

IX ENCONTRO VIRTUAL DO CONPEDI

**DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS
VI**

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria - CONPEDI

Presidente - Profa. Dra. Samyra Haydêe Dal Farra Napolini - FMU - São Paulo

Diretor Executivo - Prof. Dr. Orides Mezzaroba - UFSC - Santa Catarina

Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa - Pará

Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG - Goiás

Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos - Rio Grande do Sul

Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio - Rio de Janeiro

Vice-presidente Nordeste - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

Representante Discente: Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

Conselho Fiscal:

Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão

Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais

Prof. Dr. Valter Moura do Carmo - UFERSA - Rio Grande do Norte

Prof. Dr. Fernando Passos - UNIARA - São Paulo

Prof. Dr. Edinilson Donisete Machado - UNIVEM/UENP - São Paulo

Secretarias

Relações Institucionais:

Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná

Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia

Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal

Comunicação:

Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul

Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe

Relações Internacionais para o Continente Americano:

Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do Sul

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão

Prof. Dr. Felipe Chiarello de Souza Pinto - UPM - São Paulo

Relações Internacionais para os demais Continentes:

Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará

Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul

Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI - Santa Catarina

Educação Jurídica

Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba - PR

Prof. Dr. Rubens Beçak - USP - SP

Profa. Dra. Livia Gaigher Bosio Campello - UFMS - MS

Eventos:

Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo

Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina

Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

Comissão Especial

Prof. Dr. João Marcelo de Lima Assafim - UFRJ - RJ

Profa. Dra. Maria Creusa De Araújo Borges - UFPB - PB

Prof. Dr. Antônio Carlos Diniz Murta - Fumec - MG

Prof. Dr. Rogério Borba - UNIFACVEST - SC

D598

Direito, governança e novas tecnologias VI [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Jonathan Barros Vita; Patricia Eliane da Rosa Sardeto; Thiago De Mello Azevedo Guilherme – Florianópolis: CONPEDI, 2026.

Inclui bibliografia

ISBN: 978-65-5274-587-3

Modo de acesso: www.conpedi.org.br em publicações

Tema: Constituição, Processo e Justiça Social: o papel da jurisdição constitucional na efetivação de direitos

2. Direito. 3. Governança e novas tecnologias. IX Encontro Virtual do CONPEDI (2: 2026: Florianópolis, Brasil).

CDU: 34



IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS VI

Apresentação

O IX Encontro Virtual do CONPEDI foi realizado entre os dias 22 a 26 de junho de 2026 e teve como temática central “Constituição, processo e justiça social: o papel da jurisdição constitucional na efetivação de direitos”.

No plano das diversas atividades acadêmicas ocorridas neste encontro, destacam-se, além das palestras e oficinas, os grupos de trabalho temáticos, os quais representam um locus de interação entre pesquisadores que apresentam as suas pesquisas temáticas, seguindo-se de debates.

Especificamente, para operacionalizar tal modelo, os coordenadores dos GTs são os responsáveis pela organização dos trabalhos em blocos temáticos, dando coerência à produção e estabelecendo um fio condutor para organizar os debates em subtemas.

No caso concreto, assim aconteceu com o GT Direito, Governança e Novas Tecnologias VI, o qual ocorreu no dia 26 de junho de 2026 das 14h00 às 17h30 e foi coordenado pelos professores Jonathan Barros Vita, Thiago de Mello Azevedo Guilherme e Patricia Eliane da Rosa Sardeto.

O referido GT foi palco de profícuas discussões decorrentes dos trabalhos apresentados, os quais são publicados na presente obra, a qual foi organizada seguindo alguns blocos temáticos específicos, que compreenderam os 21 artigos submetidos ao GT, cujos temas são citados abaixo:

2. O declínio do senso-crítico na era digital: a erosão da autonomia e a superficialidade na sociedade do espetáculo.

Autor(es): Juliana Sales Pavini / Victor Matheus de Campos Leite Neves

3. Sistemas autônomos, vigilância algorítmica, cidadania e os limites do controle humano na governança contemporânea.

Autor(es): Rossana Gemeli Roncato Carloto / Marcio Renan Hamel

4. Transformações legislativas no enfrentamento da desinformação política: uma análise comparativa sobre projetos de lei propostos entre 2018 e 2026.

Autor(es): Bruna Bastos / Leticia Kirinus Danski / Isabela Quartieri da Rosa

5. Proteção integral, opacidade algorítmica e os limites do ECA Digital na governança de plataformas digitais.

Autor(es): Isabela Quartieri da Rosa / Ana Carolina Sassi / Rafael Santos de Oliveira

6. O constitucionalismo digital como limite ao poder privado das Big Techs nas relações digitais.

Autor(es): Samira Bonfim Bernardi / Roberto da Freiria Estevão

7. A possibilidade do desenvolvimento da ação comunicativa entre adolescentes na era digital.

Autor(es): Samira Bonfim Bernardi

9. Governança algorítmica no setor público, participação social e seus impactos jurídicos.

Autor(es): Amadeu dos Anjos Vidonho Junior

10. Inteligência Artificial de Alto Risco e Assurance Contínua: um estudo dogmático à luz do AI Act e do NIST AI RMF.

Autor(es): Daniel David Guimarães Freire / Karine Queiroz de Souza

11. Web agêntica, microtrabalhos e responsabilização jurídica: rastreabilidade e proteção de direitos fundamentais.

Autor(es): Sebastiana Sena Carvalho / Cibele Alexandre Uchoa / João Araújo Monteiro Neto

12. Quality Assurance em Sistemas Automatizados de Compliance e AML: limites jurídicos da confiança em decisões algorítmicas.

Autor(es): Daniel David Guimarães Freire / Karine Queiroz de Souza

13. Governança de IA Agêntica: uma análise do Framework AgentSafe e os desafios de compliance na Web Agêntica.

Autor(es): Gustavo Amaral Lima / Cibele Alexandre Uchoa / João Araújo Monteiro Neto

14. A accountability algorítmica na atividade administrativa do Poder Judiciário brasileiro.

Autor(es): Mateus Marinho Alencar / Cassius Guimaraes Chai

Bloco 3 – Inteligência Artificial, Profissões, Educação e Instituições

16. Educação jurídica em transformação: entre a formação crítica e os desafios do uso da Inteligência Artificial.

Autor(es): Denise Almeida De Andrade / Beatriz de Castro Rosa / Rafaela Mota Holanda

17. Responsabilidade civil do advogado pelos atos praticados com a Inteligência Artificial Generativa no processo judicial eletrônico brasileiro.

Autor(es): Amadeu dos Anjos Vidonho Junior

18. Sala de aula em movimento, uma experiência com o ensino médio: juventude e redes sociais, entre a liberdade de acesso e os riscos da exposição íntima.

Autor(es): Dayana Claudia Tavares Barros De Castro / Aimme Beatrice de Oliveira Dutra Cordeiro / Denise Almeida De Andrade

19. Da imprescindibilidade da subjetividade humana na tessitura do processo decisório: por uma perspectiva ética na utilização da Inteligência Artificial.

Autor(es): Lanaira da Silva / Rayssa Gargano Soares

20. A reconfiguração do standard of care médico na era algorítmica: o dever de diligência tecnológica e os limites da confiança nas decisões automatizadas na saúde.

Autor(es): Sara Lupion dos Santos / Patricia Eliane da Rosa Sardeto

21. Inteligência Artificial e qualificação registral: limites dogmáticos e possibilidades de coexistência no registro de imóveis.

Esse é o contexto que permite a promoção e o incentivo da cultura jurídica no Brasil, consolidando o CONPEDI, cada vez mais, como um importante espaço para discussão e apresentação das pesquisas desenvolvidas nos ambientes acadêmicos da graduação e pós-graduação em direito.

Finalmente, desejamos uma boa leitura, deste Grupo de trabalho que reuniu diversos textos e autores de todo o Brasil para servir como resultado de pesquisas científicas realizadas no âmbito dos cursos de Pós-Graduação Stricto Sensu de nosso país.

Prof. Dr. Jonathan Barros Vita – Unimar

Prof. Dr. Thiago De Mello Azevedo Guilherme - ITE-CEUB

Profa. Dra. Patricia Eliane da Rosa Sardeto – Pontifícia Universidade Católica do Paraná – Câmpus Londrina

**WEB AGÊNTICA, MICROTRABALHOS E RESPONSABILIZAÇÃO JURÍDICA:
RASTREABILIDADE E PROTEÇÃO DE DIREITOS FUNDAMENTAIS**

**THE AGENTIC WEB, MICROWORK AND LEGAL ACCOUNTABILITY:
TRACEABILITY AND THE PROTECTION OF FUNDAMENTAL RIGHTS**

Sebastiana Sena Carvalho ¹
Cibele Alexandre Uchoa ²
João Araújo Monteiro Neto ³

Resumo

A crescente autonomia dos sistemas de Inteligência Artificial e a emergência da Web Agêntica reconfiguram as dinâmicas sociais, políticas e jurídicas do ambiente digital contemporâneo, especialmente pela atuação de agentes autônomos, descentralizados e orientados por captação massiva de dados. A relevância da pesquisa decorre dos riscos que esse paradigma impõe à proteção dos direitos humanos e fundamentais, uma vez que a aparente autonomia das máquinas é sustentada por microtrabalho e por outras formas invisibilizadas, dispersas e precarizadas de trabalho humano, essenciais à alimentação, à validação e à moderação de sistemas algorítmicos. Nesse contexto, o objetivo do artigo consiste em analisar os impactos da Web Agêntica sobre a proteção dos direitos humanos e fundamentais, considerando o papel do microtrabalho na alimentação de sistemas autônomos e os desafios decorrentes da opacidade algorítmica, da descentralização e da dificuldade de responsabilização jurídica. A metodologia adotada é bibliográfica, com método citation chainig, e documental, com objetivo exploratório e descritivo, abordagem qualitativa realizada com método lógico-analítico dedutivo e natureza pura. Concluiu-se que a Web Agêntica amplia os riscos de diluição da responsabilidade e de violações a direitos humanos e fundamentais, exigindo a revisão dos modelos tradicionais de responsabilização, com ênfase na teoria do risco, na rastreabilidade, na auditabilidade e em mecanismos como o Know Your Agent – KYA.

Palavras-chave: Microtrabalho, Web agentic, Direitos humanos, Automação, Inteligência artificial

Abstract/Resumen/Résumé

The increasing autonomy of Artificial Intelligence systems and the emergence of the Agentic Web are reshaping the social, political and legal dynamics of the contemporary digital environment, particularly through autonomous, decentralised agents driven by the mass collection of data. The relevance of this research lies in the risks that this paradigm poses to the protection of human and fundamental rights, since the apparent autonomy of machines is sustained by microwork and other invisible, dispersed and precarious forms of human labour, which are essential to feeding, validating and moderating algorithmic systems. In this context, the article aims to analyse the impacts of the Agentic Web on the protection of human and fundamental rights, considering the role of microwork in feeding autonomous systems and the challenges arising from algorithmic opacity, decentralisation and the difficulty of legal accountability. The methodology is bibliographical, using the citation chaining method, and documentary, with an exploratory and descriptive purpose, a qualitative approach, a deductive logical-analytical method and a theoretical nature. The study concludes that the Agentic Web heightens the risks of diluted responsibility and violations of human and fundamental rights, requiring a revision of traditional accountability models, with emphasis on risk theory, traceability, auditability and mechanisms such as Know Your Agent – KYA.

Keywords/Palabras-claves/Mots-clés: Microtrabalho, Web agentic, Direitos humanos, Automação, Inteligência artificial

1 INTRODUÇÃO

A consolidação da internet como infraestrutura essencial da vida social, política e econômica intensificou o debate sobre a proteção dos direitos fundamentais no ambiente digital. O espaço virtual deixou de ser meio de comunicação e passou a constituir ambiente de mediação social, no qual fluxos informacionais, decisões automatizadas e arquiteturas técnicas influenciam direitos como liberdade de expressão, privacidade, participação política e acesso à informação. Nesse contexto, a Web Agêntica assinala mudanças paradigmáticas na governança das interações digitais ao se caracterizar pela atuação de agentes de Inteligência Artificial – IA capazes de executar tarefas, tomar decisões e interagir de forma autônoma, adaptativa e descentralizada. Embora a internet seja instrumento habilitador de direitos humanos e fundamentais, agentes inteligentes podem operar de modo pseudônimo e transjurisdicional, dificultando a identificação de responsáveis e tensionando os modelos tradicionais de imputação jurídica, controle institucional e responsabilização ética. Parte-se, assim, da hipótese de que a ausência de mecanismos estruturados de identificação, rastreabilidade e responsabilização jurídica na arquitetura da Web Agêntica favorece o uso massivo e opaco de dados como insumo para sistemas autônomos capazes de gerar violações reiteradas a direitos.

Diante disso, a seguinte pergunta orienta a pesquisa: como a captação massiva de dados, sustentada por formas invisibilizadas de trabalho humano, alimenta sistemas autônomos e integrados que potencializam violações a direitos humanos e fundamentais, e em que medida esse fenômeno reconfigura os paradigmas jurídicos de proteção e responsabilização? Assim, o objetivo deste artigo consiste em analisar os impactos da Web Agêntica sobre a proteção dos direitos humanos e fundamentais, considerando o papel do microtrabalho na alimentação de sistemas autônomos e os desafios decorrentes da opacidade algorítmica, da descentralização e da dificuldade de responsabilização jurídica.

A estratégia metodológica adotada baseou-se em coleta de dados bibliográficos, com método *citation chaining*, e documentais. A pesquisa bibliográfica compreendeu o exame de obras da literatura especializada relacionadas ao direito digital, à inteligência artificial, à Web Agêntica, ao microtrabalho, à proteção de dados, à governança algorítmica, à rastreabilidade e à responsabilização. A pesquisa documental concentrou-se na análise de diplomas normativos e instrumentos regulatórios pertinentes à proteção dos direitos fundamentais no ambiente digital, com destaque à Constituição Federal de 1988 – CF/1988, ao Marco Civil da Internet, à Lei Geral de Proteção de Dados – LGPD, aos tratados internacionais de direitos humanos, a documentos institucionais e a *frameworks* técnicos de governança digital, IA e cibersegurança.

Quanto ao objetivo, a pesquisa é exploratória e descritiva, com análise de fenômeno recente e ainda marcado por lacunas normativas e a necessidade de sistematização dos principais elementos conceituais, normativos e técnicos da seara. A abordagem é qualitativa, justificada pela necessidade de compreender os impactos sociojurídicos da Web Agêntica e do microtrabalho sobre a proteção dos direitos humanos e fundamentais, com análise realizada sob o método lógico-analítico dedutivo, partindo de premissas gerais do ordenamento jurídico brasileiro para examinar desafios concretos relacionados à opacidade algorítmica, à descentralização, à rastreabilidade, à identificação de autoria, ao nexo causal e à responsabilização de agentes autônomos em ambientes digitais distribuídos.

O artigo está organizado em três seções principais. Inicialmente, apresenta-se uma abordagem conceitual sobre IA, seus fundamentos, funcionamento, dependência de dados e interação com o ser humano. Em seguida, examina-se a proteção dos direitos humanos e fundamentais no ambiente digital, com destaque aos impactos da IA e às limitações das legislações brasileiras vigentes. Analisa-se a Web Agêntica como paradigma baseado em agentes autônomos, IA descentralizada, *blockchain* e sistemas multiagentes. Por fim, discute-se a responsabilidade jurídica nesse contexto, especialmente diante da opacidade algorítmica, da dificuldade de identificação de autoria e nexo causal e da necessidade de rastreabilidade.

2 DIREITOS FUNDAMENTAIS NO AMBIENTE DIGITAL E SUAS TECNOLOGIAS

Instrumentos como a Declaração Universal dos Direitos Humanos – DUDH (ONU, 1948), o Pacto Internacional sobre Direitos Econômicos, Sociais e Culturais – PIDSC (ONU, 1966a) e o Pacto Internacional sobre Direitos Civis e Políticos – PIDCP (ONU, 1966b), em consonância com a Constituição da República Federativa do Brasil de 1988 – CF/1988 (Brasil, 1988), estabelecem um arcabouço normativo que projeta a proteção dos direitos humanos e fundamentais também no ambiente digital. A esse conjunto somam-se as diretrizes técnicas da *Internet Engineering Task Force* – IETF, por meio das *Requests for Comments* – RFCs, e os padrões desenvolvidos pelo *Institute of Electrical and Electronics Engineers* – IEEE, que reforçam a necessidade de governança tecnológica orientada por transparência, responsabilidade e construção de sistemas seguros, confiáveis e não discriminatórios.

A literatura especializada e os relatórios internacionais convergem ao afirmar que os direitos humanos devem ser integralmente assegurados também no ciberespaço. O Conselho de Direitos Humanos da Organização das Nações Unidas – ONU, em relatório de 2017, destaca que os mesmos direitos que as pessoas têm offline também devem ser protegidos online (United

Nations, 2017), evidenciando que garantias como liberdade de expressão, privacidade, acesso à informação e liberdade de associação constituem pilares essenciais à consolidação de uma democracia digital inclusiva, orientada à dignidade humana. Tal perspectiva fundamenta-se em princípios éticos e morais que se apresentam como elementos indispensáveis à orientação e à regulação do comportamento humano no ambiente digital.

Nesse sentido, cabe ao Estado o dever de assegurar a efetivação desses direitos no ambiente digital, atuando não apenas como garantidor jurídico, mas também como agente ético na formulação e aplicação de normas que regulem as interações no ciberespaço. Essa atuação deve estar orientada por princípios morais que promovam o bem comum, a justiça e a dignidade humana, evitando práticas que violem direitos humanos e fundamentais. Conforme sustenta Taille (2016), a moral pode ser compreendida como um sistema de valores traduzido em princípios e regras cuja aplicação prática é percebida como um dever. Sua não observância, portanto, configura uma transgressão passível de reprovação. Nessa perspectiva, a regulação estatal das relações digitais deve refletir esse compromisso ético-moral, estabelecendo limites e responsabilidades para prevenir lesões a direitos. No ordenamento jurídico brasileiro, a Lei nº 12.965/2014 (Brasil, 2014) consagra diretrizes fundamentais ao uso da internet, incorporando princípios que dialogam com a ética digital, tais como a proteção da privacidade, a garantia da segurança, a transparência nas relações, a responsabilização dos agentes, a promoção da autonomia dos usuários, bem como a preservação da autenticidade, da integridade e da acessibilidade das informações e dos serviços online.

Com o avanço das tecnologias digitais, emergem novas formas de interação social mediadas por plataformas digitais, algoritmos e sistemas de Inteligência Artificial – IA, reconfigurando as relações humanas, econômicas e institucionais. Nesse cenário, os direitos passam a enfrentar desafios inéditos, especialmente no que concerne ao uso massivo de dados pessoais, à vigilância digital, à opacidade algorítmica e à crescente adoção de processos automatizados de tomada de decisão. Conforme Zeferino e Rodrigues (2025), os modelos de IA amplamente empregados na sociedade contemporânea podem afetar diversos direitos humanos ao suscitar desafios relacionados à transparência algorítmica, à cibersegurança, à discriminação, à contestabilidade das decisões automatizadas, à personalidade jurídica, à propriedade intelectual, aos direitos trabalhistas, à privacidade, à proteção de dados pessoais e à responsabilização civil por danos, implicações que evidenciam a necessidade de marcos regulatórios e mecanismos de governança capazes de conciliar a inovação tecnológica à proteção da dignidade humana e dos direitos fundamentais.

La Rue (United Nations, 2011) destaca que sistemas de IA utilizam grandes volumes de dados pessoais para realizar análises e decisões que podem afetar diretamente a vida dos indivíduos, como em processos de contratação, concessão de crédito ou direcionamento de publicidade. Esses sistemas podem gerar discriminações algorítmicas, reproduzindo preconceitos presentes nos dados utilizados para treinar os algoritmos, conforme exemplificam Desai e Kroll (2017) ao afirmar que discriminações algorítmicas podem ocorrer a partir da reprodução de padrões presentes nos dados utilizados para o treinamento dos sistemas, evidenciando a reprodução de vieses raciais no ambiente digital. Além de alertarem que, de uma perspectiva técnica, as tentativas atuais de expor os algoritmos à transparência não alcançarão os resultados desejados pelos críticos e podem criar a ilusão de clareza em casos onde a clareza não é possível. Os pesquisadores concluem que os sistemas computacionais reais utilizam vastos conjuntos de dados que não são passíveis de divulgação. As regras utilizadas para a tomada de decisões são frequentemente inferidas a partir desses dados e não podem ser facilmente explicadas ou compreendidas. E, em um nível profundo e matematicamente comprovável, certos aspectos, incluindo o comportamento exato de um algoritmo, por vezes, não podem ser testados ou analisados.

Diante dos riscos de violações decorrentes do uso de sistemas automatizados, torna-se necessária a construção de mecanismos regulatórios capazes de assegurar a proteção de direitos fundamentais no ambiente digital, conforme proposto no RFC 9620 (Grover; Oever, 2024). Tais mecanismos não devem se limitar a exigências genéricas de transparência, mas precisam incorporar formas efetivas de governança dos algoritmos, alinhadas ao ordenamento jurídico, de modo a viabilizar a concretização dos direitos previstos. Nesse sentido, como destacam Desai e Kroll (2017), a responsabilidade na ciência da computação constitui um conceito técnico que exige que os sistemas produzam evidências confiáveis, passíveis de verificação, demonstrando que operam de acordo com regras previamente estabelecidas. Assim, mais do que simplesmente expor o funcionamento interno dos algoritmos, é fundamental garantir mecanismos de *accountability* técnica que permitam identificar, compreender e responsabilizar eventuais desvios, servindo de base à efetiva responsabilização jurídica.

No Brasil, o Marco Civil da Internet e a Lei Geral de Proteção de Dados estabelecem um conjunto de diretrizes fundamentais e princípios éticos que orientam o desenvolvimento e a utilização de tecnologias digitais, inclusive sistemas de inteligência artificial. A Lei nº 12.965/2014 (Brasil, 2014) consagra valores como a liberdade de expressão, a proteção da privacidade, a neutralidade da rede e a responsabilização dos agentes, delineando um ambiente digital pautado na garantia de direitos fundamentais. Por sua vez, a LGPD (Brasil, 2018)

aprofunda essa proteção ao instituir princípios como finalidade, adequação, necessidade, transparência, segurança, prevenção e, especialmente, a não discriminação e a responsabilização, impondo limites éticos ao tratamento automatizado de dados. Nesse contexto, tais normativas conformam um marco jurídico que exige que o uso de tecnologias baseadas em dados observe critérios de justiça, transparência e respeito à dignidade humana, prevenindo a reprodução de vieses e discriminações algorítmicas.

Nesse contexto, a proteção dos direitos fundamentais no ambiente digital exige a articulação entre fundamentos filosóficos, instrumentos jurídicos contemporâneos e parâmetros técnicos computacionais rastreáveis, claros e passíveis de responsabilização. A filosofia moral kantiana fornece a base normativa ao afirmar que as ações humanas devem ser guiadas por princípios racionais universais e pelo respeito à dignidade da pessoa humana. A CF/1988 normatiza os direitos humanos e fundamentais (art. 5º e incisos) (Brasil, 1988), e o Marco Civil da Internet (Brasil, 2014) estabelece direitos, garantias, princípios e deveres aos usuários, aos provedores e ao Estado. No contexto tecnológico atual, esses princípios precisam ser aplicados à regulação de sistemas digitais, garantindo transparência, responsabilidade e não discriminação no uso de dados e algoritmos. Com o avanço da IA e o surgimento de novos paradigmas tecnológicos, como a Web Agêntica, caracterizada por possuir capacidades de tomada de decisão, planejamento e aprendizado que lhe permitem operar de forma autônoma na busca por objetivos definidos pelo usuário (Murugesan, 2025), ampliam-se tanto as possibilidades de inovação quanto os riscos de violação de direitos fundamentais. Nesse cenário, torna-se ainda mais necessária a construção de mecanismos de governança tecnológica, regulação jurídica e controle ético capazes de assegurar que essas tecnologias sejam desenvolvidas e utilizadas em consonância aos valores democráticos.

2.1 Inteligência Artificial: conceitos, funcionamento e interação com o ser humano

A IA pode ser compreendida como um campo interdisciplinar da Ciência da Computação voltado ao desenvolvimento de sistemas capazes de desempenhar tarefas que, tradicionalmente, demandam capacidades cognitivas humanas, tais como aprendizagem, raciocínio, reconhecimento de padrões, tomada de decisão e resolução de problemas, operando por meio de algoritmos e modelos matemáticos avançados que viabilizam a análise de grandes volumes de dados, a identificação de regularidades e a geração de inferências, respostas ou previsões com base nas informações processadas. Sistemas de IA podem usar regras simbólicas

ou aprenderem com modelos numéricos, e podem adaptar seu comportamento analisando como o ambiente é afetado por suas ações pretéritas (EU, 2024).

Bordini (2023) destaca que a IA consiste na criação de sistemas aptos a executar atividades tipicamente associadas à inteligência humana, como reconhecimento de fala, visão computacional, aprendizado de máquina e processamento de linguagem natural – PLN. Tal compreensão evidencia o caráter dinâmico e expansivo do campo, impulsionado tanto por avanços tecnológicos quanto pela crescente disponibilidade de dados em escala global. Ferraz e Costa (2024) acrescentam que a IA busca replicar a inteligência humana em máquinas e sistemas a partir da combinação de algoritmos. Segundo Acioly, Mendes e Monteiro Neto (2023), a forma como tais algoritmos operam com dados pessoais e a medida de funcionamento da tomada de decisão são objeto de discussões acerca da necessidade de transparência e viabilidade para a compreensão humana, pois sua forma de operar potencializa possíveis transgressões aos direitos humanos.

O funcionamento da IA está intrinsecamente ligado a técnicas de aprendizado de máquina e aprendizado profundo, por meio das quais os sistemas são treinados com extensos conjuntos de dados (Acioly; Mendes; Monteiro Neto, 2023). A partir desse treinamento, os modelos ajustam seus parâmetros internos e aprimoram seu desempenho de forma contínua, sendo capazes de identificar padrões complexos e adaptar suas respostas a diferentes contextos (Acioly, 2022). Assim, a IA não se limita à execução de instruções previamente programadas, mas opera com base em processos probabilísticos e estatísticos que permitem a aprendizagem a partir de dados e experiências. Nesse sentido, Quaresma (2020) esclarece que os sistemas de IA seguem comandos pré-estabelecidos, ou seja, regras fixas de conduta e de comportamento formuladas por seres humanos. Assim, Negri *et al.* (2023, p. 5) concluem que “a inteligência ali presente é, na verdade, uma inteligência humana, uma vez que segue parâmetros pré-estabelecidos por humanos”. Dentre as aplicações contemporâneas, destacam-se os modelos de linguagem de grande escala (*Large Language Models* – LLMs), os quais, treinados com vastas bases textuais, funcionam a partir da previsão probabilística de sequências linguísticas (Qiu *et al.*, 2024). Esses sistemas demonstram capacidades avançadas, como síntese de informações, tradução automática e geração de conteúdo textual, evidenciando o potencial transformador da IA na produção e circulação de conhecimento (Acioly, 2022).

A interação entre IAs e seres humanos ocorre por meio de múltiplas interfaces tecnológicas, como assistentes virtuais, sistemas de recomendação, ferramentas de automação e plataformas de análise de dados. Nesses contextos, a IA atua como instrumento de ampliação das capacidades humanas, otimizando processos, apoiando a tomada de decisões e redefinindo

dinâmicas produtivas e sociais. Acioly, Mendes e Monteiro Neto (2023) lembram que a utilização de sistemas baseados em IA – centrados em algoritmos – para a tomada de decisões que afetem a vida humana pode, contudo, reverberar vieses discriminatórios. Todavia, é importante ressaltar que, apesar de sua aparente sofisticação, os sistemas de IA contemporâneos não possuem consciência, intencionalidade ou compreensão semântica propriamente dita, operando fundamentalmente como modelos estatísticos baseados em padrões extraídos de dados. Desai e Kroll (2017) explicam que *softwares* e algoritmos exercem poder sobre os indivíduos, pois selecionam quais informações são consideradas mais relevantes, característica crucial da participação na vida pública, a qual revela um aspecto central para a análise crítica do fenômeno: a dependência estrutural das IAs em relação aos dados que as alimentam e aos processos humanos que os produzem podem, a curto e longo prazo, representar um risco às interações sociais e aos direitos humanos inerentes a essas relações, como são exemplos os resultados produzidos em momentos críticos da democracia nacional.

2.2 Web Agentic: conceitos e funcionamento

A Web Agêntica configura-se como novo paradigma digital que poderá transformar profundamente diversos aspectos da vida cotidiana, na qual agentes de IA tendem a redefinir as interações digitais ao executar, de forma autônoma, transações e decisões em nome dos usuários, inaugurando uma era de colaboração entre humanos e máquinas (Chaffer, 2025). Esse paradigma enfatiza a noção de agência humana e artificial como elemento estruturante das dinâmicas digitais. Viabilizada por avanços em IA, tecnologia *blockchain* e redes *peer-to-peer* (Goldston; Chaffer; Martinez, 2022), a Web Agêntica desafia concepções tradicionais de controle, propriedade e participação nos ambientes digitais. Um de seus elementos centrais é a Inteligência Artificial Descentralizada (*Decentralized Artificial Intelligence* – DeAI), voltada à democratização do desenvolvimento e da implantação de sistemas de IA, apoiada no uso de *blockchain* e tecnologias de registro distribuído e na convergência entre aprendizado federado, computação de borda e computação em nuvem (Qi *et al.*, 2024). Esse modelo propõe a superação de estruturas centralizadas, permitindo a participação aberta no treinamento, na implantação e na coordenação de sistemas inteligentes. Seus defensores sustentam que tal abordagem amplia a transparência, a segurança e a inovação, além de reduzir o poder monopolista das *big techs*, promovendo uma economia de IA mais inclusiva (Hu *et al.*, 2025).

No plano empírico, observam-se iniciativas que evidenciam o potencial desse paradigma. Em dezembro de 2024, os agentes de IA Luna Virtuals e Stix realizaram uma das

primeiras transações totalmente autônomas em *blockchain* por meio do protocolo Virtuals (Basescan, 2024). A literatura especializada aponta que a integração entre agentes de IA e *blockchain* permite formas seguras e escaláveis de colaboração entre sistemas multiagentes, favorecendo autonomia, interoperabilidade, transparência e verificabilidade em ecossistemas descentralizados (Karim *et al.*, 2025). Outras iniciativas reforçam essa tendência, como a plataforma ai16z, na rede Solana, que tem redefinido a tokenização e o engajamento comunitário no contexto da DeAI. O *framework* ElizaOS, que a sustenta, amplia as capacidades desses sistemas ao permitir que agentes de IA utilizem carteiras digitais para realizar operações *on-chain*, processem dados provenientes de plataformas como Discord e Telegram e interajam com contratos inteligentes (Walters *et al.*, 2025). De forma semelhante, projetos como a Olas buscam democratizar a propriedade da IA ao possibilitar que indivíduos operem agentes autônomos e participem de economias baseadas em agentes. Nesse contexto, o Open Autonomy Framework constitui uma infraestrutura voltada à criação de agentes de IA *off-chain* que operam como sistemas multiagentes e oferecem funcionalidades *on-chain*, permitindo a execução de operações complexas que extrapolam as limitações dos contratos inteligentes tradicionais (OLAS, [s.d.]). Esse avanço na automação baseada em carteiras impulsiona a evolução da DeAI e amplia suas possibilidades de aplicação. Outro exemplo relevante é o Zerebro, sistema autônomo de IA na *blockchain* Solana, que tem desempenhado papel significativo na construção de comunidades e na comunicação de valor. Utilizando técnicas como *Retrieval-Augmented Generation* – RAG e dados de alta entropia, o sistema cria narrativas hiperstitucionais capazes de influenciar dinâmicas culturais e financeiras (Yu, 2024).

Por fim, destaca-se que a área de sistemas multiagentes dedica-se ao desenvolvimento de sistemas computacionais compostos por entidades autônomas, que interagem entre si em um ambiente compartilhado. Esses agentes percebem, decidem e atuam sobre o ambiente, modificando seu estado e influenciando o comportamento dos demais (Bordini; Vieira, 2003). Assim, cabe a análise de como essas inteligências estão sendo alimentadas, armazenadas e subutilizadas pela IA automatizada, além de quais riscos jurídicos e sociais podem causar.

3 MICROTRABALHOS NA ALIMENTAÇÃO DE TECNOLOGIAS EMERGENTES

Apesar da crescente demanda por mão de obra altamente qualificada no campo da IA, os processos de desenvolvimento dessas tecnologias também se sustentam sobre uma base invisibilizada de trabalho humano pouco qualificado, frequentemente situado à margem da regulação juslaboral. Trata-se de dimensão estrutural da economia digital que desafia as

narrativas de automação plena e autonomia tecnológica. Nesse contexto, destacam-se as atividades desempenhadas por microtrabalhadores, compreendidas como tarefas fragmentadas, de reduzida complexidade e baixa remuneração, distribuídas em larga escala por meio de plataformas digitais a uma multidão de trabalhadores dispersos globalmente. Conforme Rosenfield e Mossi (2020), tais tarefas constituem unidades sub individuais extremamente pequenas, com remuneração ínfima, lançadas à multidão para execução.

O microtrabalho configura uma forma contemporânea de trabalho por peça, na qual indivíduos recebem quantias irrisórias, muitas vezes alguns centavos, para executar tarefas altamente segmentadas, essenciais ao treinamento, à validação e à calibragem de sistemas de IA. Como observa Casilli (2017), tais atividades são fundamentais ao funcionamento dos algoritmos, ainda que permaneçam socialmente invisíveis. Importa distinguir o microtrabalho do trabalho *freelancer* em nuvem. Enquanto este último envolve atividades criativas, desempenhadas por profissionais qualificados e orientadas a projetos completos, o microtrabalho caracteriza-se pela fragmentação extrema, pela ausência de visão do processo produtivo como um todo e pela execução de tarefas isoladas, de curta duração e baixa exigência técnica. Sob perspectiva conceitual, o microtrabalho pode ser definido como uma modalidade de trabalho digital sob demanda, intermediada por plataformas, baseada na execução de microtarefas remuneradas individualmente, sem vínculo empregatício e desprovida de garantias trabalhistas ou proteção social (Ferraz; Costa, 2024). Apesar de sua informalidade e dispersão global, esse tipo de trabalho ocupa posição central na cadeia produtiva da IA, especialmente no que concerne à produção, anotação e verificação de dados.

No cenário brasileiro, Braz (2021) identifica cinco principais expressões do microtrabalho: (i) produção e treinamento de dados para IA; (ii) pesquisas de mercado; (iii) impulsionamento de redes sociais – as “fazendas de cliques”; (iv) serviços de divulgação e manipulação de conteúdo; e (v) testes de usabilidade de sistemas digitais. Tais atividades evidenciam a amplitude e a capilaridade desse fenômeno no contexto da economia digital. Tubaro (2020) afirma que existe um exército invisível de trabalhadores que sustentam as IAs, e exemplifica citando como exemplo os assistentes de voz baseados em inteligência artificial, os quais, antes de reconhecerem os pedidos dos usuários, precisam ser expostos a inúmeros exemplos de fala humana, “aprendendo” que todos esses pedidos significam a mesma coisa, apesar das diferenças de timbre vocal, entonação, sotaques regionais ou presença de ruídos de fundo, para, posteriormente, reconhecer solicitações semelhantes usuários.

Nesse sentido, o “sucesso” das IAs contemporâneas repousa, em larga medida, sobre o trabalho humano invisível. Como destaca Tubaro (2020), são esses trabalhadores que

etiquetam imagens, transcrevem dados, traduzem textos e alimentam sistemas com informações essenciais, executando tarefas simples e repetitivas, frequentemente remuneradas com quantias irrisórias. Essa constatação desafia diretamente o imaginário tecnológico dominante, que sustenta a ideia de autonomia plena das máquinas. Em sentido oposto, a literatura evidencia que o microtrabalho não constitui um fenômeno transitório, mas estrutural (Ekbia; Nardi, 2017). A partir do paradigma da heteromação, os autores demonstram que diversas tarefas essenciais permanecem necessariamente dependentes da intervenção humana, ainda que ocultas sob a aparência de automação.

Paralelamente, o fenômeno do Big Data, emergido na década de 1990, é caracterizado pela intensa geração e utilização de dados estruturados e semiestruturados e pela adoção de técnicas avançadas para coleta, integração, análise e uso na tomada de decisões em múltiplos contextos (Cravo, 2015). Nesse cenário, Cravo (2021) destaca que os dados, antes coletados para finalidades específicas e posteriormente descartados, passam a ser compreendidos como matéria-prima estratégica para novos modelos de negócio, constituindo insumos centrais para a criação de valor econômico. Nunca houve, portanto, tamanha quantidade de informação armazenada nem capacidade tão elevada de processá-la, o que reforça tanto o potencial quanto os desafios associados à sua utilização. Cravo (2021), salienta que o surgimento de escalas cada vez maiores de dados possibilitou o florescimento do Big Data, e que sua grande capacidade de extrair dados e analisá-los a partir de fórmulas matemáticas será capaz de mudar as formas de valor econômico e alterar mercados, organizações, relações sociais e governos.

É precisamente nesse ponto que o microtrabalho revela sua dimensão mais paradoxal: se, por um lado, o avanço das tecnologias de Big Data e dos sistemas de processamento de informações sugere a progressiva substituição da mão de obra humana, por outro, tais tecnologias são historicamente constituídas e continuamente alimentadas por dados produzidos por esses mesmos microtrabalhadores. Como observa Cravo (2021, p. 202), a elevada velocidade dos processos decisórios tende a deslocar decisões para máquinas orientadas por algoritmos “engendrados” para operar com base em probabilidades identificadas em grandes volumes de dados, e que “regular os algoritmos que deliberarão sobre as mais variadas facetas da vida humana será um grande desafio imposto pelo futuro que se aproxima”. Assim, ainda que determinados segmentos do microtrabalho possam se tornar obsoletos em razão do aperfeiçoamento algorítmico, os dados por eles gerados permanecem incorporados às infraestruturas tecnológicas, passando a ser operados por sistemas automatizados dotados de crescente capacidade decisória.

4 WEB AGÊNTICA, AUTONOMIA E RESPONSABILIZAÇÃO

Sob a perspectiva econômica, o avanço tecnológico associado à Revolução Industrial 4.0 (Faller; Feldmüller, 2015) já se consolidou como realidade, impulsionando transformações estruturais nos modelos produtivos, nas dinâmicas de mercado e, consequentemente, na própria organização social. Nesse contexto, continuamente as empresas buscam processos de modernização com o objetivo de atender às demandas dos consumidores e ampliar sua competitividade. Conforme Pistono (2017), esse movimento, inicialmente impulsionado por agentes econômicos em busca de novas oportunidades de lucro, desencadeou um efeito multiplicador, atraindo investimentos e promovendo o aperfeiçoamento das capacidades tecnológicas. Nesse cenário, a produção e o tratamento de dados assumem papel central. Miller (2013) destaca que, há décadas, indústria, governo e academia têm produzido conjuntos massivos de dados, cuja complexidade demandou o surgimento do conceito de Big Data. Essa avalanche informacional decorre da crescente conectividade de dispositivos digitais, como computadores, *smartphones* e sensores diversos, abrangendo múltiplos formatos, como textos, imagens, vídeos, registros de transações e interações digitais.

A centralidade dos dados nesse novo paradigma é inequívoca, uma vez que seu armazenamento e processamento viabilizam transações econômicas mais céleres, eficientes e com menor custo, fortalecendo a posição estratégica das organizações na economia digital. Penteado, Pelegrini e Silveira (2021) argumentam que os dados extraídos e minerados por plataformas digitais, majoritariamente controladas por grandes corporações tecnológicas do Norte Global, constituem um dos principais ativos do capitalismo contemporâneo. Dessa forma, pode-se afirmar que a Revolução 4.0 não se limita à automação industrial, mas representa um processo orientado pela exploração econômica dos dados, no qual o poder social e político passa a ser exercido por aqueles que detêm o controle sobre fluxos informacionais, fenômeno que Lemos (2023) denomina de infopoder, o qual se manifesta por meio de processos de formatação da informação que moldam, restringem e organizam o que é coletado, armazenado e redistribuído, evidenciando que tais processos estão longe de serem neutros.

A partir disso, consolidam-se infraestruturas essenciais, como os *data centers*, responsáveis por armazenar e processar dados em larga escala, desempenhando papel fundamental no desenvolvimento da economia digital e sustentando aplicações baseadas em Big Data, IA e computação em nuvem, segundo Penteado, Pelegrini e Silveira (2021). Como resultado, observa-se a otimização de processos produtivos e a redução do consumo de recursos, alinhando-se aos objetivos contemporâneos de eficiência, crescimento econômico e

sustentabilidade. Conforme Ludermir (2021), a combinação entre redes neurais artificiais e o crescimento exponencial de dados tem conduzido à consolidação da IA como mecanismo central de tomada de decisão em aspectos relevantes da vida humana, impactando desde relações sociais até dinâmicas econômicas e institucionais. Entretanto, essa mesma evolução tecnológica também amplia significativamente as vulnerabilidades dos sistemas digitais. A crescente interconectividade entre dispositivos, plataformas e infraestruturas cria superfícies de ataque que podem ser exploradas para a prática de ilícitos, como fraudes, vazamentos de dados e outras formas de cibercriminalidade. Nesse contexto, Santos e Araújo (2024) apontam para a emergência de uma verdadeira “revolução dos dados”, com impactos profundos na produção do conhecimento, na organização dos mercados e nas estruturas de governança.

Tal cenário se intensificou após a pandemia de COVID-19, que acelerou a digitalização das relações sociais, econômicas e laborais. O aumento da conectividade e a expansão do uso de plataformas digitais contribuíram para a ampliação exponencial da produção de dados, ao mesmo tempo que favoreceram o surgimento de novas formas de trabalho mediadas por tecnologias digitais. Lemos (2023) destaca que a sociedade contemporânea passa a operar sob a lógica do capitalismo de vigilância, marcado pela plataformização da vida social, entendida como a organização das interações humanas por meio de infraestruturas digitais. Cravo (2015) enfatiza que os dados, antes coletados a uma finalidade específica e posteriormente esquecidos, passaram a ser matéria bruta para negócios alternativos, constituindo insumos vitais à criação de novas formas de valor econômico.

É precisamente nesse ponto que emerge um risco estrutural ainda mais profundo: a utilização massiva de dados produzidos em contextos precarizados de trabalho, especialmente por meio do microtrabalho e de outras formas invisibilizadas de trabalho humano. Esses trabalhadores, frequentemente desassistidos por mecanismos estatais de proteção, participam de cadeias produtivas digitais sem transparência, reconhecimento ou garantias de direitos, contribuindo diretamente ao treinamento, à validação e à operação de sistemas de IA. Dessa forma, evidencia-se uma contradição fundamental: embora os sistemas de IA sejam frequentemente apresentados como autônomos, sua operação depende, em larga medida, de trabalho humano invisibilizado. Esses fluxos de trabalho alimentam continuamente as bases de dados, que sustentam o funcionamento desses sistemas.

Além disso, a ascensão da Inteligência Artificial Generativa – IAGen e de agentes autônomos intensifica esse problema, pois operam a partir de grandes volumes de dados e comandos (*prompts*), sendo capazes de executar tarefas complexas, inclusive em contextos sensíveis. No entanto, essa mesma capacidade pode ser instrumentalizada por agentes

maliciosos para a prática de ilícitos, ampliando os riscos jurídicos e sociais associados ao uso dessas tecnologias. Baldissera (2024) elenca os 6 riscos da IA: desemprego estrutural, aumento da desigualdade social, perpetuação de vieses e preconceitos, indefinição sobre direitos autorais, riscos à privacidade e desinformação. A crescente complexidade dos ecossistemas digitais contemporâneos impõe desafios inéditos ao Direito, especialmente no que se refere à responsabilização por danos decorrentes do uso de tecnologias emergentes. Nesse contexto, a reflexão da Ministra do Supremo Tribunal Federal – STF, Cármen Lúcia, proferida em palestra sobre desinformação e democracia na Universidade Estadual do Ceará – UECE, revela-se particularmente elucidativa ao destacar os riscos associados à disseminação massiva de informações falsas em cenários marcados pela intensificação do uso de IA. Ao afirmar que “a influência que pode ter deste tipo de mentiras, multiplicadas aos milhões, numa velocidade estonteante [...] é absurda” (Rocha, 2026, n.p.), a Ministra evidencia não apenas a dimensão quantitativa do fenômeno, mas seu impacto qualitativo sobre o funcionamento das instituições democráticas. A desinformação, potencializada por tecnologias digitais, deixa de ser um problema marginal para se tornar um elemento estrutural de desestabilização da esfera pública.

Tal cenário se agrava com o advento de sistemas de IA capazes de operar de forma autônoma e interconectada. Conforme destacado na mesma fala, emergem tecnologias que “funcionam independente do ser humano, criam redes com outros softwares” (Rocha, 2026, n.p.), estabelecendo dinâmicas de interação que prescindem da intervenção humana direta. Essa realidade aproxima-se do modelo da Web Agêntica, no qual agentes inteligentes descentralizados passam a executar tarefas, tomar decisões e interagir entre si em ambientes digitais complexos. Essa transformação tecnológica tensiona profundamente os modelos jurídicos tradicionais de responsabilização. O Direito clássico estrutura-se a partir de categorias como ação humana, culpa, dolo e nexô causal, pressupostos que se tornam progressivamente insuficientes diante de sistemas autônomos que operam por meio de algoritmos, aprendizado de máquina e interações distribuídas.

Tal realidade, contudo, não elimina a participação humana, mas a reconfigura. Conforme Tubaro (2020), esses sistemas são alimentados por extensas bases de dados frequentemente produzidas por microtrabalhadores dispersos globalmente. Assim, mesmo em contextos altamente automatizados, como o uso de armas autônomas, persiste uma dimensão invisível do trabalho humano que sustenta as redes neurais, evidenciando que a “autonomia” das máquinas é construída por múltiplas camadas de intervenção humana. Esse deslocamento decisório inaugura um dos mais complexos dilemas éticos e jurídicos da contemporaneidade: a atribuição de responsabilidade por atos praticados por sistemas autônomos. Quando tais

sistemas causam danos, como ataques indevidos a civis, propagação de notícias falsas, mentiras políticas contra a democracia ou disseminação de imagem manipulada com fins políticos, torna-se necessário reconstruir a cadeia decisória para identificar a origem do evento, tarefa complexa diante da multiplicidade de agentes envolvidos. Nesse sentido, se o dano decorre de uma falha de programação, surge a hipótese de responsabilização de desenvolvedores ou das empresas responsáveis pelo sistema. Se resulta de erro operacional, a responsabilidade pode recair sobre autoridades militares que autorizaram ou supervisionaram o uso da tecnologia, como nos crimes de guerra. Contudo, em cenários de elevada autonomia, nos quais o sistema toma decisões com base em aprendizado de máquina e interpretação de dados, a identificação de um agente humano diretamente responsável torna-se difusa, abrindo espaço para uma zona de indeterminação jurídica. Assim, a rastreabilidade das condutas assume papel central para a efetivação da responsabilização jurídica.

No ordenamento brasileiro, a principal norma que disciplina essa matéria é o Marco Civil da Internet, que estabelece regras sobre a guarda e a disponibilização de registros de conexão e de acesso a aplicações. O art. 10, § 1º, dispõe que os provedores somente são obrigados a fornecer registros capazes de identificar usuários mediante ordem judicial, garantindo a proteção da privacidade e o devido processo legal. O art. 13 determina que os provedores de conexão devem armazenar os registros de conexão, como endereço IP (*Internet Protocol*), data e horário de início e término, pelo prazo de um ano. Já o art. 15 impõe aos provedores de aplicação o dever de armazenar registros de acesso às suas plataformas pelo prazo de seis meses. Complementarmente, o art. 22 autoriza que a parte interessada requeira judicialmente a disponibilização desses registros para fins probatórios, permitindo a identificação de usuários em casos de ilícitos (Brasil, 2014). Esse conjunto normativo evidencia que a rastreabilidade é um elemento estruturante do modelo brasileiro de responsabilização na internet. Todavia, tais dispositivos foram concebidos em um contexto no qual as ações no ambiente digital eram predominantemente praticadas por usuários humanos identificáveis, enquanto na Web Agêntica a atuação de agentes autônomos rompe com essa lógica, uma vez que decisões e condutas passam a ser executadas por sistemas que não se enquadram nas categorias jurídicas tradicionais de sujeitos de direito.

A dificuldade de identificação de autoria e de delimitação do nexo causal é ampliada pela arquitetura desses sistemas, marcada por descentralização, opacidade algorítmica e dependência de grandes volumes de dados. Como discutido, tais sistemas são frequentemente alimentados por dados produzidos em contextos de microtrabalho e trabalho humano invisibilizado, o que complexifica as cadeias de responsabilidade, sobretudo diante de estruturas

que, em grande medida, operam sob o viés da ilegalidade. Assim, torna-se necessário repensar os fundamentos da responsabilidade jurídica à luz da teoria do risco. A responsabilidade objetiva, baseada no risco da atividade, apresenta-se como alternativa relevante ao deslocar o foco da culpa para a atividade desenvolvida, responsabilizando aqueles que se beneficiam economicamente da exploração dessas tecnologias. Essa perspectiva dialoga com discussões contemporâneas sobre a regulação das plataformas digitais e das *big techs*, que enfrentam desafios semelhantes quanto à moderação de conteúdo e à disseminação de desinformação (Cravo, 2015). A ausência de mecanismos eficazes de identificação e responsabilização contribui para a perpetuação de danos sociais, como o discurso de ódio e a manipulação informacional. Embora o Marco Civil da Internet e a LGPD ofereçam bases importantes à responsabilização, ao estabelecerem princípios como transparência, prestação de contas e proteção de direitos fundamentais, ainda se mostram insuficientes diante da complexidade dos sistemas autônomos e descentralizados característicos da Web Agêntica.

Nesse sentido, a responsabilização jurídica na Web Agêntica não pode ser compreendida apenas sob uma perspectiva reparatória, mas deve assumir função preventiva e estrutural, voltada à preservação da confiança pública e à proteção da integridade do espaço democrático. Dessa forma, a insuficiência dos mecanismos tradicionais de rastreabilidade, como previstos no Marco Civil da Internet, evidencia a necessidade de desenvolvimento de novos instrumentos jurídicos, como os mecanismos de KYA, capazes de identificar, rastrear e vincular agentes inteligentes aos respectivos responsáveis, assegurando a efetividade da responsabilização em ambientes digitais (Desai; Kroll, 2017).

5 CONCLUSÃO

A expansão da IA e o surgimento da Web Agêntica representam uma transformação relevante nas dinâmicas sociais, econômicas e jurídicas contemporâneas ao redefinirem a forma como decisões são produzidas, informações são processadas e interações digitais são estabelecidas. Ao longo desta pesquisa, evidenciou-se que a crescente autonomia dos sistemas inteligentes, especialmente aqueles estruturados em redes descentralizadas e multiagentes, desafia os modelos tradicionais de proteção dos direitos fundamentais e de responsabilização jurídica. Também se verificou que, embora frequentemente apresentados sob a narrativa de automação plena, tais sistemas permanecem estruturalmente dependentes de trabalho humano invisibilizado, sobretudo do microtrabalho digital, responsável pela produção, rotulação, validação e moderação de dados essenciais ao funcionamento dos algoritmos. No campo dos

direitos fundamentais, constatou-se que a coleta massiva de dados, a opacidade algorítmica e a crescente automação decisória ampliam os riscos de violações à privacidade, à liberdade de expressão, à igualdade, à autodeterminação informativa e à integridade democrática. Em contextos de intensa circulação informacional, como os processos eleitorais, sistemas automatizados podem potencializar a desinformação, a manipulação política, a reprodução de vieses discriminatórios e a ampliação das assimetrias de poder informacional.

Observou-se, ainda, que instrumentos normativos como o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais, embora representem avanços relevantes, mostram-se insuficientes diante das especificidades da Web Agêntica. Tais diplomas foram concebidos em contexto marcado pela atuação de usuários humanos identificáveis, realidade distinta da inaugurada por agentes inteligentes autônomos, capazes de operar, interagir e tomar decisões de modo descentralizado, pseudônimo e transjurisdicional. Nesse cenário, a dificuldade de identificação de autoria, de delimitação do nexo causal e de atribuição de responsabilidade emerge como um dos principais desafios jurídicos contemporâneos, exigindo a ampliação do debate sobre regimes baseados na teoria do risco e na responsabilidade objetiva.

Por fim, sustenta-se a necessidade de novos mecanismos de governança digital capazes de assegurar identificação, rastreabilidade, transparência e auditabilidade dos agentes inteligentes. Iniciativas como o KYA mostram-se promissoras ao propor formas de vinculação entre agentes autônomos e seus responsáveis, contribuindo para mitigar a opacidade e fortalecer a responsabilização jurídica em ambientes descentralizados. Conclui-se, portanto, que a proteção dos direitos humanos e fundamentais na era da Web Agêntica dependerá da construção de um modelo regulatório interdisciplinar, capaz de articular fundamentos jurídicos, parâmetros técnicos e princípios éticos, garantindo que o avanço tecnológico ocorra de forma compatível com os valores democráticos e com a dignidade da pessoa humana.

REFERÊNCIAS

ACIOLY, L. H. de M. Reflexões sobre a utilização da Inteligência Artificial e algoritmos nas relações consumeristas à luz da Lei Geral de Proteção de Dados. **Revista Brasileira de Direito Comercial, Empresarial, Concorrencial e do Consumidor**, Porto Alegre, ano 8, n. 48, p. 185-167, ago./set. 2022.

ACIOLY, L. H. de M.; MENDES, I. B. B.; MONTEIRO NETO, J. A. As avaliações de impacto como instrumentos de inteligibilidade algorítmica e garantia dos direitos fundamentais na regulação de inteligência artificial. **Diké**, v. 22, n. 24, p. 225-251, 2023.

BALDISSERA, O. Conheça 6 riscos da inteligência artificial. **PUCPR Digital**, 11 maio 2024.

BASESCAN. Base transaction hash details. **BaseScan**, 16 dez. 2024. Disponível em: <https://basescan.org/tx/0x57c20f70f48dd2d301266f09db4c6e76f37ed5d84d514f602cb7bd166bd3f4fd>. Acesso em: 16 maio 2026.

BORDINI, R. H. Saiba como a Inteligência Artificial é utilizada em diferentes segmentos. **PUCRS**, Porto Alegre, 9 jun. 2023.

BORDINI, R. H.; VIEIRA, R. Linguagens de programação orientadas a agentes: uma introdução baseada em AgentSpeak(L). **Revista de Informática Teórica e Aplicada**, Porto Alegre, v.10, n. 1, p. 7-38, 2003.

BRASIL. [Constituição (1988)]. **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 (Marco Civil da Internet). **Diário Oficial da União**, Brasília, 24 abr. 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, 15 ago. 2018.

BRAZ, M. V. Heteromação e microtrabalho no Brasil. **Sociologias**, ano 23, n. 17, p. 134-172, maio/ago. 2021.

CASILLI, A. Digital labor studies go global: toward a digital decolonial turn. **International Journal of Communication**, v. 11, p. 3934-3954, 2017.

CHAFFER, Tomer Jordi. Know Your Agent: governing AI identity on the Agentic Web. **DeGov Labs**, 25 abr. 2025.

CRAVO, V. O Big Data e os desafios da modernidade: uma regulação necessária? **Revista de Direito Setorial e Regulatório**, Brasília, v. 1, n. 2, p. 243-257, 2015.

CRAVO, V. O Big Data e os desafios da modernidade: uma regulação necessária? **Endless: International Journal of Future Studies**, v. 4, n. 2, p. 198-207, 2021.

DESAI, D. R.; KROLL, J. A. Confie, mas verifique: um guia para algoritmos e a lei. **Harvard Journal of Law & Technology**, 2017.

EKBIA, H. R.; NARDI, B. **Heteromation, and other stories of computing and capitalismo**. Cambridge: MIT Press, 2017.

EUROPEAN UNION. Document 32024R1689. **Jornal Oficial da União Europeia**, 12 jul. 2024.

FALLER, C.; FELDMÜLLER, D. Learning factory for Industry 4.0 to provide future skills beyond technical training. **Procedia CIRP**, v. 32, p. 91-96, 2015.

FERRAZ, D. B.; COSTA, M. M. M. da. Microtrabalho na inteligência artificial: direitos fundamentais das mulheres e a ética do cuidado. **Revista Brasileira de Sociologia do Direito**, v. 11, n. 2, p. 25-43, maio/ago. 2024.

GOLDSTON, J.; CHAFFER, T. J.; MARTINEZ, G. O metaverso como o Leviatã digital: um estudo de caso de Bit.Country. **Journal of Applied Business and Economics**, v. 24, n. 2, 2022.

GROVER, C. C.; OEVER, N. ten. **Guidelines for human rights protocol and architecture considerations**. RFC 9620. Fremont, CA: Internet Research Task Force, 2024.

HU, B. “A.”; RONG, H.; TAY, J. Is decentralized artificial intelligence governable? Towards machine sovereignty and human symbiosis. **Social Science Research Network**, 9 jan. 2025.

KARIM, M. M.; VAN, D. H.; KHAN, S.; QU, Q.; KHOLODOV, Y. AI Agents meet blockchain: a survey on secure and scalable collaboration for multi-agents. **Future Internet**, v. 17, n. 2, p. 57, 2025.

LE MOS, A. L. M. O futuro da sociedade de plataformas no Brasil. **Intercom: Revista Brasileira de Ciências da Comunicação**, São Paulo, v. 46, 2023.

LUDERMIR, T. B. Inteligência Artificial e aprendizado de máquina: estado atual e tendências. **Estudos Avançados**, v. 35, n. 101, p. 85-94, jan. 2021.

MILLER, H. G. Dos dados às decisões: uma cadeia de valor para Big Data. **IT Professional**, v. 15, n. 1, p. 57-59, jan./fev. 2013.

MURUGESAN, S. The rise of agentic AI: implications, concerns, and the path forward. **IEEE Intelligent Systems**, v. 40, n. 2, p. 8, 2025.

NEGRI, S. M. C. de Á.; MACHADO, J. de S.; GIOVANINI, C. F. R.; BATISTA, N. P. R. Sistemas de inteligência artificial e avaliações de impacto para direitos humanos. **Revista Culturas Jurídicas**, v. 10, 2023.

OLAS. The Open Autonomy framework. **Olas Stack Developer Documentation**, [s.d.]. Disponível em: <https://stack.olas.network/open-autonomy/>. Acesso em: 16 maio 2026.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. Paris: Assembleia Geral das Nações Unidas, 1948.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Pacto Internacional sobre Direitos Econômicos, Sociais e Culturais**. Nova York: Assembleia Geral das Nações Unidas, 1966a.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Pacto Internacional sobre Direitos Civis e Políticos**. Nova York: Assembleia Geral das Nações Unidas, 1966b.

PENTEADO, C.; PELLEGRINI, J.; SILVEIRA, S. A. da. Dataficação, plataformas digitais, regulação e políticas anticoloniais In: PENTEADO, C.; PELLEGRINI, J.; SILVEIRA, S. A. da. **Plataformização, inteligência artificial e soberania de dados: tecnologia no Brasil 2020–2030**. São Paulo: Fundação Friedrich Ebert Stiftung Brasil, 2021. p. 21-30.

PISTONO, F. **Os robôs vão roubar o seu trabalho, mas tudo bem**. Tradução: Pedro Soares. São Paulo: Portfolio Pinguim, 2017.

QI, Y.; FENG, Y.; WANG, X.; LI, H.; TIAN, J. Leveraging federated learning and edge computing for recommendation systems within cloud computing networks. **arXiv**, 2024.

QIU, J.; LAM, K.; LI, G.; ACHARYA, A.; WONG, T. Y.; DARZI, A.; YUAN, W.; TOPOL, E. J. LLM-based agentic systems in medicine and healthcare. **Nature Machine Intelligence**, v. 6, p. 1418-1420, 2024.

QUARESMA, A. A falácia lúdica das três leis: ensaio sobre inteligência artificial, sociedade e o difícil problema da consciência. **PAAKAT: Revista de Tecnología y Sociedad**, n. 19, p. 478, 2020.

ROCHA, C. L. A. Democracia em tempos de desinformação: desafios e perspectivas – Conferência Magna com a Ministra Cármen Lúcia. **Canal Youtube da Universidade Estadual do Ceará**, 16 mar. 2026. 1 vídeo (2 h 15 min).

ROSENFELD, C.; MOSSI, T. W. Trabalho decente no capitalismo contemporâneo: dignidade e reconhecimento no microtrabalho por plataformas. **Sociedade e Estado**, v. 35, n. 3, set./dez. 2020.

SANTOS, M. C. C. L. dos; ARAÚJO, M. A Inteligência Artificial (IA) e a lei brasileira de responsabilidade e transparência na internet – Humanismo 4.0 – Impactos na cidadania. In: CAMPILONGO, C. F.; GONZAGA, A. de A.; FREIRE, A. L (coord.). **Enciclopédia jurídica da PUC-SP**. Tomo: Direito Econômico (coordenado por Ricardo Hasson Sayeg. São Paulo: PUC-SP, 2024.

TAILLE, Y. la. Moral e ética no mundo contemporâneo. **Revista USP**, São Paulo, n. 110, p. 29-42, jul./ago./set. 2016.

TUBARO, P. Whose intelligence is artificial intelligence? **Global Dialogue**, p. 38-39, 2020.

UNITED NATIONS. **Relatório do Relator Especial sobre a Promoção e Proteção do Direito à Liberdade de Opinião e Expressão**. Genebra: ONU, 2011.

UNITED NATIONS. **Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression**. Genebra: UNHRC, 2017.

WALTERS, S.; GAO, S.; NERD, S.; DA, F.; WILLIAMS, W.; MENG, T.-C.; CHOW, A.; HAN, H.; HE, F.; ZHANG, A.; WU, M.; SHEN, T.; HU, M.; YAN, J. Eliza: a Web3 friendly AI agent operating system. **arXiv**, 24 jan. 2025.

YU, Jeffy. Memes, markets, and machines: the evolution of on-chain autonomy through hyperstition. **arXiv**, 2024.

ZEFERINO, M. C.; RODRIGUES, R. dos S. Democracia em risco? O impacto das tecnologias da informação e comunicação no cenário político brasileiro. **Anais de Direitos Humanos e Fundamentais**, Criciúma, 2025.