasília, DF: CNJ, 2026.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** 7. ed. São Paulo: Atlas, 2022.

LENDVAI, Gergely Ferenc; GOSZTONYI, Gergely. **Algorithmic bias as a core legal dilemma in the age of artificial intelligence: conceptual basis and the current state of regulation.** Laws, Basel, v. 14, n. 3, art. 41, 2025.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica.** 9. ed. São Paulo: Atlas, 2021.

OECD. **Governing with artificial intelligence: are governments ready?** Paris: OECD Publishing, 2024.

OECD. **Trends in AI incidents and hazards reported by the media.** Paris: OECD Publishing, 2026.

OHCHR. **The right to privacy in the digital age: report of the United Nations High**

Commissioner for Human Rights. Geneva: United Nations, 2021.

UNESCO. **Recommendation on the ethics of artificial intelligence.** Paris: UNESCO, 2021.

UNIÃO EUROPEIA. **Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024.** Estabelece regras harmonizadas em matéria de inteligência artificial. Luxemburgo: Jornal Oficial da União Europeia, 2024.