

INTELIGÊNCIA ARTIFICIAL E A INTERSEÇÃO ENTRE RISCOS, VIOLÊNCIA E REGULAÇÃO: UMA REVISÃO INTEGRATIVA

ARTIFICIAL INTELLIGENCE AND THE INTERSECTION OF RISKS, VIOLENCE, AND REGULATION: AN INTEGRATIVE REVIEW

INTELIGENCIA ARTIFICIAL Y LA INTERSECCIÓN ENTRE RIESGOS, VIOLENCIA Y REGULACIÓN: UNA REVISIÓN INTEGRATIVA

Sabryna Feitosa Ferreira do Amaral Freire ¹, Julia Moura de Miranda Coelho ², Arnaldo de França Caldas Junior ³, Luiz Gutenberg Toledo de Miranda Coelho Junior ⁴

DOI: 10.54899/dcs.v23i93.6317

Recibido: 24/07/2026 | Aceptado: 24/07/2026 | Publicación en línea: 10/08/2026.

RESUMO

A inteligência artificial (IA) consolidou-se como uma tecnologia estratégica em diferentes setores da sociedade, ao mesmo tempo em que suscita preocupações relacionadas aos riscos sociais, à violência digital e aos desafios regulatórios decorrentes de sua utilização. Este estudo teve como objetivo analisar a literatura científica publicada no período de 2022 a 2025 acerca da relação entre inteligência artificial, riscos sociais, violência digital e respostas regulatórias. Trata-se de uma revisão integrativa da literatura, desenvolvida a partir de buscas realizadas nas bases Scientific Electronic Library Online (SciELO) e Portal de Periódicos CAPES, utilizando descritores definidos pelo DeCS (Descritores em Ciências da Saúde) e combinados por operadores booleanos. Foram identificados 80 registros, dos quais 41 atenderam aos critérios de elegibilidade e compuseram a amostra final da revisão. Os resultados evidenciaram que a produção científica tem concentrado suas análises nos riscos sociais associados à inteligência artificial, nas diferentes manifestações de violência digital e nos desafios relacionados à construção de modelos regulatórios capazes de conciliar inovação tecnológica e proteção de direitos fundamentais. Conclui-se que a inteligência artificial, além de representar um vetor de inovação, tem sido associada à ampliação de riscos sociais e diferentes manifestações de violência digital, evidenciando a necessidade de abordagens integradas e de marcos regulatórios mais robustos, orientados à proteção de direitos fundamentais.

Palavras-chave: Inteligência Artificial. Riscos. Violência. Regulação.

¹ Mestranda em Perícia Forense, Faculdade de Odontologia de Pernambuco (FOP), Universidade de Pernambuco (UPE), Recife, Pernambuco, Brasil. E-mail: sabryna.amaralfreire@upe.br
Orcid: <https://orcid.org/0009-0004-2074-9884>

² Graduada em Odontologia, Faculdade de Odontologia de Pernambuco (FOP), Universidade de Pernambuco (UPE), Recife, Pernambuco, Brasil. E-mail: juliamouramc@gmail.com
Orcid: <https://orcid.org/0000-0003-0769-6760>

³ Doutor em Saúde Coletiva, Faculdade de Odontologia de Pernambuco (FOP), Universidade de Pernambuco (UPE), Recife, Pernambuco, Brasil. E-mail: arnaldo.caldas@upe.br Orcid: <https://orcid.org/0000-0002-3713-7532>

⁴ Doutor em Saúde Coletiva, Faculdade de Odontologia de Pernambuco (FOP), Universidade de Pernambuco (UPE), Recife, Pernambuco, Brasil. E-mail: luiz.gutenberg@upe.br Orcid: <https://orcid.org/0000-0002-2030-1092>

ABSTRACT

Artificial intelligence (AI) has become a strategic technology across different sectors of society while simultaneously raising concerns regarding social risks, digital violence, and the regulatory challenges arising from its use. This study aimed to analyze the scientific literature published between 2022 and 2025 on the relationship between artificial intelligence, social risks, digital violence, and regulatory responses. This study consists of an integrative literature review based on searches conducted in the Scientific Electronic Library Online (SciELO) and the CAPES Periodicals Portal, using descriptors defined by the Health Sciences Descriptors (DeCS) and combined through Boolean operators. A total of 80 records were identified, of which 41 met the eligibility criteria and comprised the final review sample. The findings showed that scientific production has focused its analyses on the social risks associated with artificial intelligence, the different manifestations of digital violence, and the challenges related to the development of regulatory frameworks capable of reconciling technological innovation with the protection of fundamental rights. It is concluded that artificial intelligence, in addition to representing a driver of innovation, has been associated with the expansion of social risks and different manifestations of digital violence, highlighting the need for integrated approaches and more robust regulatory frameworks aimed at protecting fundamental rights.

Keywords: Artificial Intelligence. Risks. Violence. Regulation.

RESUMEN

La inteligencia artificial (IA) se ha consolidado como una tecnología estratégica en diferentes sectores de la sociedad, al tiempo que suscita preocupaciones relacionadas con los riesgos sociales, la violencia digital y los desafíos regulatorios derivados de su utilización. Este estudio tuvo como objetivo analizar la literatura científica publicada entre 2022 y 2025 acerca de la relación entre la inteligencia artificial, los riesgos sociales, la violencia digital y las respuestas regulatorias. Se trata de una revisión integrativa de la literatura, desarrollada a partir de búsquedas realizadas en las bases de datos Scientific Electronic Library Online (SciELO) y el Portal de Periódicos CAPES, utilizando descriptores definidos por los Descriptores en Ciencias de la Salud (DeCS) y combinados mediante operadores booleanos. Se identificaron 80 registros, de los cuales 41 cumplieron los criterios de elegibilidad y conformaron la muestra final de la revisión. Los resultados evidenciaron que la producción científica ha concentrado sus análisis en los riesgos sociales asociados a la inteligencia artificial, en las diferentes manifestaciones de la violencia digital y en los desafíos relacionados con la construcción de marcos regulatorios capaces de conciliar la innovación tecnológica con la protección de los derechos fundamentales. Se concluye que la inteligencia artificial, además de representar un motor de innovación, ha sido asociada con la ampliación de los riesgos sociales y las diferentes manifestaciones de la violencia digital, poniendo de relieve la necesidad de enfoques integrados y de marcos regulatorios más sólidos, orientados a la protección de los derechos fundamentales.

Palabras clave: Inteligencia Artificial. Riesgos. Violencia. Regulación.



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

INTRODUÇÃO

A inteligência artificial (IA) consolidou-se como uma das tecnologias mais transformadoras da contemporaneidade, promovendo mudanças significativas nas relações sociais, econômicas e institucionais. Nos últimos anos, sua rápida evolução ampliou a incorporação de sistemas inteligentes ao cotidiano humano, redefinindo processos decisórios, automatizando atividades e expandindo a produção e o tratamento de informações em diferentes setores da sociedade. Conforme afirma Kasparov (2017), a ascensão da IA representa não apenas um avanço tecnológico, mas uma transformação paradigmática capaz de reconfigurar a relação entre humanos e máquinas.

Entretanto, esse desenvolvimento não ocorre em um contexto de neutralidade. Sob a perspectiva de Zuboff (2019), a contemporaneidade é marcada pelo denominado "capitalismo de vigilância", modelo fundamentado na extração massiva de dados pessoais sob a promessa de conveniência e eficiência, mas que frequentemente compromete direitos fundamentais e a autonomia dos indivíduos. Em perspectiva convergente, Crawford (2021) argumenta que sistemas de inteligência artificial podem reproduzir valores, interesses e padrões presentes nos contextos em que são desenvolvidos e utilizados, contribuindo para a ampliação de desigualdades e vulnerabilidades sociais.

Na ausência de marcos regulatórios robustos, a tecnologia tende a ser apropriada de maneira indiscriminada, permitindo que suas capacidades sejam utilizadas para a sofisticação de práticas ilícitas e para a precarização de direitos. Essa vulnerabilidade manifesta-se de forma particularmente crítica no fenômeno da violência digital. Ferramentas baseadas em IA, especialmente aquelas associadas à inteligência artificial generativa, têm viabilizado a disseminação estratégica de desinformação, fraudes baseadas em engenharia social e a criação de conteúdos manipulados por meio de *deepfakes* (UNESCO, 2024). A gravidade desse cenário é corroborada pelo Relatório de Riscos Globais (2024), do Fórum Econômico Mundial, que aponta a desinformação impulsionada por sistemas de inteligência artificial entre os principais desafios à estabilidade política e social contemporânea.

No contexto brasileiro, essa problemática evidencia-se por meio de ocorrências concretas, como o uso de vídeos manipulados em contextos eleitorais e a disseminação não consentida de material íntimo, prática que atinge predominantemente mulheres e adolescentes (Lima *et al.*, 2024; Rossel-Castagneto, 2025; Vargas-Chaves, 2025). Tais situações demonstram que a IA pode

potencializar práticas de desinformação, comprometer a integridade do debate público e intensificar formas de violência digital que afetam diretamente a dignidade, a identidade e a privacidade das vítimas (Lorca; García-Mingo, 2023; Bañuelos-Capistrán, 2024). Nesse sentido, Braga e Cardoso (2017) realçam que os algoritmos não são neutros e, quando operam de forma opaca e baseados em dados enviesados, podem institucionalizar desigualdades sociais, reforçando a necessidade de abordagens críticas sobre o uso e a regulação dessas tecnologias.

Diante desse cenário, observa-se o avanço de iniciativas regulatórias voltadas à construção de mecanismos capazes de compatibilizar inovação tecnológica, proteção de direitos fundamentais e segurança jurídica. Em âmbito internacional, destaca-se a aprovação do *Artificial Intelligence Act (AI Act)*, pelo Parlamento Europeu, em março de 2024, estabelecendo um marco regulatório baseado na classificação dos sistemas de inteligência artificial segundo níveis de risco, com exigências proporcionais relacionadas à transparência, à supervisão humana e à proteção de direitos fundamentais. Esse modelo tem sido apontado como uma das principais referências contemporâneas para a governança da inteligência artificial (Hoch; Engelmann, 2023; Matos, 2024; Butcher, 2024).

No Brasil, embora o uso da inteligência artificial tenha se expandido significativamente, ainda não existe uma lei geral que discipline de forma abrangente o desenvolvimento, a implementação e a utilização dessas tecnologias. O debate legislativo concentra-se principalmente nos Projetos de Lei nº 21/2020 e nº 2.338/2023, este último considerado a principal proposta voltada à regulamentação da inteligência artificial no país (Marcílio, 2025). Paralelamente, observa-se a consolidação de um modelo regulatório setorial, composto por instrumentos como a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), a Lei nº 15.123/2025, que agravou a pena do crime de violência psicológica contra a mulher quando praticado mediante o uso de inteligência artificial, a Lei nº 15.211/2025 (Estatuto Digital da Criança e do Adolescente), além dos Decretos Federais nº 12.975/2026 e nº 12.976/2026, voltados, respectivamente, à atualização da regulamentação do Marco Civil da Internet e ao fortalecimento das medidas de proteção de mulheres e meninas no ambiente digital (Brasil, 2018; Brasil, 2025; Brasil, 2026; Nunes, 2026; Martins; Barbosa, 2026).

Embora a produção científica sobre inteligência artificial tenha crescido significativamente nos últimos anos, observa-se que os estudos tendem a abordar de forma segmentada aspectos relacionados aos riscos sociais, à violência digital ou às respostas regulatórias, com limitada articulação entre essas dimensões. Tal fragmentação dificulta a

compreensão integrada do fenômeno, especialmente considerando que os riscos associados à inteligência artificial frequentemente se materializam em práticas de violência digital, as quais, por sua vez, demandam respostas regulatórias adequadas e eficazes.

Diante desse cenário, justifica-se a realização desta revisão integrativa, que tem como objetivo analisar a literatura científica publicada no período 2022 a 2025 acerca da inteligência artificial e a interseção com riscos sociais, violência digital e respostas regulatórias.

METODOLOGIA

O presente estudo consiste em uma revisão integrativa da literatura, por se tratar de um método amplo e abrangente que permite a inclusão de estudos com diferentes abordagens metodológicas, bem como documentos normativos e institucionais utilizados para contextualizar o cenário regulatório relacionado ao objeto de estudo. A revisão integrativa constitui um método que possibilita a síntese do conhecimento produzido sobre determinado tema, permitindo a reunião, análise crítica e integração de evidências científicas, de modo a proporcionar uma compreensão abrangente do fenômeno investigado (Souza *et al.*, 2010).

Para a condução da revisão, foram observadas as etapas propostas por Whittemore e Knafl (2005): (i) formulação da questão de pesquisa e dos objetivos da revisão; (ii) definição dos critérios para seleção dos estudos; (iii) categorização das produções incluídas; (iv) avaliação crítica dos estudos; (v) análise e síntese dos dados; e (vi) apresentação dos resultados.

A formulação da questão norteadora foi orientada pela estratégia PICO (*Population/Problem, Intervention, Comparison e Outcome*), adaptada à natureza teórica e interdisciplinar da pesquisa, de modo a contemplar a análise da relação entre inteligência artificial, riscos sociais, violência digital e respostas regulatórias. A questão norteadora da revisão consistiu em identificar **como a literatura científica publicada no período de 2022 a 2025 aborda inteligência artificial e a intercessão com os riscos sociais, violência digital e respostas regulatórias.**

As buscas foram realizadas nas bases Scientific Electronic Library Online (SciELO) e Portal de Periódicos CAPES, selecionadas por reunirem produção científica relevante nas áreas de interesse da pesquisa. Complementarmente, foram consultados documentos normativos e institucionais disponíveis nos portais oficiais do Governo Federal, Conselho Nacional de Justiça (CNJ), Jusbrasil e Migalhas por meio de busca livre, considerando sua relevância para

contextualizar o cenário regulatório da inteligência artificial, não compondo o corpus científico da revisão integrativa.

Os descritores foram definidos a partir do **DeCS (Descritores em Ciências da Saúde)**, em português, inglês e espanhol, sendo utilizados os termos "**inteligência artificial**", "**risco**", "**violência**" e "**regulamentação**", combinados por operadores booleanos, conforme apresentado na Tabela 1.

Tabela 1

Base consultada

Base de dados	Estratégia de busca
SciELO	"inteligência artificial AND risco"; "inteligência artificial AND violência"; "inteligência artificial AND regulamentação"
Periódicos CAPES	"inteligência artificial AND risco"; "inteligência artificial AND violência"; "inteligência artificial AND regulamentação"

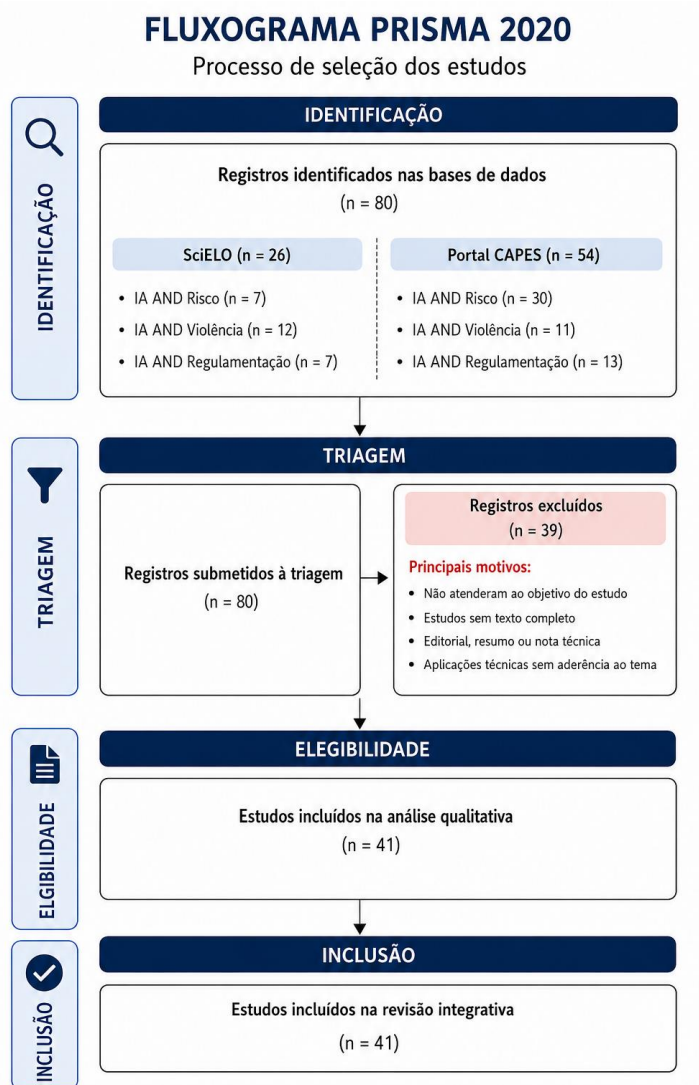
Fonte: Elaborado pela autora 2026

Os critérios de inclusão compreenderam estudos publicados no período de 2022 a 2025, disponibilizados na íntegra, revisados por pares, redigidos em português, inglês ou espanhol e diretamente relacionados à temática da pesquisa. Foram excluídos editoriais, resumos, notas técnicas, produções sem estrutura científica definida, estudos sem acesso ao texto completo e publicações que abordassem predominantemente aplicações técnicas ou setoriais da inteligência artificial, sem relação direta com os riscos sociais, a violência digital e as respostas regulatórias.

A seleção dos estudos ocorreu em conformidade com os critérios de elegibilidade previamente estabelecidos, sendo o processo sintetizado no **Fluxograma PRISMA 2020 (Figura 1)**.

Figura 1.

Fluxograma PRISMA 2020 do processo de seleção dos estudos.



Fonte: Elaborado pela autora 2026

Ao final do processo de busca durante o período de 2022 a 2025 foram identificados 80 registros, dos quais 39 foram excluídos por não atenderem aos critérios de elegibilidade, resultando em uma amostra final composta por 41 estudos incluídos na revisão integrativa.

RESULTADOS E DISCUSSÕES

Caracterização dos Estudos Incluídos - (n=41)

A busca realizada nas bases Scientific Electronic Library Online (SciELO) e Portal de Periódicos CAPES resultou na seleção de 41 estudos que atenderam aos critérios de elegibilidade estabelecidos para esta revisão integrativa. A caracterização da produção científica analisada é apresentada na Tabela 2.

Tabela 2

Caracterização da produção científica

SciELO -Inteligência Artificial AND Risco					
Nº	Autores/Ano	Título	Tipo de Estudo	Objetivo	Resultados
01	Ulloa Ruiz, Mónica A.; Graells, Guillem Bas (2025)	La securitización de la inteligencia artificial: un análisis de sus impulsores y sus consecuencias	Estudo qualitativo (análise crítica do discurso)	Identificar os fatores que impulsionam a securitização da IA e avaliar suas consequências na formulação de políticas públicas	Evidencia que a IA vem sendo tratada como questão de segurança, gerando respostas políticas baseadas em ameaça ou risco, com impactos na governança e na regulação
02	Sánchez-Bolívar, Lionel; Escalante-González <i>et al.</i> (2024)	La ética de la inteligencia artificial en educación: ¿Amenaza u oportunidad?	Estudo misto (revisão sistemática + análise qualitativa SWOT/DAFO)	Analisar os limites éticos do uso da inteligência artificial no contexto educacional	Identifica benefícios da IA no ensino, mas evidencia riscos como plágio e uso indevido, destacando a necessidade de limites éticos e normativos
03	Sanabria Moyano, Jesús E.; Roa Avella, Marcela <i>et al.</i> (2022)	Tecnología de reconocimiento facial y sus riesgos en los derechos humanos	Estudo qualitativo (análise documental e jurídico-descritiva)	Examinar o funcionamento do reconhecimento facial e seus impactos no direito penal e nos direitos humanos	Demonstra que o uso da IA em reconhecimento facial gera riscos ao devido processo, à privacidade e à não discriminação
Periódicos CAPES - Inteligência Artificial AND Risco					
04	Lemos & Espíndola (2024)	A questão algorítmica: a pós-verdade e a crise da democracia	Teórico/analítico	Analisar a relação entre algoritmos, pós-verdade e crise democrática	Evidencia que sistemas algorítmicos contribuem para desinformação e risco à democracia
05	Mota (2022)	Direito internacional humanitário e as	Revisão bibliográfica	Analisar a responsabilidade jurídica no uso de	Aponta riscos jurídicos e lacunas regulatórias no

		armas autônomas letais		armas autônomas com IA	uso de IA em contextos militares
06	Rossetti & Silva (2023)	Direitos Fundamentais no uso de Inteligência Artificial no Poder Judiciário brasileiro	Qualitativo jurídico	Analisar riscos do uso da IA no Judiciário brasileiro	Identifica riscos a direitos fundamentais, como privacidade e transparência
07	Miranda Jr. & Wilke (2024)	Institucionalidade, governamentalidade e inteligência artificial: democracia inteligente ou democracia artificial?	Teórico crítico	Analisar impactos da IA na democracia e governamentalidade	Evidencia riscos à democracia e manipulação social por meio de IA
08	Cambráia & Pyrrho (2024)	Inteligência artificial e injustiça	Teórico ético	Analisar desafios éticos da IA	Evidencia riscos de desigualdade e injustiça algorítmica
09	Leal & Paulo (2023)	Algoritmos discriminatórios e jurisdição constitucional	Jurídico	Analisar discriminação algorítmica	Demonstra riscos jurídicos e sociais da IA
10	Bergqvist <i>et al.</i> (2024)	Conluio por inteligência artificial	Teórico econômico	Analisar IA em práticas anticompetitivas	Indica risco de colusão e falhas regulatórias
11	Araújo & Cornacchione (2024)	IA na contabilidade gerencial	Qualitativo	Avaliar impactos da IA na contabilidade	Aponta riscos organizacionais e éticos
12	Cabral, J. P. G.; Rocha, H. F.; Souza, A. P. J.; Oliveira, D. J.; Lima, J. F. (2024)	Direito e tecnologia: o uso da inteligência artificial na justiça do trabalho	Qualitativo exploratório	Analisar impactos da IA na Justiça do Trabalho	Evidencia riscos relacionados à automação, falhas sistêmicas, segurança de dados e necessidade de regulação
13	Silveira, S. A. (2024)	Questões conjunturais sobre a regulação da IA	Teórico crítico	Analisar disputas regulatórias da IA	Aponta riscos sociais como concentração de poder, opacidade algorítmica e exclusão social
14	Pimentel, A. F.; Araújo, B. M. V.; Maciel, T. M. (2023)	Uma análise da “modernização reflexiva” e da “sociedade do risco”: o risco da aplicação da inteligência artificial nas minutas de decisões judiciais brasileiras	Teórico-jurídico	Analisar riscos da IA no Judiciário	Demonstra riscos decisórios e institucionais da IA em decisões judiciais

15	Siqueira, D. P.; Morais, F. S.; Tena, L. P. (2023)	Voz reproduzida por IA acelera reflexões sobre a necessidade da proteção da personalidade em ambiente virtual	Jurídico	Analisar impactos da IA na reprodução de voz	Evidencia riscos à personalidade, identidade e direitos fundamentais
SciELO - “Inteligência Artificial AND Violência”					
16	Stropparo, Pablo Ezequiel (2022)	El derecho a la libertad de expresión en Argentina. Estado de derecho, democracia y desacuerdos en el caso nodio	Teórico-analítico	Analisar política pública de combate à desinformação	Evidencia relação entre IA, desinformação e violência simbólica
17	Coddou Mc Manus, Alberto <i>et al.</i> (2025)	IA y violencia contra las mujeres: la automatización de la evaluación del riesgo	Qualitativo jurídico	Analisar uso de IA na avaliação de risco de violência de gênero	IA melhora proteção, mas gera riscos a direitos fundamentais
18	Roa Avella, Marcela del Pilar <i>et al.</i> (2023)	Los estándares internacionales de protección de la Violencia Basada en Género de las mujeres aplicados a la Inteligencia Artificial predictiva	Qualitativo	Analisar IA na proteção contra violência de gênero	IA contribui à proteção, mas apresenta desafios jurídicos
19	Gaal Fong, Juan Carlos <i>et al.</i> (2022)	Manipulación ideológica en redes sociales: acoso, engaño y violencia en el entorno digital	Qualitativo	Analisar uso de bots e IA na manipulação digital	IA amplifica discurso de ódio e violência digital
20	Santillán-Molina, Alberto Leonel <i>et al.</i> (2025)	Política de inteligencia artificial y protección en violencia de género para garantizar tutela judicial efectiva	Jurídico	Analisar uso de IA na proteção judicial	IA acelera proteção, mas exige cautela institucional
21	Lorca, Jacinto G.; García-Mingo, Elisa (2023)	Comunidades digitales misóginas de difusión de imágenes sexuales sin consentimiento	Qualitativo	Analisar comunidades digitais	IA facilita violência sexual digital
22	Rossel-Castagneto, María Lorena (2025)	Regular el odio digital: entre la libertad de expresión y la protección de	Jurídico	Analisar discurso de ódio	IA amplia violência estrutural

		colectivos vulnerables			
23	Vargas-Chaves, Iván (2025)	Take It Down Act: un análisis crítico de su rol contra la difusión no consentida de imágenes y deepfakes	Jurídico	Avaliar lei	Regulação limitada frente à violência digital
Periódicos CAPES - “Inteligência Artificial AND Violência”					
24	Roa Avella, Marcela del Pilar; Santofimio Moyano, Jesús Eduardo; Hurtado, Katherine Dinas (2023)	Herramientas de predicción de violencia basada en género y feminicidio mediante la Inteligencia Artificial	Qualitativo jurídico	Analisar uso de IA na predição de violência de gênero	IA permite previsão de risco, mas apresenta limitações metodológicas e riscos de viés
25	Mendes, Isabelle Brito Bezerra (2022)	Inteligência artificial e violência doméstica: a garantia à integridade física por meio da relativização da privacidade	Jurídico	Analisar uso de IA na prova e combate à violência doméstica	IA (assistentes virtuais) pode auxiliar no combate à violência, com tensão entre privacidade e proteção
26	Turetta, Denise Futumi <i>et al.</i> (2024)	Curadoria de dados na prevenção da violência contra a mulher: uma análise crítica	Revisão narrativa	Analisar curadoria de dados na prevenção da violência	IA contribui para prevenção, mas apresenta riscos de viés e exclusão de dados
27	Martínez Suárez, Yolanda (2024)	Opresión, desigualdad e inteligencia artificial	Teórico crítico	Analisar IA sob perspectiva de desigualdade e violência estrutural	IA reproduz desigualdades e formas estruturais de violência
SciELO - “Inteligência Artificial AND Regulamentação”					
28	Cajahuanca Cadillo, Gersíño Walter (2025)	Ciencias jurídicas en la era digital: revisión sistemática sobre innovaciones y desafíos legales actuales	Revisão sistemática	Analisar impacto da IA no Direito	Necessidade de atualização normativa e proteção de direitos digitais
29	Estrella Tutivén, Ingrid Viviana; Garde Cano, Cristina (2025)	Ética Jornalística na Era da Inteligência Artificial: Rumo a uma Atualização dos Códigos Deontológicos no	Qualitativo	Atualizar princípios éticos e regulatórios	Necessidade de regulação equilibrada e ética

		Contexto Ibero-Americano			
30	Londoño Villarreal, Luis Felipe (2025)	Guía de cumplimiento: regulación de IA generativa en asesoría jurídica por chatbot en Colombia	Normativo comparado	Analisar regulação de chatbots jurídicos	Necessidade de avaliação de risco, transparência e proteção de dados
31	Bedregal Aguilar, Alex David (2025)	¿Justicia automatizada? Estudio de la interdisciplinariedad de la inteligencia artificial y el derecho en la administración de justicia	Teórico jurídico	Analisar IA no Judiciário	Necessidade de diretrizes regulatórias para uso adequado
32	Medina Romero, Miguel Ángel; Torres Chávez, Tania Haidée (2025)	Regulación de la Inteligencia Artificial: Desafíos para los Derechos Humanos en México	Qualitativo jurídico	Analisar IA e direitos humanos	Lacunas regulatórias e riscos à privacidade e não discriminação
Portal de Periódicos CAPES - “Inteligência Artificial AND Regulamentação”					
33	Rafael Gonçalves Mota (2022)	Direito internacional humanitário e as armas autônomas letais	Revisão	IA em conflitos	Lacuna regulatória internacional
34	Milton Pereira de França Netto, Gustavo Ferreira Santos, Alexandre Freire Pimentel (2024)	O desafio da regulação das deepfakes	Qualitativo	Deepfakes	Necessidade de regulação específica
35	Hérica Cristina Paes Nascimento, Maíque Barbosa de Souza, Patrícia Da Silveira Oliveira (2021)	A regulação da inteligência artificial e novos contornos para caracterização da responsabilidade civil	Teórico	IA e responsabilidade	Novos parâmetros jurídicos
36	Stephanny Resende de Melo, Clara Cardoso Machado	Algoritmos raciais e o pensamento de colonialidade como entrave aos direitos humanos: uma nova forma de	Qualitativo	IA e discriminação	Necessidade de regulação ética

	Jaborandy (2023)	estruturação das discriminações raciais			
37	Renascha Gabrielly Soares Lima, Helton Carlos Praia de Lima, Alyson de Jesus dos Santos (2024)	Contramedidas ao uso de inteligência artificial por meio de deepfakes como ferramenta de desinformação política no processo eleitoral brasileiro	Revisão	IA eleitoral	Necessidade de regulação
38	Marcelo Amaral de Matos (2024)	Inteligência artificial e sua regulamentação	Teórico	IA e legislação	Regulação impacta adoção
39	Jaqueline da Silva Paulichi, Matheus Ribeiro de Oliveira Wolowski (2021)	O dilema jurídico da propriedade intelectual na inteligência artificial: a máquina poderá ser titular de direito autoral?	Teórico	Direito autoral	Lacuna normativa
40	Patrícia Adriani Hoch, Wilson Engelmann (2023)	Regulação da Inteligência Artificial no Judiciário Brasileiro e Europeu	Comparado	BR x UE	Necessidade de estrutura regulatória
41	Paulo Boa Sorte, Deborah Teles de Meneses Gonçalves, Giulia Pereira Santos (2024)	Transfobia algorítmica	Qualitativo	IA e discriminação	Regulação inclusiva necessária

Os estudos incluídos contemplam publicações realizadas entre 2022 e 2025 e apresentam predominância de pesquisas qualitativas, teóricas, jurídicas e revisões da literatura. A análise da produção científica selecionada evidencia diferentes perspectivas acerca da relação entre inteligência artificial, riscos sociais, violência digital e respostas regulatórias, que serão discutidas nas seções seguintes.

Da Eficiência à Vulnerabilidade: a Inteligência Artificial e a Reconfiguração dos Riscos Sociais

Os estudos incluídos na estratégia de busca "**Inteligência Artificial**" AND "**Risco**", realizada nas bases **SciELO** e **Portal de Periódicos CAPES**, demonstram que a inteligência artificial tem sido abordada como uma tecnologia associada à produção de riscos sociais, institucionais e jurídicos decorrentes da opacidade algorítmica, da autonomia decisória e da utilização de bases de dados enviesadas (Leal; Paulo, 2023; Cambraia; Pyrrho, 2024; Nas, 2024). Nesse contexto, os riscos associados à IA decorrem não apenas do funcionamento técnico dos sistemas, mas também de sua capacidade de reproduzir e ampliar desigualdades, vieses e vulnerabilidades presentes nas estruturas sociais.

A literatura evidencia que sistemas de IA podem comprometer direitos fundamentais, como privacidade, transparência e não discriminação, especialmente em aplicações relacionadas ao reconhecimento facial e à tomada de decisões judiciais (Sanabria Moyano *et al.*, 2022; Rossetti & Silva, 2023). Também aponta que algoritmos favorecem processos de manipulação informacional e desinformação, afetando a democracia e a governança (Lemos & Espíndola, 2024; Miranda Jr. & Wilke, 2024). Entre os principais riscos identificados destaca-se a discriminação algorítmica, decorrente da incorporação de vieses presentes nas bases de dados utilizadas para treinamento dos sistemas, produzindo impactos diretos sobre grupos vulneráveis (Leal & Paulo, 2023; Cambraia & Pyrrho, 2024; Nas, 2024). Conforme destacam Leal e Paulo (2023, p. 173), "a principal causa dos riscos discriminatórios [...] é a qualidade dos dados utilizados pelos algoritmos".

Os estudos também demonstram preocupações relacionadas à utilização da inteligência artificial em processos decisórios institucionais, especialmente no Poder Judiciário, em razão da automação, da opacidade algorítmica e das limitações à auditoria dos sistemas (Cabral *et al.*, 2024; Pimentel *et al.*, 2023). Essas limitações comprometem a transparência, a *accountability* e o controle social (Leal & Paulo, 2023, p. 174). No campo da governança de dados, observa-se que o compartilhamento de informações pessoais, embora necessário em determinados contextos, pode ampliar riscos à privacidade (Pinto *et al.*, 2022, p. 3), agravados pela comercialização indevida e pelo vazamento de dados (Pinto *et al.*, 2022, p. 4-5). Os estudos indicam ainda que aplicações baseadas em IA podem influenciar processos decisórios, segmentar usuários e restringir o acesso a bens e serviços essenciais, configurando formas contemporâneas de exclusão

social automatizada (Pinto *et al.*, 2022, p. 9). Ao operar com grandes volumes de dados, a tecnologia potencializa desigualdades já existentes, uma vez que "quando estes dados se tornam parte de uma IA [...] os vícios presentes ao sistema poderão se amplificar [...] e causar danos" (Nas, 2024, p. 6). No setor da saúde, essa preocupação estende-se à influência exercida pelos sistemas inteligentes sobre decisões médicas, reforçando a necessidade de preservar a supervisão humana em contextos decisórios sensíveis (Pinto *et al.*, 2022, p. 9).

Os estudos incluídos na estratégia de busca "**Inteligência Artificial**" AND "**Risco**", realizada nas bases **SciELO** e **Portal de Periódicos CAPES**, demonstram que a inteligência artificial tem sido abordada como uma tecnologia associada à produção de riscos sociais, institucionais e jurídicos decorrentes da opacidade algorítmica, da autonomia decisória e da utilização de bases de dados enviesadas (Leal; Paulo, 2023; Cambraia; Pyrrho, 2024; Nas, 2024). Nesse contexto, os riscos associados à IA decorrem não apenas do funcionamento técnico dos sistemas, mas também de sua capacidade de reproduzir e ampliar desigualdades, vieses e vulnerabilidades presentes nas estruturas sociais.

A literatura evidencia que sistemas de IA podem comprometer direitos fundamentais, como privacidade, transparência e não discriminação, especialmente em aplicações relacionadas ao reconhecimento facial e à tomada de decisões judiciais (Sanabria Moyano *et al.*, 2022; Rossetti & Silva, 2023). Também aponta que algoritmos favorecem processos de manipulação informacional e desinformação, afetando a democracia e a governança (Lemos & Espíndola, 2024; Miranda Jr. & Wilke, 2024). Entre os principais riscos identificados destaca-se a discriminação algorítmica, decorrente da incorporação de vieses presentes nas bases de dados utilizadas para treinamento dos sistemas, produzindo impactos diretos sobre grupos vulneráveis (Leal & Paulo, 2023; Cambraia & Pyrrho, 2024; Nas, 2024). Conforme destacam Leal e Paulo (2023, p. 173), "a principal causa dos riscos discriminatórios [...] é a qualidade dos dados utilizados pelos algoritmos".

Os estudos também demonstram preocupações relacionadas à utilização da inteligência artificial em processos decisórios institucionais, especialmente no Poder Judiciário, em razão da automação, da opacidade algorítmica e das limitações à auditoria dos sistemas (Cabral *et al.*, 2024; Pimentel *et al.*, 2023). Essas limitações comprometem a transparência, a *accountability* e o controle social (Leal & Paulo, 2023, p. 174). No campo da governança de dados, observa-se que o compartilhamento de informações pessoais, embora necessário em determinados contextos, pode ampliar riscos à privacidade (Pinto *et al.*, 2022, p. 3), agravados pela comercialização

indevida e pelo vazamento de dados (Pinto *et al.*, 2022, p. 4-5). Os estudos indicam ainda que aplicações baseadas em IA podem influenciar processos decisórios, segmentar usuários e restringir o acesso a bens e serviços essenciais, configurando formas contemporâneas de exclusão social automatizada (Pinto *et al.*, 2022, p. 9). Ao operar com grandes volumes de dados, a tecnologia potencializa desigualdades já existentes, uma vez que "quando estes dados se tornam parte de uma IA [...] os vícios presentes ao sistema poderão se amplificar [...] e causar danos" (Nas, 2024, p. 6). No setor da saúde, essa preocupação estende-se à influência exercida pelos sistemas inteligentes sobre decisões médicas, reforçando a necessidade de preservar a supervisão humana em contextos decisórios sensíveis (Pinto *et al.*, 2022, p. 9).

A Reconfiguração da Violência na Era da Inteligência Artificial

Os estudos incluídos na estratégia de busca "**Inteligência Artificial**" AND "**Violência**", realizada nas bases **SciELO** e **Portal de Periódicos CAPES**, demonstram que a inteligência artificial vem reconfigurando as dinâmicas contemporâneas da violência, especialmente no ambiente digital. A literatura identifica diferentes manifestações associadas à IA, incluindo violência digital, discurso de ódio e desinformação (Gaal Fong *et al.*, 2022; Stropparo, 2022; Rossel-Castagneto, 2025), violência de gênero (Coddou Mc Manus *et al.*, 2025; Roa Avella *et al.*, 2023; Santillan-Molina *et al.*, 2025), violência sexual digital decorrente de *deepfakes* e da divulgação não consentida de imagens íntimas (Vargas-Chaves, 2025; Lorca; García-Mingo, 2023; Bañuelos-Capistrán, 2024), violência política baseada em mecanismos automatizados de manipulação informacional (Rossel-Castagneto, 2025) e formas de violência estrutural relacionadas à reprodução de desigualdades e assimetrias de poder (Martínez Suárez, 2024; Sívori; Parreiras; Peña, 2023).

Os estudos apontam que algoritmos de recomendação e sistemas automatizados potencializam a disseminação de conteúdos violentos, discursos de ódio e desinformação (Gaal Fong *et al.*, 2022; Stropparo, 2022). Nesse contexto, a IA "Também facilitou a proliferação do discurso de ódio em ambientes digitais" (tradução própria), enquanto "o discurso de ódio não se limita mais ao incitamento direto à violência" (Rossel-Castagneto, 2025, p. 96 e 99) (tradução própria), evidenciando que essas práticas assumem formas cada vez mais difusas e ampliadas pelas plataformas digitais. De modo semelhante, mecanismos automatizados, como *bots*, vêm sendo utilizados para "posicionar tendências nas redes sociais e atacar candidatos adversários"

(Rossel-Castagneto, 2025, p. 102) (tradução própria), ampliando estratégias de manipulação informacional e violência política.

A violência de gênero constitui outro tema recorrente na literatura. Os estudos evidenciam que a inteligência artificial pode ser empregada tanto na prevenção quanto na amplificação da violência contra mulheres, especialmente em sistemas de avaliação de risco e proteção às vítimas (Coddou Mc Manus *et al.*, 2025; Roa Avella *et al.*, 2023). Todavia, limitações institucionais podem comprometer sua efetividade, uma vez que "O processo pode demorar várias horas, colocando em risco a segurança da vítima" (Santillan-Molina *et al.*, 2025) (tradução própria). Também são identificadas novas formas de violência associadas ao uso de *deepfakes* e à divulgação não consentida de imagens íntimas, capazes de atingir diretamente a dignidade e a identidade das vítimas (Vargas-Chaves, 2025; Lorca & García-Mingo, 2023). Nesse cenário, sistemas de IA generativa ampliam a produção de conteúdos ilícitos, incluindo "desinformação com conteúdo falso e crimes como roubo de identidade pornográfica não consensual" (Bañuelos-Capistrán, 2024, p. 8) (tradução própria).

Além das manifestações mais evidentes da violência digital, a literatura demonstra que os impactos da inteligência artificial alcançam dimensões estruturais relacionadas à reprodução de desigualdades e relações de poder (Martínez Suárez, 2024; Sívori; Parreiras; Peña, 2023). Martínez Suárez (2024) questiona a suposta neutralidade da IA ao aplicar à tecnologia as categorias de opressão propostas por Iris Marion Young, evidenciando como sistemas algorítmicos podem reproduzir injustiças historicamente consolidadas. De forma convergente, Sívori, Parreiras e Peña (2023) destacam que desigualdades de gênero, vieses discriminatórios e estruturas de poder permanecem presentes nas dinâmicas tecnológicas contemporâneas. Conforme assinala Martínez Suárez (2024, p. 31), trata-se de um fenômeno cujas "consequências não intencionais [...] tornam a identificação ainda mais complexa" (tradução própria), dificultando o reconhecimento e o enfrentamento da violência algorítmica.

Regulação da Inteligência Artificial: entre Lacunas Normativas e Modelos Emergentes

Os estudos incluídos na estratégia de busca "**Inteligência Artificial**" AND "**Regulamentação**", realizada nas bases **SciELO** e **Portal de Periódicos CAPES**, demonstram que a literatura científica enfatiza a necessidade de construção de marcos normativos capazes de responder aos desafios impostos pela inteligência artificial. Apesar dos avanços observados, a

regulamentação da IA permanece em processo de consolidação, sendo marcada por lacunas normativas, dificuldades de implementação e limitações dos modelos jurídicos tradicionais.

Os estudos evidenciam que um dos principais desafios regulatórios refere-se à inadequação da responsabilidade civil para lidar com danos causados por sistemas de inteligência artificial. A autonomia e a complexidade desses sistemas dificultam a identificação do agente responsável, exigindo a reformulação de categorias jurídicas clássicas (Nascimento *et al.*, 2021). Nesse contexto, a literatura destaca a necessidade de adoção de princípios voltados à governança da IA, especialmente transparência, explicabilidade, *accountability* e proteção dos direitos fundamentais, considerados essenciais para assegurar o desenvolvimento e o uso ético da tecnologia (Matos, 2024; Bedregal Aguilar, 2025).

Outro aspecto recorrente refere-se à regulamentação de aplicações específicas da inteligência artificial, como *deepfakes*, sistemas de recomendação e algoritmos empregados em contextos institucionais. Os estudos apontam a necessidade de normas específicas voltadas à proteção de dados, ao enfrentamento da desinformação e à preservação da integridade do processo democrático (França Netto *et al.*, 2024; Lima *et al.*, 2024). Nessa perspectiva, Hoch e Engelmann (2023) destacam o modelo europeu baseado na classificação dos sistemas de IA conforme seu potencial de risco, permitindo a adoção de diferentes níveis de controle e supervisão, referência frequentemente mencionada pela literatura analisada.

No contexto brasileiro, os estudos indicam que a regulação da inteligência artificial ainda se encontra em fase de desenvolvimento, embora iniciativas legislativas demonstrem esforços para a construção de um marco regulatório. Destacam-se o Projeto de Lei nº 21/2020 e o Projeto de Lei nº 2.338/2023, este voltado ao estabelecimento de normas gerais para o desenvolvimento, implementação e uso responsável de sistemas de inteligência artificial no país (Brasil, 2020; Brasil, 2023). Paralelamente, o Brasil passou a integrar a **Parceria Global em Inteligência Artificial (GPAI)**, iniciativa internacional voltada ao desenvolvimento de pesquisas e boas práticas para o uso ético e responsável da IA, ampliando sua participação nos debates internacionais sobre governança tecnológica (Gov.br, 2023).

O cenário regulatório brasileiro também passou por atualizações recentes, destacando-se a promulgação do **Estatuto Digital da Criança e do Adolescente** (Lei nº 15.211/2025), voltado à ampliação da proteção de crianças e adolescentes no ambiente digital (Brasil, 2025; Nunes, 2026), e da **Lei nº 15.123/2025**, que alterou o Código Penal para aumentar a pena do crime de violência psicológica contra a mulher quando praticado mediante o uso de inteligência artificial

ou de recursos tecnológicos capazes de alterar imagem ou som da vítima (Brasil, 2025). Essas medidas dialogam diretamente com fenômenos como os *deepfakes*, compreendidos como conteúdos sintéticos produzidos por inteligência artificial para simular imagens, áudios ou vídeos falsos (Rossel-Castagneto, 2025). Somam-se a esse cenário também, o recentíssimo Decreto nº 12.975/2026, que atualizou a regulamentação do Marco Civil da Internet, e o Decreto nº 12.976/2026, voltado à proteção de mulheres e meninas na internet e ao enfrentamento da violência digital (Brasil, 2026; Brasil, 2026). Conforme observam Martins e Barbosa (2026), essas medidas fortalecem mecanismos de responsabilização das plataformas digitais e ampliam estratégias de prevenção e enfrentamento de práticas ilícitas em ambientes digitais.

Paralelamente às iniciativas legislativas, observa-se o fortalecimento de mecanismos institucionais voltados à governança da inteligência artificial no âmbito do Poder Judiciário. Documentos recentes do Conselho Nacional de Justiça evidenciam a incorporação de diretrizes relacionadas à transparência, supervisão e conformidade no uso da IA, bem como o reconhecimento da violência digital como tema de proteção de direitos fundamentais, especialmente em relação às mulheres, meninas e pessoas em situação de vulnerabilidade (CNJ, 2024; CNJ, 2025). Embora tais documentos não integrem o corpus científico desta revisão, sua análise complementa o cenário regulatório brasileiro ao demonstrar que a preocupação com a governança da inteligência artificial também vem sendo incorporada pelas instituições públicas.

Interseção entre Inteligência Artificial, Riscos Sociais, Violência Digital e Respostas Regulatórias

A análise integrada dos estudos evidencia que a produção científica recente sobre inteligência artificial permanece predominantemente fragmentada. Enquanto parte da literatura concentra-se nos riscos associados à opacidade algorítmica, à discriminação e à governança de dados (Leal; Paulo, 2023; Cambraia; Pyrrho, 2024; Pimentel *et al.*, 2023), outro conjunto de estudos prioriza manifestações de violência digital, como discurso de ódio, desinformação, *deepfakes* e violência de gênero (Gaal Fong *et al.*, 2022; Rossel-Castagneto, 2025; Vargas-Chaves, 2025; Coddou Mc Manus *et al.*, 2025). Paralelamente, os trabalhos voltados à regulação concentram-se na construção de mecanismos de governança, responsabilização e proteção de direitos fundamentais (Hoch; Engelmann, 2023; Matos, 2024; Bedregal Aguilar, 2025). Observa-se, contudo, que ainda são limitados os estudos que analisam essas dimensões de forma articulada.

Embora abordados sob perspectivas distintas, os resultados demonstram que essas três dimensões mantêm estreita relação entre si. Os riscos decorrentes da opacidade algorítmica, da reprodução de vieses e da automação de decisões constituem fatores que potencializam diferentes formas de violência digital, como discurso de ódio, manipulação informacional, violência de gênero e utilização de *deepfakes* (Leal; Paulo, 2023; Cambraia; Pyrrho, 2024; Gaal Fong *et al.*, 2022; Rossel-Castagneto, 2025; Vargas-Chaves, 2025). Em resposta a esses desafios, a literatura enfatiza a necessidade de mecanismos regulatórios baseados em transparência, explicabilidade, *accountability*, supervisão humana e proteção de direitos fundamentais (Hoch; Engelmann, 2023; Matos, 2024; Bedregal Aguilar, 2025).

Esse conjunto de evidências demonstra que os impactos da inteligência artificial transcendem a dimensão estritamente tecnológica e alcançam aspectos sociais, jurídicos e institucionais. Nessa perspectiva, a efetividade das respostas regulatórias depende da adoção de modelos de governança capazes de integrar gestão de riscos, prevenção das diferentes formas de violência digital e proteção dos direitos fundamentais, superando abordagens fragmentadas ainda predominantes na literatura analisada.

CONCLUSÃO

A presente revisão integrativa permitiu analisar como a literatura científica recente tem abordado a relação entre inteligência artificial, riscos sociais, violência digital e respostas regulatórias. Os estudos evidenciam que, embora a inteligência artificial impulse processos de inovação em diferentes setores, sua utilização também amplia desafios relacionados à opacidade algorítmica, à reprodução de vieses, à automação de decisões e à proteção de direitos fundamentais, produzindo impactos que extrapolam a dimensão tecnológica e alcançam aspectos sociais, jurídicos e institucionais.

Os achados demonstram que a violência digital constitui uma das principais manifestações associadas ao uso da inteligência artificial, abrangendo práticas como desinformação, discursos de ódio, violência de gênero, *deepfakes* e divulgação não consentida de imagens íntimas. Paralelamente, a literatura converge para a necessidade de modelos regulatórios orientados pela transparência, explicabilidade, supervisão humana, responsabilização (*accountability*) e gestão de riscos, como forma de compatibilizar a inovação tecnológica com a proteção dos direitos fundamentais.

A análise integrada da produção científica evidenciou, contudo, que os estudos permanecem predominantemente fragmentados, concentrando-se, em geral, na investigação isolada dos riscos sociais, da violência digital ou das respostas regulatórias. Como contribuição, esta revisão integra essas dimensões em uma perspectiva analítica única, sistematizando evidências, identificando convergências e lacunas na literatura e reforçando a necessidade de abordagens interdisciplinares capazes de subsidiar o aprimoramento da governança da inteligência artificial, a formulação de políticas públicas e o desenvolvimento de marcos regulatórios mais compatíveis com os desafios contemporâneos.

REFERÊNCIAS

- Braga, F. M. F., & Cardoso, P. V. (2017). [Resenha do livro *Weapons of math destruction: How big data increases inequality and threatens democracy*, de C. O'Neil]. *Mural Internacional*, 7(1), 94–97.<https://doi.org/10.12957/rmi.2016.25939>
- Brasil. (2025). *Lei nº 15.123, de 24 de abril de 2025. Altera o art. 147-B do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para estabelecer causa de aumento de pena no crime de violência psicológica contra a mulher quando praticado com o uso de inteligência artificial ou de qualquer outro recurso tecnológico que altere imagem ou som da vítima*.https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15123.htm
- Brasil. (2025). *Lei nº 15.211, de 17 de setembro de 2025. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente)*.https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15211.htm
- Brasil. (2026). *Decreto nº 12.975, de 20 de maio de 2026. Altera o Decreto nº 8.771, de 11 de maio de 2016, que regulamenta a Lei nº 12.965, de 23 de abril de 2014*.https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/decreto/d12975.htm.
- Brasil. (2026). *Decreto nº 12.976, de 20 de maio de 2026. Estabelece diretrizes para a proteção de mulheres na internet e para o enfrentamento da violência contra mulheres em ambiente digital*.https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/decreto/d12976.htm
- Brasil. Câmara dos Deputados. (2020). *Projeto de Lei nº 21, de 2020. Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil e dá outras providências*.<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2236340>
- Brasil. Senado Federal. (2023). *Projeto de Lei nº 2.338, de 2023. Dispõe sobre o uso da inteligência artificial*.<https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>
- Butcher, I. (2024, March 13). Parlamento Europeu aprova lei de inteligência artificial. *TELETIME*.<https://teletime.com.br/13/03/2024/parlamento-europeu-aprova-lei-de-inteligencia-artificial/>

- Cambraia, L., & Pyrrho, M. (2024). Inteligência artificial e injustiça: Para além de uma análise ética encantada dos algoritmos. *Revista Iberoamericana de Bioética*, 25, 1–15. <https://doi.org/10.14422/rib.i25.y2024.001>
- Coddou Mc Manus, A., Ruiz-Eskide Enríquez, I., Bergeret Sáez, D., Loyola Olmos, C., & Sánchez Andrade, V. (2025). IA y violencia contra las mujeres: La automatización de la evaluación del riesgo. *Política Criminal*, 20(40), 346–383. <http://dx.doi.org/10.4067/s0718-33992025000200346>
- Conselho Nacional de Justiça. (2024). *Justiça em números 2024*. <https://bibliotecadigital.cnj.jus.br/jspui/handle/123456789/860>
- Conselho Nacional de Justiça. (2024). *O uso da inteligência artificial generativa no Poder Judiciário brasileiro: Relatório de pesquisa*. <https://bibliotecadigital.cnj.jus.br/xmlui/handle/123456789/976>
- Conselho Nacional de Justiça. (2025). *Resolução nº 615, de 11 de março de 2025: Estabelece diretrizes para o desenvolvimento, utilização e governança de soluções desenvolvidas com recursos de inteligência artificial no Poder Judiciário*. <https://atos.cnj.jus.br/atos/detalhar/6001>
- Conselho Nacional de Justiça- CNJ. (2025). *Direitos das pessoas defensoras de direitos humanos: Parâmetros interamericanos para o sistema de justiça*. <https://www.cnj.jus.br/wp-content/uploads/2025/12/direitos-das-pessoas-defensoras-de-direitos-humanos-05-12-25-1-1.pdf>
- Crawford, K. (2021). *Atlas of AI: Power, politics, and the planetary costs of artificial intelligence*. Yale University Press
- Kasparov, G. (2017). *Deep thinking: Where machine intelligence ends and human creativity begins*. John Murray.
- Lage, F. de C. (2022). *Manual de inteligência artificial no direito brasileiro* (2ª ed.). Editora Juspodivm.
- Leal, M. C. H., & Paulo, L. M. (2023). Algoritmos discriminatórios e jurisdição constitucional: Os riscos jurídicos e sociais do impacto dos vieses nas plataformas de inteligência artificial de amplo acesso. *Revista de Direitos e Garantias Fundamentais*, 24(3), 165–187. <https://doi.org/10.18759/rdgf.v24i3.2311>
- Marcílio, T. (2025). Caminhos do PL 2.338/23. *Migalhas*. <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/430410/caminhos-do-pl-2-338-23>.
- Martínez Suárez, Y. (2024). Opresión, desigualdad e inteligencia artificial. *Eu-topías: Revista de Interculturalidad, Comunicación y Estudios Europeos*, 28, 23–33. <https://doi.org/10.7203/eutopias.28.29053>
- Matos, M. A. de. (2024). Inteligência artificial e a sua regulamentação. *Revista Políticas Públicas & Cidades*, 13(2), e1477. <https://doi.org/10.23900/2359-1552v13n2-416-2024>

- Mota, R. G. (2022). Direito internacional humanitário e as armas autônomas letais. *Revista de Direito Internacional*, 19(3), 337–354. <https://doi.org/10.5102/rdi.v19i3.8599>
- Naffi, N. (2025, October 1). Deepfakes and the crisis of knowing. *UNESCO*. <https://www.unesco.org/en/articles/deepfakes-and-crisis-knowing>.
- Nas, E. (2024). Territórios do conhecimento: O debate bioético da IA responsável e decolonial. *Mediações: Revista de Ciências Sociais*, 29(3), 1–18. <https://doi.org/10.5433/2176-6665.2024v29n3e50076>
- Nunes, P. A. (2026). *ECA Digital entra em vigor com a finalidade de ampliar a proteção de crianças e adolescentes no ambiente online*. Tribunal de Justiça do Estado do Amazonas. <https://www.tjam.jus.br/index.php/menu/sala-de-imprensa/16528-eca-digital-entra-em-vigor-com-a-finalidade-de-ampliar-a-protecao-de-criancas-e-adolescentes-no-ambiente-online>
- O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown.
- Rossetti, R., & Silva, C. V. de M. e. (2024). Direitos fundamentais no uso de inteligência artificial no Poder Judiciário brasileiro. *Revista Tecnologia e Sociedade*, 20(59), 219–235. <https://doi.org/10.3895/rts.v20n59.16406>
- Russell, S., & Norvig, P. (2013). *Inteligência artificial* (3ª ed.). Elsevier.
- Sanabria Moyano, J. E., Roa Avella, M. del P., & Lee Pérez, O. I. (2022). Tecnología de reconocimiento facial y sus riesgos en los derechos humanos. *Revista Criminalidad*, 64(3), 61–78. <https://doi.org/10.47741/17943108.366>
- Sánchez-Bolívar, L., Escalante-González, S., & Martínez-Martínez, A. (2024). La ética de la inteligencia artificial en educación: ¿Amenaza u oportunidad? *Revista Electrónica Educare*, 28(S), 1–20. <https://doi.org/10.15359/REE.28-S.20541>
- Silveira, S. A. da. (2024). Questões conjunturais sobre a regulação da IA. *RECIIS – Revista Eletrônica de Comunicação, Informação & Inovação em Saúde*, 18(3), 458–466. <https://doi.org/10.29397/reciis.v18i3.4634>
- Sívori, H. F., Parreiras, C., & Peña, P. (2023). Apresentação: Por que perspectivas latino-americanas sobre feminismo, gênero e sexualidade em tecnologias digitais. *Sexualidad, Salud y Sociedad – Revista Latinoamericana*, 39, e22300. <https://doi.org/10.1590/1984-6487.sess.2023.39.e22300.a.pt>
- Souza, M. T., Silva, M. D., & Carvalho, R. (2010). Revisão integrativa: o que é e como fazer. *Einstein (São Paulo)*, 8(1), 102–106. <https://doi.org/10.1590/S1679-45082010RW1134>
- United Nations. (2024). *Governing AI for Humanity: Final Report*. 2024. https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_en.pdf.
- Vargas-Chaves, I. (2025). *Take it Down Act: un análisis crítico de su rol contra la difusión no consentida de imágenes y deepfakes*. *Revista Criminalidad*, 67(3), 39–55.

<https://doi.org/10.47741/17943108.729>

Whittemore, R., & Knafl, K. (2005). The integrative review: Updated methodology. *Journal of Advanced Nursing*, 52(5), 546–553. <https://doi.org/10.1111/j.1365-2648.2005.03621.x>

Zuboff, S. (2019). *The age of surveillance capitalism*. Profile Books.