

VIII ENCONTRO VIRTUAL DO CONPEDI

**DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS
II**

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

D597

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

Coordenadores: Cinthia Obladen de Almendra Freitas; Yuri Nathan da Costa Lannes. – Florianópolis: CONPEDI, 2025.

Inclui bibliografia

ISBN: 978-65-5274-156-1

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

Tema: Direito Governança e Políticas de Inclusão

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias. VIII Encontro Virtual do CONPEDI (2; 2025; Florianópolis, Brasil).

CDU: 34



Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

VIII ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

Apresentação

O VIII Encontro Virtual do CONPEDI, organizado pelo CONPEDI, teve como tema central “Direito Governança e Políticas de Inclusão”. A partir dessa temática, foram promovidos intensos debates entre pesquisadores nacionais e internacionais, com apresentações de trabalhos previamente selecionados por meio de avaliação duplo-cega por pares.

Os artigos reunidos nesta publicação foram apresentados no Grupo de Trabalho “Direito, Governança e Novas Tecnologias II”, realizado no dia 27 de junho de 2025, e refletem o estado atual das pesquisas desenvolvidas por graduandos e pós-graduandos em direito em diversas instituições brasileiras. O conjunto de trabalhos revela a diversidade temática e a profundidade das discussões jurídicas contemporâneas sobre os impactos da tecnologia na sociedade.

As apresentações cobriram uma ampla gama de tópicos que envolvem a interface entre tecnologia, direito, demonstrando um panorama das preocupações acadêmicas sobre o reconhecimento facial, a inteligência artificial e os desafios ao judiciário, direitos autorais e inteligência artificial, democracia digital e pós-verdade, governo digital, políticas públicas, sociedade digital e transformação do direito privacidade, desinformação e desigualdades digitais. Com o intuito de facilitar a leitura e destacar os enfoques abordados, os trabalhos foram organizados nos seguintes eixos temáticos:

1. Reconhecimento Facial, Vigilância e Direitos Fundamentais - Este eixo concentra estudos sobre o uso da tecnologia de reconhecimento facial no contexto da segurança pública e seus impactos sobre direitos fundamentais, com ênfase em discriminação algorítmica, proteção de

Reconhecimento facial para vigilância: comparação das aplicações da inteligência artificial em eventos de massa no Brasil e em experiências internacionais (Yuri Nathan da Costa Lannes / Júlia Mesquita Ferreira / Lais Faleiros Furuya)

Reconhecimento facial e a violação de direitos fundamentais: discriminação algorítmica, vigilância em massa e a necessidade de regulação no Brasil (Bibiana Paschoalino Barbosa / Anderson Akira Yamaguchi / Ruan Ricardo Bernardo Teodoro)

2. Inteligência Artificial, Judiciário e Regulação - Este eixo analisa a aplicação da inteligência artificial no sistema de justiça e os desafios regulatórios do contexto brasileiro, com foco na governança tecnológica e nos riscos da opacidade algorítmica:

O uso da inteligência artificial no Poder Judiciário brasileiro e a Resolução do Conselho Nacional de Justiça n.º 615/2025 (Simone Stabel Daudt / Rosane Leal Da Silva / Julia Daudt Mansilha)

Inteligência artificial e a crise da regulação clássica: um estudo sobre o atual contexto regulatório brasileiro (Fernanda Sathler Rocha Franco / Luiz Felipe de Freitas Cordeiro / Marina Moretzsohn Chust Trajano)

Direito à transparência, inteligência artificial e desafios técnicos: uma análise do Projeto de Lei nº 2.338/23 (Fernanda Sathler Rocha Franco)

Opacidade algorítmica estratégica e risco sistêmico informacional nas eleições: considerações para uma governança anti-manipulação das democracias digitais (Helena Dominguez Paes Landim Bianchi / Maria Clara Giasseti Medeiros Corradini Lopes)

3. Direitos Autorais, Propriedade Intelectual e IA - Reúne pesquisas que discutem a

O uso indevido das imagens geradas pelos filtros Ghibli e a proteção do direito à imagem sob a perspectiva da Lei Geral de Proteção de Dados (LGPD) (Lilian Benchimol Ferreira / Maria Cristina Almeida Pinheiro de Lemos / Narliane Alves De Souza E Sousa)

4. Democracia Digital, Desinformação e Pós-Verdade - Trabalhos que discutem os impactos da tecnologia na propagação de fake news, movimentos ideológicos e desinformação em contextos democráticos:

Movimentos antifeministas e desinformação: quando a misoginia se propaga em fake News (Juliana Aparecida de Jesus Pires / Irineu Francisco Barreto Junior / Samyra Haydêe Dal Farra Napolini)

A sociedade do cansaço e pós-verdade: fake news sobre as urnas eletrônicas (Bruna Figueiredo Dos Santos / Zulmar Antonio Fachin)

5. Governança Digital, Políticas Públicas e Compartilhamento de Dados - Aborda o papel das políticas públicas e da governança digital no século XXI, destacando os desafios do uso de dados por entes públicos e o potencial das tecnologias no desenvolvimento social:

Governança digital e democracia no século XXI: o papel das políticas públicas na era da inteligência artificial (Daniel David Guimarães Freire)

O potencial do compartilhamento de dados entre entes federativos para o desenvolvimento de políticas públicas inteligentes (Ana Cristina Neves Valotto Postal / Paulo Cezar Dias / Rodrigo Abolis Bastos)

6. Tecnologia, Sustentabilidade e Transformação Econômica - Esse eixo reúne trabalhos sobre o impacto das inovações tecnológicas em setores como o agronegócio e as ecotecnologias, destacando aspectos de compliance, sustentabilidade e tributação:

7. Sociedade Digital, Infância e Transformações do Direito - Trabalhos que discutem os efeitos das tecnologias emergentes sobre a infância, os registros civis, a exposição digital e os reflexos no Direito Civil e registral:

A vitrine digital da infância e o papel do Direito: análise do sharenting e das iniciativas legislativas brasileiras (Ana Júlia Oliveira Machado / Bibiana Paschoalino Barbosa)

Inovações e desafios na implantação das tecnologias notariais e registrais: uma análise do e-Notariado cinco anos após sua criação (José Luiz de Moura Faleiros Júnior / Francislene Silva Da Costa Garcia / Isabela da Cunha Machado Resende)

O impacto da tecnologia na sociedade aberta: desafios e oportunidades para o Direito Civil (Viviane Ferreira Mundim / Najua Samir Asad Ghani / Patricia Maria Paes de Barros)

Treinamento de inteligência artificial e consumidores mudando marcas de seus bens em protesto político (Carlos Alberto Rohrmann)

Espera-se que esta publicação contribua para o aprofundamento dos debates sobre os desafios jurídicos da era digital, estimulando novas reflexões e a produção científica crítica e inovadora. Agradecemos a todos os pesquisadores, pareceristas e organizadores que tornaram este Grupo de Trabalho possível. Desejamos uma excelente leitura!

Cinthia Obladen de Almendra Freitas – PUC-PR

Liton Lanes Pilau Sobrinho – UNIVALI

Yuri Nathan da costa Lannes - FDF

**OPACIDADE ALGORÍTMICA ESTRATÉGICA E RISCO SISTÊMICO
INFORMACIONAL NAS ELEIÇÕES: CONSIDERAÇÕES PARA UMA
GOVERNANÇA ANTI-MANIPULAÇÃO DAS DEMOCRACIAS DIGITAIS**

**STRATEGIC ALGORITHMIC OPACITY AND INFORMATIONAL SYSTEMIC
RISK IN ELECTIONS: CONSIDERATIONS FOR AN ANTI-MANIPULATION
GOVERNANCE OF DIGITAL DEMOCRACIES**

Helena Dominguez Paes Landim Bianchi ¹

Maria Clara Giassetti Medeiros Corradini Lopes ²

Resumo

O presente artigo analisa a problemática da opacidade algorítmica estratégica como fator de risco sistêmico para as democracias digitais contemporâneas. Em contraste com a visão tradicional de opacidade como mero subproduto técnico, sustenta-se que algoritmos opacos vêm sendo deliberadamente utilizados para manipular processos eleitorais, afetando o acesso à informação, a formação da opinião pública e a integridade do voto. Por outro lado, também é apresentada a perspectiva do paradoxo da transparência, que assevera a possibilidade de aumento da manipulação. A pesquisa adota o método dedutivo e baseia-se em revisão bibliográfica e documental de fontes nacionais e internacionais, com enfoque interdisciplinar no Direito, Ciência Política e Governança Digital. O estudo demonstra que a manipulação algorítmica, potencializada pela opacidade estratégica, gera impactos que extrapolam danos individuais, configurando riscos sistêmicos informacionais que ameaçam a confiança pública, a estabilidade institucional e os direitos humanos. Examina-se criticamente as abordagens regulatórias atuais, como o Regulamento Europeu de Inteligência Artificial (AI Act) e o Projeto de Lei n.º 2.338/2023 no Brasil, evidenciando seus limites diante da manipulação algorítmica intencional. Ao final, propõe-se a necessidade de um novo paradigma de governança anti-manipulação algorítmica, que una transparência, rastreabilidade, auditorias de impacto e mecanismos de proteção reforçada para grupos vulneráveis.

Palavras-chave: Opacidade algorítmica, Democracia digital, Risco sistêmico, Governança de algoritmos, Direitos humanos

manipulate electoral processes, affecting access to information, the formation of public opinion and the integrity of the vote. On the other hand, the perspective of the transparency paradox is also presented, which asserts the possibility of increased manipulation. The research adopts the deductive method and is based on a bibliographic and documentary review of national and international sources, with an interdisciplinary focus on Law, Political Science and Digital Governance. The study shows that algorithmic manipulation, enhanced by strategic opacity, generates impacts that go beyond individual harm, configuring systemic informational risks that threaten public trust, institutional stability and human rights. Current regulatory approaches are critically examined, such as the European Artificial Intelligence Regulation (AI Act) and Bill 2.338/2023 in Brazil, highlighting their limits in the face of intentional algorithmic manipulation. Finally, it proposes the need for a new anti-algorithmic manipulation governance paradigm that combines transparency, traceability, impact audits and enhanced protection mechanisms for vulnerable groups.

Keywords/Palabras-claves/Mots-clés: Algorithmic opacity, Digital democracy, Systemic risk, Algorithm governance, Human rights

INTRODUÇÃO

A inteligência artificial (IA) está transformando sociedades, setores econômicos e o mundo do trabalho, e é provável que isso aconteça cada vez mais no futuro. Como definição, sistemas de IA buscam simular traços humanos como conhecimento, raciocínio, solução de problemas, percepção, aprendizado e planejamento. O uso da IA pode superar barreiras e jurisdições nacionais, bem como permite aplicações variadas para a indústria, comércio, ciência, academia e política.

Nos últimos anos, o mundo tem testemunhado uma revolução da IA, trazendo descobertas de novas tarefas que as máquinas podem realizar. Especialmente considerando as técnicas de processamento de linguagem natural e sua ampla capacidade de interpretação de grandes volumes de informações, uma nova onda causada pela IA generativa - que possui capacidade de geração de conteúdos de texto, imagem, vídeo ou áudio - tem sido combustível para o aumento da presença de IA em todas as esferas da vida em sociedade e de aceleração da discussão de seus impactos (Jungherr, 2023, p.1), sejam eles positivos ou negativos.

Isso porque, tal como outras tecnologias, os efeitos benéficos da inovação - como melhoria do bem-estar e o progresso das pessoas, a contribuição para atividades econômicas sustentáveis e positivas, e o impulsionamento de eficiência e produtividade - hão de ser ponderados e balanceados com seus impactos e riscos provocados ou exacerbados em razão da IA, sobretudo os impactos sociais, políticos e democráticos.

Para adentrar a temática do uso de IA em eleições, faz-se mister destacar que frequentemente mobilizações políticas são impulsionadas por novas tecnologias, as quais permitem que as pessoas encontrem novas formas para se informar, expressar suas opiniões e mudar os regimes políticos dos seus países, enquanto cidadãos. Um exemplo disto foi a massiva presença das redes sociais no contexto da “Primavera Árabe”, em 2011 (Alcoforado et al., 2024, p. 407).

Logo, campanhas eleitorais na atualidade já são inseridas no contexto de ampla utilização de serviços digitais e tecnologias, sendo elemento crucial para definição da estratégia política e dos resultados buscados nas urnas. Da mesma forma, o desenvolvimento tecnológico se torna parte da governança pública e de demais organizações essenciais ao processo eleitoral, como institutos de pesquisa, jornalismo e telecomunicações. Nesse cenário, é fundamental considerar que o processo de democratização pode se beneficiar da IA, das novas tecnologias e das promessas de uma democracia digital (De Oliveira, 2024, p.2).

Observando a inteligência artificial, em especial os processos internos que ocorrem para a tomada de decisão da máquina, nota-se uma dificuldade involuntária de compreender plenamente o funcionamento interno dos algoritmos - ainda que, por ventura, não haja intenção explícita de ocultação. Tal fenômeno é denominado “opacidade algorítmica” e costuma decorrer, segundo Burrell (2016), da inevitável complexidade técnica dos sistemas de *machine learning*, do sigilo industrial ou das limitações cognitivas humanas (analfabetismo técnico).

Com a ascensão das plataformas digitais como agentes políticos e econômicos centrais na sociedade informacional, entretanto, passou-se à emergência de uma opacidade estratégica, configurada pela utilização de práticas deliberadas de ocultação, dissimulação ou obstrução da compreensão pública sobre os mecanismos de funcionamento dos algoritmos, com o objetivo de potencializar práticas de manipulação de informações e comportamentos sociais (Pasquale, 2015).

Tem-se, portanto, a instrumentalização da opacidade como ferramenta ativa de dominação política, desinformação dirigida e reforço de assimetrias de poder nas democracias digitais. O uso estratégico da opacidade transforma o risco algorítmico de individualizado em coletivo e sistêmico, afetando a integridade eleitoral, a formação da opinião pública e a confiança social nas instituições democráticas.

A questão da manipulação algorítmica nas eleições não se limita a um problema ético ou moral isolado. A amplitude, velocidade e opacidade com que essas práticas se espalham configuram um fenômeno com características típicas de risco sistêmico — conceito originalmente desenvolvido na teoria financeira para descrever ameaças que podem colapsar sistemas inteiros (Gai; Kapadia, 2010).

Conforme será abordado ao longo deste trabalho, a manipulação algorítmica pode desestabilizar as fundações do sistema democrático ao erodir a confiança coletiva nos processos eleitorais, amplificar a desinformação em escala massiva e incontrolável, promover desigualdades políticas ocultas e silenciosas e tornar o ambiente informacional altamente volátil e polarizado.

Segundo o Global Risks Report 2024 do Fórum Econômico Mundial, a desinformação algorítmica é hoje considerada um dos principais fatores de risco sistêmico globais, ao lado de ameaças climáticas e cibernéticas (WEF, 2024).

Assim, tratar a manipulação algorítmica apenas como violação pontual ou fraude eleitoral subestima seus efeitos. É necessário reconhecê-la como ameaça estrutural à

estabilidade democrática, exigindo a implementação de políticas de governança anti-manipulação algorítmica robustas, preventivas e internacionalmente coordenadas.

Dessarte, o objetivo geral do presente trabalho é analisar como a opacidade algorítmica estratégica agrava riscos sistêmicos à democracia em processos eleitorais e propor soluções de governança anti-manipulação.

Os objetivos específicos, por sua vez, perpassam por identificar como algoritmos opacos são utilizados para manipular processos eleitorais, demonstrar a escalada para risco sistêmico informacional e propor princípios de governança jurídica e ética anti-manipulação.

Para alcançar os objetivos propostos, a pesquisa se utiliza de metodologia bibliográfica e documental, com método dedutivo-analítico e abordagem interdisciplinar.

DESENVOLVIMENTO

INTELIGÊNCIA ARTIFICIAL, DEMOCRACIA E ELEIÇÕES

Uma importante aplicação da IA é percebida para a melhoria da precisão e eficácia das pesquisas eleitorais, com algoritmos que podem classificar registros eleitorais, informações demográficas e publicações em mídias sociais e, com isso, prever melhor o comportamento dos eleitores e os resultados das eleições. Campanhas políticas são beneficiadas ao planejar melhor e concentrar suas estratégias, resultando em campanhas mais eficientes e focadas (Chennupati, 2024, p.30).

Ainda, para otimizar a eficiência dos métodos preparatórios para votação, os processos de registro de eleitores podem se tornar mais acessíveis e eficazes ao serem automatizados e simplificados, minimizando o erro humano e garantindo o registro preciso dos eleitores qualificados (Chennupati, 2024, p.30).

Destaca-se também o uso de IA aliado à detecção e prevenção de fraudes eleitorais, examinando enormes volumes de dados para encontrar anomalias, como registros duplicados ou tentativas de ataque, garantindo uma contagem de votos precisa e protege a integridade do processo de votação (Chennupati, 2024, p.30)

Não obstante, ao passo que as tecnologias podem ser veículos benéficos à promoção de direitos políticos, também são espaço para geração de tensão social e polarização, além da facilitação de propagação de discursos extremistas e disseminação de notícias falsas. (Alcoforado et al., 2024, p. 407).

O primeiro impacto à democracia considerado neste artigo consiste na deterioração do discurso político pela desinformação possibilitada pela IA (Jungherr, 2023, p.1). Isso porque cidadãos bem-informados e espaços de debate e crítica são princípios fundamentais da democracia e, sem eles, a qualidade do debate pelo qual as sociedades devem passar para melhorar a si mesmas pode degradar (Alcoforado et al., 2024, p. 407). Há que se considerar como a IA afeta a capacidade de tomada de decisão a partir do ambiente de informação no qual se inserem os eleitores (Jungherr, 2023, p.3-4). Ou seja, como as pessoas são expostas e podem acessar informações políticas, podem expressar suas opiniões e como essas bases informacionais potencialmente aumentam as oportunidades de manipulação. (Jungherr, 2023, p.4)

Apesar da inundação de informações existente no ambiente eleitoral, sua modelagem pela IA com base nas preferências ou comportamentos inferidos das pessoas permite tanto a criação de bolhas que ecoam a mesma opinião; quanto a exposição exagerada dos pontos de discordância, aumentando o conflito político (Jungherr, 2023, p.4). Aliada a isso, a manipulação da informação com IA pode afetar a autonomia informacional individual, mediante influências para mudança de opiniões e comportamentos com conteúdos fabricados (Jungherr, 2023, p.5).

Sobre este tema, estudos demonstram que a desinformação lidera o ranking de riscos globais no ano de 2024 (WEF, 2024, p. 18), atribuindo às interfaces fáceis de usar para modelos de IA e seu consequente uso em grande escala, fatores que contribuem para uma explosão de informações falsificadas e do chamado conteúdo “sintético”, desde a clonagem sofisticada de voz até sites falsificados (WEF, 2024, p. 18). A alta colocação neste ranking decorre (i) da presença de desinformação em processos eleitorais pode desestabilizar seriamente a legitimidade real e percebida dos governos recém-eleitos e (ii) de que a desinformação é cada vez mais personalizada e direcionada a grupos específicos, como comunidades minoritárias, além de ser disseminada por meio de plataformas de mensagens mais opacas, tornando difícil o discernimento não apenas para indivíduos alfabetizados digitalmente, mas também para mecanismos de detecção (WEF, 2024, p. 19). Sobre este último ponto, ainda que a própria IA possa auxiliar na identificação de destes conteúdos falsos para impedir sua divulgação, o fato de não serem objetivos ou estáveis e exigirem interpretação dificulta a atuação automatizada, correndo o risco de suprimir o discurso político legítimo (Jungherr, 2023, p.5).

Outro impacto à democracia está relacionado à parcialidade e à imparcialidade da IA usada nas eleições, e o reforço de vieses preexistentes (Chennupati, 2024, p.31). A

democracia depende de as pessoas terem direitos iguais de participação e representação, e na medida em que confiança da IA em dados que documentam o passado, corre-se o risco de dar continuidade à discriminação do passado no futuro, enfraquecendo assim a democracia. (Jungherr, 2023, p.7). A partir disso, pode-se considerar que representações da opinião pública baseadas em IA e o corpo político sejam tendenciosos contra grupos marginalizados no passado; aumentem a influência democrática de alguns grupos e diminuam a de outros; contribuam para o aumento de recursos para os já privilegiados, tornando suas vozes, interesses, atitudes, preocupações e queixas mais visíveis e acessíveis aos tomadores de decisão, ignorando as preferências de grupos menos visíveis (Jungherr, 2023, p.7).

Ainda, em relação a igualdade entre candidatos também é problematizada. As mudanças tecnológicas têm efeitos sobre a competição política, na medida em que permite o favorecimento assimétrico de atores ou grupos, dependendo de seu alinhamento ou desalinhamento com as possibilidades que emergem da tecnologia do momento (Jungherr, 2023, p.2).

Somam-se a este conjunto os impactos à acessibilidade e à inclusão em locais cujas desigualdades sociais possibilitam o risco de excluir pessoas e das oportunidades de votar com uso de tecnologias devido à falta de alfabetização digital e de acesso justo à tecnologia (Chennupati, 2024, p.31). Por exemplo, o Brasil se manteve como um dos 10 países mais desiguais do planeta, cujas desigualdades de gênero, raça/etnia e renda continuam a gerar exclusão social, pobreza, injustiça e violação sistemática dos direitos humanos (De Oliveira, 2024, p.14).

Como último impacto deste levantamento, cabe mencionar a quebra de confiança no processo democrático. O conhecimento escasso ou insuficiente sobre IA pode causar desconfiança na população sobre o uso de IA nas eleições, já que as pessoas precisam entender seus benefícios, riscos e limitações. As preocupações éticas de transparência e explicabilidade incluem informações sobre o funcionamento dessas tecnologias frente a questionamentos sobre proteção de sua privacidade e de seus dados, bem como o receio da vigilância dos eleitores (Chennupati, 2024, p.31). Por outro lado, a confiança de eleitores na integridade do processo eleitoral também tem como ponto chave a segurança da IA, especialmente ao considerar que sistemas de votação dependentes de IA podem ser suscetíveis a ataques cibernéticos, o que compromete a legitimidade das eleições (Chennupati, 2024, p.31).

Para análise legislativa, considera-se como ponto de partida, o principal e pioneiro padrão intergovernamental sobre IA: a recomendação sobre IA adotada pelo conselho da

Organização para a Cooperação e Desenvolvimento Econômico (OCDE). Esta recomendação foi adotada em 22 de maio de 2019 sob proposta do Comitê de Política Digital e revisada em 8 de novembro de 2023, focando em promover a inovação e a confiança na IA, ao mesmo tempo em que garante o respeito aos direitos humanos e valores democráticos (OCDE, 2024).

Para alcançar este propósito, a recomendação da OCDE parte da constituição de cinco princípios para uma IA confiável, sendo eles: a promoção do crescimento inclusivo, desenvolvimento sustentável e bem-estar, buscando resultados benéficos para as pessoas e o planeta e reduzindo desigualdades; o respeito pelo Estado de direito, os direitos humanos e os valores democráticos, garantindo justiça, privacidade e combate à desinformação; a transparência e explicabilidade, informando o funcionamento dos sistemas e permitindo entendimento e contestação de resultados por aqueles afetados; a robustez, segurança e proteção, prevenindo danos e preservando a integridade do sistema; e a responsabilidade, garantindo responsabilização pelo funcionamento, além da rastreabilidade e gestão de riscos.

Como diretrizes da OCDE para políticas nacionais e cooperação internacional para uma IA confiável, destaca-se que governos devem: investir em pesquisa e desenvolvimento de IA; incentivar um ecossistema inclusivo e sustentável para IA, facilitando o compartilhamento ético e seguro de dados; criar um ambiente regulatório flexível para o desenvolvimento e operação de IA confiável; preparar a sociedade para a transformação do trabalho com IA; incentivar a cooperação internacional, mediante compartilhamento de conhecimento e desenvolvimento de padrões técnicos globais.

Tanto os princípios quanto as diretrizes são observadas internacionalmente por formuladores de políticas públicas e reguladores, assim como por organizações que desenvolvem, implementam e adquirem sistemas de IA pelo mundo. Nota-se como tendência para regulação de IA e governança de IA uma abordagem ética e responsável.

A nível nacional, destaca-se que o tema não é um campo alheio ao ordenamento jurídico brasileiro, posto que o Brasil já possui importantes iniciativas de regulação a nível nacional. Contudo, pretende-se com esta pesquisa aprofundar a abordagem regulatória atual e as oportunidades de associação aos princípios internacionais para a IA ética e confiável.

Atualmente, o Brasil possui um Projeto de Lei (PL) em andamento, que dispõe sobre o uso da IA: o PL nº 2.338/2023. Este não foi o primeiro projeto de lei a discutir o tema, todavia é considerado como o mais relevante por concentrar as disposições das principais proposituras sobre IA nas casas legislativas no Brasil. Atualmente, o PL nº 2.338/2023 é acompanhado pela Comissão de Juristas (CJSUBIA) e pela Comissão Temporária Interna

sobre Inteligência Artificial no Brasil (CTIA), e teve seu texto aprovado pelo Senado em dezembro de 2024, aguardando o trâmite legislativo na Câmara dos Deputados.

Enquanto o Brasil carece de regulação específica sobre IA, faz-se mister considerar demais legislações aplicáveis à problemática em discussão. O ordenamento jurídico brasileiro conta com dispositivos que acomodam a vedação de disseminação de informações falsas que resultem em danos a qualquer pessoa, em que pese não haver marco regulatório específico para lidar com casos em que a desinformação afeta o processo eleitoral (Rubio; Monteiro, 2023, p.499), especialmente com o envolvimento de IA para tanto.

De toda forma, desde 2018 se intensificaram as ações de reguladores no Brasil sobre a desinformação, como o lançamento do “Programa de Combate à Desinformação” pela Justiça Eleitoral. E em razão das ameaças à integridade do processo eleitoral no Brasil, tendo na eleição de 2022 o elevado envolvimento de vários atores e *bots* (robôs) lançando mensagens coordenadas por meio de diferentes plataformas ao mesmo tempo, em verdadeiros ecossistemas de desinformação (Rubio; Monteiro, 2023, p.497), o Tribunal Superior Eleitoral (TSE) se mostrou atuante para regular o uso de tecnologias que trouxesse efeito nocivo às eleições.

No exercício de sua competência regulamentar, que encontra previsão no Código Eleitoral (artigos 1º e 23, IX), o TSE editou resoluções relevantes sobre o tema (Rubio; Monteiro, 2023, p.500). Ao alterar a Resolução nº 23.610/2019, que trata de propaganda eleitoral, o Tribunal incluiu em 2024, de maneira inédita, diversas novidades que envolvem a inteligência artificial, dentre elas: (i) a proibição das *deepfakes*; (ii) a obrigação de aviso sobre o uso de IA na propaganda eleitoral; (iii) a restrição do emprego de robôs para intermediar contato com o eleitor (de modo que não se permite a simulação de diálogo com candidato ou qualquer outra pessoa); e (iv) responsabilização das empresas de tecnologia e redes sociais (*Big Techs*) que não retirarem do ar, imediatamente, conteúdos com desinformação, discurso de ódio, ideologia nazista e fascista, além dos antidemocráticos, racistas e homofóbicos.

Adicionalmente, há que se destacar que os esforços da Justiça Eleitoral no combate à desinformação frente ao uso de tecnologias em campanhas eleitorais também alcançaram o campo da cooperação internacional. Iniciativas como a participação em missões de observação eleitoral no México, na Costa Rica ou na Colômbia, e uma missão técnica realizada em parceria com a União Europeia, ajudaram Brasil a se conectar com as práticas mais modernas e a garantir que seu plano fosse elaborado de forma bastante realista e adaptado às últimas tendências e necessidades. (Rubio; Monteiro, 2023, p.502).

OPACIDADE ALGORÍTMICA: DE PROBLEMA TÉCNICO A ESTRATÉGIA POLÍTICA

A opacidade algorítmica, segundo Burrell (2016, p. 19), diz respeito acerca da “*readability*” do código. Nesse contexto, Mittelstadt *et al* (2016, p. 3) elucida que “as tarefas realizadas pelo aprendizado de máquina são difíceis de prever antecipadamente (como uma nova entrada será tratada) ou de explicar posteriormente (como uma determinada decisão foi tomada)”.

A opacidade algorítmica é classificada por Burrell (2016) em três grandes categorias: (i) opacidade como segredo corporativo ou estatal intencional, (ii) opacidade como analfabetismo técnico e (iii) uma opacidade a partir da complexidade das operações internas dos sistemas de IA.

Sob a perspectiva da opacidade algorítmica, a transparência é frequentemente defendida como fundamental à construção de sistemas de inteligência artificial éticos e confiáveis. O resultado esperado é que, a partir da observação do funcionamento dos algoritmos, seja possível garantir a auditabilidade, a responsabilização e a proteção de direitos fundamentais frente à atuação de sistemas automatizados. Isto é, quanto mais transparência, maior o controle e a proteção sobre o funcionamento de algoritmos

Simultaneamente, entretanto, emerge um fenômeno paradoxal: quanto maior a transparência sem salvaguardas, maior pode ser a capacidade de agentes mal-intencionados explorarem as vulnerabilidades algorítmicas para manipular eleições.

Denominado “paradoxo da transparência algorítmica”, esse fenômeno revela-se especialmente grave no ambiente político-eleitoral, ora tratado neste trabalho (Burt, 2019).

Nesse sentido, Pasquale (2014, p. 141) argumenta que, embora a transparência seja muitas vezes desejada, a exposição do código dos algoritmos pode, em alguns casos, torná-los ineficazes. Sugere, então, que mesmo que as empresas fossem obrigadas a expor o design de seus algoritmos, isso poderia dificultar a eficácia dos mesmos. Isto é, a publicização do código-fonte pode contribuir para que pessoas mal intencionadas, como hackers ou golpistas, encontrem vulnerabilidades e as utilizem para fins manipulativos.

Kosinski e Stillwell (2017) asseveram que a exposição pública dos critérios de funcionamento dos algoritmos de ranqueamento e personalização pode ser utilizada por grupos organizados para otimizar estratégias de *microtargeting* psicológico, fragmentando o espaço público e ampliando a polarização. Em vez de apenas permitir auditoria democrática, a

transparência indiscriminada pode aprimorar a eficiência da manipulação informacional. Da mesma forma, Brunton e Nissenbaum (2015) sustentam que sistemas expostos integralmente à luz pública tornam-se suscetíveis àquilo que chamam de *gameability*: a habilidade de atores externos "jogarem contra o próprio sistema", utilizando suas regras conhecidas para produzir efeitos adversos.

Em processos eleitorais, as situações descritas ampliam a disseminação de desinformação, o impulsionamento de *fake news* e a radicalização política direcionada.

Aliás, tais técnicas de fato já foram utilizadas, causando impactos homéricos na sociedade, vide o caso Cambridge Analytica, nas eleições estadunidenses de 2014. Na ocasião, a empresa usou técnicas de perfilamento psicológico baseadas em pequenos sinais públicos para manipular preferências eleitorais — quanto mais detalhes tinham sobre o funcionamento do sistema de anúncios do Facebook, mais eficientes se tornaram. Já nas eleições de 2020, observou-se que campanhas de desinformação russa e doméstica aproveitaram transparências parciais dos sistemas de ranqueamento para burlar moderação e amplificar conteúdo tóxico.

Nesse cenário, é certo que a proposta de governança algorítmica para democracias digitais demanda a superação da transparência como solução universal. Em vez disso, torna-se necessário pensar em transparência segura, pautada na abertura seletiva de informações para auditorias independentes, proteção de segredos industriais legítimos e prevenção ativa de estratégias de manipulação eleitoral.

DA MANIPULAÇÃO ALGORÍTMICA AO RISCO SISTÊMICO INFORMACIONAL

Como demonstrado, a manipulação algorítmica emerge como uma estratégia sofisticada de influência política nas democracias digitais contemporâneas. Diferentemente de formas tradicionais de persuasão, a manipulação algorítmica opera de maneira invisível, utilizando algoritmos de filtragem, ranqueamento e recomendação para modificar a exposição informacional dos cidadãos (Jungherr, 2023). Em ambientes digitais dominados por plataformas como redes sociais e buscadores, a arquitetura algorítmica transforma o espaço público em terreno fértil para ações de manipulação informacional.

O ambiente digital é permeado por algoritmos que organizam, selecionam e amplificam conteúdos de acordo com critérios comerciais de maximização de engajamento (Pariser, 2011). Essa lógica cria não apenas bolhas informacionais, mas também um ambiente altamente manipulável, no qual *microtargeting* político, amplificação de discursos extremistas

e disseminação seletiva de informações tornam-se práticas recorrentes (Kosinski; Stillwell, 2017; Tufekci, 2015).

Esse cenário da manipulação algorítmica engendra verdadeiro efeito cascata. Inicialmente, pequenas distorções no fluxo de informação — como a promoção de *fake news* ou conteúdos polarizadores — parecem inofensivas. No entanto, dado o alcance exponencial de viralização dos algoritmos, essas distorções são rapidamente amplificadas em larga escala. Como evidenciado nos estudos sobre contágio em redes (Gai; Kapadia, 2010), o ambiente digital possibilita que choques locais evoluam para disfunções sistêmicas, desestabilizando o tecido social e a confiança institucional.

Um dos fenômenos mais preocupantes resultantes dessa dinâmica é a desinformação massiva. A facilidade de circulação de conteúdos falsos, aliados aos incentivos algorítmicos para promoção de narrativas emocionalmente apelativas, gera um cenário onde a verdade factual perde terreno frente à viralização de discursos fabricados (Ferraz; Alcoforado, 2024). O resultado é a corrosão da capacidade do cidadão de fazer escolhas informadas, comprometendo a legitimidade do processo democrático.

Consequentemente, o sistema político é acometido por uma crise de confiança pública e do pleno exercício de voto e de direitos dos cidadãos. Como observa Dalton (2005), a confiança é um recurso essencial para a estabilidade democrática; sua erosão leva à deslegitimação de eleições, da mídia tradicional, e das instituições representativas. Em ambiente saturado por desinformação, eleitores tornam-se céticos em relação às informações recebidas e suscetíveis à radicalização.

A vulnerabilidade eleitoral torna-se uma expressão prática do risco sistêmico informacional. De acordo com o Global Risks Report 2024 (WEF, 2024), a desinformação massiva foi classificada como um dos principais fatores de instabilidade global, justamente por sua capacidade de sabotar processos democráticos inteiros. Isto é, a fragilidade informacional e a manipulação são capazes de provocar impactos globais, alterando resultados eleitorais, afetando diretamente a estabilidade política e a governança democrática e comprometendo a governabilidade futura ao instaurar a dúvida sobre a validade das instituições democráticas. A natureza interconectada das plataformas digitais garante que crises locais de informação possam rapidamente adquirir dimensão transnacional, erodindo a legitimidade eleitoral e institucional e culminando em um latente risco sistêmico informacional.

REGULAÇÃO E GOVERNANÇA ANTI-MANIPULAÇÃO

Apesar dos avanços legislativos internacionais e nacionais na tentativa de regulamentar o uso da inteligência artificial (IA), os modelos atuais de transparência enfrentam limites importantes diante da complexidade e dos riscos sistêmicos associados à manipulação algorítmica em processos eleitorais.

No contexto brasileiro, o Projeto de Lei nº 2.338/2023 propõe incorporar fundamentos éticos e democráticos para o desenvolvimento e o uso da IA, inspirando-se nos princípios da OCDE. Embora importante, o projeto também herda as limitações de foco na transparência como solução primária, deixando lacunas na previsão de instrumentos para enfrentamento da manipulação informacional ativa e da captura do espaço público digital (Brasil, 2023).

Diante desse cenário, torna-se imprescindível a adoção de estratégias de governança para a resiliência democrática. Isso implica o desenvolvimento de políticas públicas focadas não apenas na transparência algorítmica, mas também na detecção, mitigação e responsabilização da manipulação informacional. Em suma, enfrentar o risco sistêmico informacional exige uma abordagem abrangente que reconheça a manipulação algorítmica como uma ameaça estrutural à sobrevivência da democracia.

Isto é, evidencia-se a necessidade de evolução do paradigma regulatório, não bastando exigir transparência *ex post* ou notificações genéricas ao usuário, mas sim a criação de modelos regulatórios baseados em governança anti-manipulação ativa, o que requer a adoção de mecanismos mais robustos e preventivos.

Assim, justifica-se a criação e adequação de instrumentos visando garantir a integridade dos processos democráticos, e combater a manipulação, especialmente no âmbito eleitoral. Sem a implementação de medidas, os esforços regulatórios tendem a ser insuficientes para conter os efeitos cascata da manipulação algorítmica sobre a democracia. Assim, a governança anti-manipulação se coloca como condição necessária para a proteção efetiva dos processos eleitorais na sociedade informacional.

Nesse sentido, destacam-se as auditorias de risco para sistemas de IA aplicados à política e eleições, com ênfase em impacto informacional e riscos de manipulação de opinião pública, a ser realizadas por entidades independentes e registradas junto a autoridades eleitorais e de proteção de dados. A rastreabilidade algorítmica também pode surtir efeitos positivos, exigindo que as plataformas e desenvolvedores de IA documentem fluxos de dados,

critérios de ranqueamento e decisões de modulação de conteúdo, de forma a permitir investigações posteriores e responsabilização.

Nada obstante, destaca-se a imposição de deveres proativos de candidatos e partidos políticos, incluindo a obrigação de reportar o uso de sistemas algorítmicos em campanhas, identificar conteúdos sintéticos ou personalizados, e garantir a conformidade com princípios de veracidade, igualdade de oportunidades e integridade democrática.

Isto é, faz-se necessário refletir sobre a estruturação de um modelo de governança que combine transparência regulada, auditorias independentes obrigatórias e mecanismos de controle prévio sobre a exposição pública dos sistemas, especialmente na esfera sensível das eleições, para enfrentamento do paradoxo da transparência algorítmica.

CONCLUSÕES

Ao longo deste trabalho, evidenciou-se que a opacidade algorítmica constitui um grande desafio à preservação da democracia. O ambiente eleitoral digital, mediado por sistemas automatizados de filtragem, ranqueamento e recomendação de informações, tornou-se terreno fértil para práticas de manipulação invisível, comprometendo diretamente a formação da vontade popular e a igualdade de oportunidades entre candidatos.

Conforme discutido, a opacidade dos algoritmos não decorre apenas da complexidade técnica, mas também de uma utilização estratégica voltada a dificultar a fiscalização, ocultar a modulação de conteúdos e viabilizar campanhas de desinformação massiva. Essa manipulação silenciosa dos fluxos informacionais gera efeitos em cascata, minando a confiança pública, polarizando o debate político e fragilizando a legitimidade dos resultados eleitorais.

As eleições, enquanto expressão máxima da soberania popular, tornam-se particularmente vulneráveis diante de mecanismos opacos de influência, que operam abaixo do limiar da percepção cidadã e à margem dos instrumentos tradicionais de controle jurídico-eleitoral. A disseminação de notícias falsas, a segmentação discriminatória de públicos e o direcionamento opaco de conteúdos políticos são práticas que afetam não apenas a liberdade de escolha, mas a própria integridade do processo democrático.

Neste cenário, fica claro que soluções baseadas exclusivamente na transparência formal dos algoritmos são insuficientes para conter a manipulação informacional. Faz-se necessária a adoção de uma governança anti-manipulação algorítmica, que imponha deveres proativos de rastreabilidade, auditorias de risco informacional e responsabilidade objetiva a

plataformas digitais e agentes políticos. Tais medidas devem ser orientadas por princípios constitucionais como o pluralismo político, a igualdade no processo eleitoral e o direito à informação verdadeira.

A defesa da democracia na sociedade informacional exige, portanto, a superação da opacidade como barreira técnica e estratégica, e a consolidação de instrumentos jurídicos que preservem o espaço público digital como arena livre, plural e acessível de deliberação política. A proteção das eleições contra a manipulação algorítmica não é apenas uma necessidade técnica ou regulatória: é uma exigência democrática fundamental.

REFERÊNCIAS

ALCOFORADO, A.; FERRAZ, T. P.; BUSTOS, E.; OLIVEIRA, A. S.; GERBER, R.; SANTORO, G. L. DU M.; FAMA, I. C.; VELOSO, B. M.; SIQUEIRA, F. L.; COSTA, A. H. R. Democracia aumentada: inteligência artificial como ferramenta de combate à desinformação. **Estudos Avançados**, v. 38 (111), p. 407-426, 2024. DOI: 10.1590/s0103-4014.202438111.021. Disponível em: <https://www.scielo.br/j/ea/a/nXMjhFNh5PGYcQ9f8hzVr3f/?format=pdf&lang=pt>. Acesso em: 10 abr. 2025.

BRUNTON, F.; NISSENBAUM, H. Obfuscation: A User's Guide for Privacy and Protest. **MIT Press**, 2015.

BURRELL, Jenna. How the machine 'thinks': Understanding opacity in machine learning algorithms. **Big Data & Society**, v. 3, n. 1, 2016. Disponível em: <https://journals.sagepub.com/doi/full/10.1177/2053951715622512>. Acesso em: 27 abr. 2025.

BURT, Andrew. The AI transparency paradox. **Harvard Business Review**, 2019. Disponível em: <https://hbsp.harvard.edu/product/H05BRU-PDF-ENG>. Acesso em: 27 abr. 2025.

CARLSSON, V.; RÖNNBLÖM, M. From politics to ethics: transformations in EU policies on digital technology. **Technology in Society**, v. 71, p. 1-8, 2022. DOI: 10.1016/j.techsoc.2022.102145. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0160791X2200286X>. Acesso em: 10 abr. 2025.

CHENNUPATI, A. The threat of artificial intelligence to elections worldwide: a review of the 2024 landscape. **World Journal of Advanced Engineering Technology and Sciences**, v. 12, n. 1, p. 29-34, 2024. DOI: 10.30574/wjaets.2024.12.1.0177. Disponível em: <https://wjaets.com/content/threat-artificial-intelligence-elections-worldwide-review-2024-landscape>. Acesso em: 10 abr. 2025.

DALTON, Russell J. Democratic Challenges, Democratic Choices. **Oxford University Press**, 2005.

DE OLIVEIRA, N. H. A decolonial critical theory of artificial intelligence: intersectional egalitarianism, moral alignment, and AI governance. **Unisinos Journal of Philosophy**, v. 25, n. 1, p. 1-18, 2024. DOI: 10.4013/fsu.2024.251.14. Disponível em: <https://www.scielo.br/j/fun/a/g5MwkPjfQfZ4m3Mf59CNJnk/?format=pdf&lang=en>. Acesso em: 10 abr. 2025.

GAI, Prasanna; KAPADIA, Sujit. Contagion in financial networks. **Proceedings of the Royal Society A**, v. 466, n. 2120, p. 2401–2423, 2010. Disponível em: <https://royalsocietypublishing.org/doi/10.1098/rspa.2009.0410>. Acesso em 27 abr. 2025.

JUNGHERR, Andreas. Artificial Intelligence and Democracy: A Conceptual Framework. **Social Media + Society**, v. 9, n. 3, p. 1-14, 2023. DOI: 10.1177/20563051231186353. Disponível em: <https://journals.sagepub.com/doi/epub/10.1177/20563051231186353>. Acesso em: 10 abr. 2025.

KOSINSKI, Michal; STILLWELL, David. Psychological targeting as an effective approach to digital mass persuasion. **Proceedings of the National Academy of Sciences**, 2017. Disponível em: <https://www.pnas.org/doi/10.1073/pnas.1710966114>. Acesso em: 27 abr. 2025.

OCDE - Organisation for Economic Co-operation and Development. Recommendation of the Council on Artificial Intelligence. **OECD/LEGAL/0449**, adotado em 21 mai. 2019 e revisado em 02 mai. 2024. Disponível em: <https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449> Acesso em: 10 abr. 2025.

PARISER, Eli. The Filter Bubble: What the Internet Is Hiding from You. **Penguin Press**, 2011.

PASQUALE, Frank. The Black Box Society: The Secret Algorithms that Control Money and Information. **Cambridge: Harvard University Press**, 2015.

RAHWAN, Iyad. Society-in-the-loop: programming the algorithmic social contract. **Ethics and Information Technology**, v. 20, p. 5–14, 2018. Disponível em: <https://doi.org/10.48550/arXiv.1707.07232>. Acesso em 27 abr. 2025.

RODRIGO LÓPEZ, J. F. Tragic realism: how to regulate deepfakes in Colombia?. **Latin American Law Review**, v. 1, n. 8, p. 125-145, 2022. DOI: 10.29263/lar08.2022.08. Disponível em: <https://revistas.uniandes.edu.co/index.php/lar/article/view/4715>. Acesso em: 10 abr. 2025.

RUBIO, R.; MONTEIRO, V. de A. Preserving trust in democracy: the Brazilian Superior Electoral Court's quest to tackle disinformation in elections. **South African Journal of International Affairs**, v. 30, n. 3, p. 497-520, 2023. DOI: 10.1080/10220461.2023.2274860. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/10220461.2023.2274860>. Acesso em: 10 abr. 2025.

TUFEKCI, Zeynep. Algorithmic harms beyond Facebook and Google: emergent challenges of computational agency. **Colorado Technology Law Journal**, 2015. Disponível em: <https://scholar.law.colorado.edu/ctlj/vol13/iss2/4/>. Acesso em 27 abr. 2025.

UNIÃO EUROPEIA. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho. Cria regras harmonizadas em matéria de inteligência artificial. **Bruxelas: União Europeia**, 2024. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=OJ:L_202401689. Acesso em: 10 abr. 2025.

WEF - WORLD ECONOMIC FORUM. In partnership with Marsh McLennan and Zurich Insurance Group. **The Global Risks Report 2024**. 19th edition, 10 jan. 2024. ISBN: 978-2-940631-64-3. Disponível em: <https://www.weforum.org/publications/global-risks-report-2024/in-full/>. Acesso em: 10 abr. 2025.