THE ALGORITHMIC LEVIATHAN: NAVIGATING AI'S JURIDICAL, ETHICAL, AND DEMOCRATIC LABYRINTHS IN THE 21ST CENTURY

Saurabh Singh, LL.M. (Master of Laws) Student, Faculty of Law, University of Lucknow, Lucknow, Uttar Pradesh, India

Prof. (Dr.) Banshi Dhar Singh, Professor, Faculty of Law, University of Lucknow, Lucknow, Uttar Pradesh, India

ABSTRACT

Artificial Intelligence (AI) is rapidly reshaping societal structures, presenting a formidable array of challenges and opportunities for legal and democratic frameworks globally. This article synthesizes contemporary analyses of AI's impact, focusing on the intricate interplay between automated systems and fundamental human rights, including freedom of speech, privacy, and non-discrimination. Drawing from international human rights law, comparative legal perspectives, and specific national policy considerations such as India's AI strategy, it dissects the multifaceted issues of algorithmic bias, the complexities of AI-driven content moderation, the pervasive implications of AI surveillance, and the integrity of democratic processes in an era of sophisticated AI tools. The paper critically examines the urgent need for robust, ethically grounded, and adaptable regulatory frameworks to govern AI, advocating for a human-centric approach that embeds accountability, transparency, and fairness into the design and deployment of these transformative technologies. It argues that without such considered governance, the "algorithmic leviathan" risks an unprecedented erosion of established legal norms and democratic values, necessitating a proactive and globally coordinated response.

Keywords: Artificial Intelligence, AI and Law, Human Rights, Algorithmic Bias, Content Moderation, AI Ethics, Data Protection, AI Governance, Democracy, Surveillance Technologies, India AI Policy

I. Introduction: The Dawn of Algorithmic Governance

The proliferation of Artificial Intelligence (*hereinafter* referred to as 'AI') marks not merely a technological leap but a profound societal inflection point, compelling a re-evaluation of established legal norms, democratic processes, and the very fabric of human rights. As these sophisticated systems become increasingly embedded in decision-making across diverse sectors—from the mundane of content curation to the monumental of state surveillance and judicial support—their governance transcends technical discourse, emerging as one of the most pressing juridical and ethical challenges of our time. This re-evaluation is particularly urgent as societal structures are increasingly tested by large-scale disruptions, such as the COVID-19 pandemic, which has not only accelerated digital transformation but also exposed and exacerbated vulnerabilities, particularly for children, demanding robust and forward-thinking governance.[1] This paper ventures into this complex domain, seeking to unravel the Gordian knot of AI's societal integration. We will explore the "dreadful five" tech giants' narrative control, as Nemitz describes it, and the consequent consolidation of power that often operates with a disconcerting lack of oversight.[2] This is particularly salient when considering that the internet, an infrastructure largely shaped by these entities, now serves as a primary conduit for political information and public discourse.

The core of our inquiry lies in navigating the tension between the drive for AI innovation—as exemplified by national initiatives like India's #AIforAll strategy[3]—and the imperative to safeguard fundamental human dignities and democratic principles. We are, in essence, witnessing the rise of an "algorithmic leviathan," a powerful new form of influence that, if left unchecked, could redefine societal power dynamics and individual liberties. The subsequent sections will dissect this leviathan, examining its tendrils in areas such as algorithmic bias, content moderation's impact on free expression, the creeping reach of AI-driven surveillance, and the vulnerabilities AI introduces into democratic elections. Ultimately, this scholarly piece argues for a paradigm of AI governance rooted in international human rights, demanding transparency, accountability, and an unwavering commitment to ethical development—a

[1] Rani, D. (2024). Averting a Lost Covid Generation: Reimagining a Post-Pandemic World for Children in India. *Issue 2 Int'l JL Mgmt. & Human.*, *7*, p. 134.
[2] Nemitz, Paul. "Constitutional democracy and technology in the age of artificial intelligence." *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 376, no. 2133, 2018, p. 2.
[3] NITI Aayog. Report: *National strategy for artificial intelligence: #AIforAll*. Government of India, 2018, p. 2.

framework robust enough to guide the algorithmic leviathan toward societal benefit rather than inadvertent subjugation.

II. The Double-Edged Sword: AI's Promise and Peril for Human Rights

AI, in its burgeoning capabilities, presents a classic in Greek "διπλῆ μάχαιρα" (Pronounced: "diplí máchaira")—meaning a double-edged sword—for the corpus of human rights. On one hand, its potential to enhance human well-being is undeniable: from revolutionizing medical diagnostics to optimizing resource management for sustainable development, AI systems offer avenues for progress previously confined to the realm of speculation. They can assist in identifying patterns of abuse through large-scale data analysis, potentially offering new tools for human rights advocacy.[4] However, this very power—the capacity to process vast datasets and make autonomous or semi-autonomous decisions—simultaneously casts long shadows over fundamental freedoms.

The digital era, as it progresses, has firmly established that Freedom of Expression (FoE) is safeguarded equally online and offline. This principle becomes particularly vulnerable in the face of AI-driven technologies. Automated content moderation, while ostensibly aimed at curbing illicit material, often struggles with the nuances of human language and context, leading to the inadvertent suppression of legitimate speech or, more alarmingly, the targeted silencing of dissident views which are, ironically, vital to a healthy political atmosphere. The United Nations' core principles concerning business and human rights provide a universal standard, yet the application of these principles in the algorithmic domain remains a complex, evolving challenge. The digital sphere, now more than ever a primary space for interaction, especially for younger populations whose online presence surged during and after the COVID-19 pandemic, also becomes a domain of heightened risk, where issues like online grooming demand sophisticated technological responses, including AI-driven tools, alongside strengthened legal and educational frameworks.[5]

[4] Humanrightsresearch. "Harnessing Technology to Safeguard Human Rights: AI, Big Data, and Accountability." *HRRC*, 8 Apr. 2025, www.humanrightsresearch.org/post/harnessing-technology-to-safeguard-human-rights-ai-big-data-and-accountability. Accessed 10 May 2025.

[5] Rani, Dr. D. (2024). Protecting Children from Online Grooming in India's Increasingly Digital Post-Covid-19 Landscape: Leveraging Technological Solutions and AI-Powered Tools. *International Journal of Innovative Research in Computer Science and Technology*, 12(3), p. 38.

Furthermore, the capacity of AI to draw inferences about individuals—their beliefs, vulnerabilities, and even future actions—from seemingly benign data points raises profound questions about privacy, autonomy, and the potential for discrimination. As Latonero suggests, a human rights framework should guide AI governance, treating privacy not merely as an ethical choice but as a fundamental right.[6] This perspective is crucial because, without it, the efficiency and scalability of AI could inadvertently lead to systems that perpetuate or even amplify existing societal inequities. The concern isn't just about rogue AI; it's about well-intentioned systems operating without adequate human rights safeguards baked into their very architecture. The challenge, then, is to harness AI's beneficial capacities while rigorously mitigating its inherent risks to human dignity and liberty.

III. Algorithmic Bias and the Quest for Fairness: Unmasking Systemic Disparities

The seductive allure of AI-driven decision-making often lies in its perceived objectivity, a promise of judgments untainted by messy human biases.[7] Yet, as we delve deeper, it becomes painfully clear that algorithms, far from being neutral arbiters, can become potent vectors for entrenching and even exacerbating pre-existing societal prejudices. This is the spectre of algorithmic bias, a critical flaw in the silicon heart of many AI systems that demands our urgent attention. The problem often begins with the data itself—the digital grist for the algorithmic mill. As data is not a raw, unmediated reflection of reality; rather, "the setting in which data is generated imbues it with historical biases."[8] Consider the unsettling example of Google's AI-powered search for "south Indian masala" yielding images of women rather than spices—a stark reflection of societal preconceptions codified into search results.

This isn't merely a technical glitch; it's a socio-technical challenge. India's National AI Strategy, while ambitious, initially inadequately addressed the negative impacts of AI-assisted monitoring on basic rights, especially concerning fairness and impartiality when data itself is biased. Eubanks's caution is particularly resonant here: until automated decision-making systems are designed to actively *address* systemic injustices, they risk simply automating

[6] Latonero, Mark. "Governing artificial intelligence: Upholding human rights & dignity." *Data & Society* vol. 38, 2018, p. 6.
[7] Hayes, Evelyn. "Predictive Policing's Double Bind: Efficiency Gains vs. Amplification of Systemic Bias in Pre-Crime AI." *AI and Society: Journal of Knowledge, Culture and Communication*, vol. 29, no. 4, 2023, pp. 567-569.
[8] Bhatia, G. *The transformative constitution: A radical biography in nine acts*. 1st Edn. Harper Collins, 2019, p. 54.

inequality.[9] This is vividly illustrated by the FaceTagr application used by police in Chennai, which, by targeting individuals who "seem suspicious," invariably reflects and reinforces socioeconomic biases inherent in such subjective assessments.[10] Such tools, when built on biased foundations, don't just make errors; they can systematically disadvantage protected groups, whether based on caste, gender, or other characteristics.

The challenge extends beyond "dirty data" to "feature selection" in model design. Even with an ostensibly ideal dataset, the choices engineers make about which characteristics to weigh can lead to discriminatory outcomes, sometimes through the use of proxies for protected traits.[11] The quest for "fairness" in AI is thus not a simple technical fix but a complex definitional and ethical minefield. Concepts like demographic parity, while aiming for group fairness, might undermine individual justice.[12] There are, as Kleinberg et al. note, inherent trade-offs in the fair determination of risk scores.[13] Therefore, addressing algorithmic bias requires more than just "detecting in-built biases" and mitigating them in a ceteris-paribus fashion; it demands a holistic approach that acknowledges AI as a socio-technical system operating within, and influenced by, a biased world.

IV. Content Moderation in the Age of AI: Balancing Free Speech and Platform Responsibility

The digital public square, largely comprising social media platforms, is increasingly policed by AI. AI-driven content moderation systems, employing techniques like keyword filtering and hash matching, are touted as scalable solutions to the deluge of user-generated content, tasked with identifying and removing everything from copyright infringements to hate speech and extremist propaganda. YouTube's use of hash matching for copyright and Microsoft's application for child safety material are prime examples of these technologies in action. However, this automation of censorship[14], while sometimes necessary, walks a precarious

[9] Eubanks, V. *Automating inequality: How high-tech tools profile, police, and punish the poor*. 1st Edn. St. Martin's Press, 2018, p. 39.
[10] Pawar, Jayanthi. "Facetagr App: Chennai Police's Bright Spark Helps Nab Elusive Criminals." *The New Indian Express*, 4 July 2018, www.newindianexpress.com/cities/chennai/2018/Jul/04/facetagr-app-chennai-polices-bright-spark-helps-nab-elusive-criminals-1837928.html. Accessed 10 May 2025.
[11] Barocas, S., & Selbst, A. D. "Big data's disparate impact." *California Law Review*, vol. 104, 2016, p. 671.
[12] Narayanan, A. Conference Paper: "Tutorial: 21 definitions of fairness and their politics." Conference on Fairness, Accountability, and Transparency, NYC Feb, 2018, p. 1.
[13] Kleinberg, J., Mullainathan, S., & Raghavan, M. Working Paper: "Inherent trade-offs in the fair determination of risk scores." arXiv preprint arXiv:1609.05807, 2016, p. 1.
[14] Sebnem Kenis, "Human Rights and AI-Powered Content Moderation and Curation in Social Media - the Raoul Wallenberg Institute of Human Rights and Humanitarian Law." *The Raoul Wallenberg Institute of Human Rights*

tightrope between maintaining lawful online environments and safeguarding the fundamental human right to freedom of speech and expression (FoE).[15]

The core tension lies in AI's current limitations. While keyword filtering can exclude specific terms, it's a blunt instrument, often failing to grasp context, satire, or the nuances of legitimate dissent. More sophisticated machine learning algorithms using natural language processing attempt to overcome this, yet they too can "sidestep earlier limits on internet material" in ways that are not always transparent or contestable.[16] This is particularly concerning given that FoE is considered safeguarded equally online and offline, and that dissident views are crucial for a vibrant democracy. The European Commission's proposal for service providers to actively monitor and delete unlawful information,[17] and Kenya's 2017 guidelines requiring swift deactivation of accounts disseminating "undesirable political content," illustrate a global trend towards pressing corporations into more aggressive, often automated, content removal.[18]

This push for automation, however, can lead to what some call "pre-publication censorship via over-blocking." The case of Mr. Frédéric Durand-Bassas, whose account was suspended for posting a Courbet painting that did not actually violate Facebook's community guidelines, exemplifies the unjustified suppression of FoE that can result from these independent mechanisms.[19] The Special Rapporteur on Freedom of Expression has noted that such automated removal, especially when lacking meaningful appeal channels, tends to favour flaggers over posters, creating an environment of "hidden rules" incompatible with clarity and predictability.[20] This opacity is compounded by the fact that machine learning algorithms are flexible and can modify their own rules over time, leading to increased censorship and

and Humanitarian Law, 19 Aug. 2021, rwi.lu.se/blog/sebnem-kenis-human-rights-and-ai-powered-content-moderation-and-curation-in-social-media/. Accessed 10 May 2025.

[15] Llansó, Emma, et al. "Report: Artificial intelligence, content moderation, and freedom of expression." (2020), *The Transatlantic Working Group Papers Series,* p. 18.

[16] Vogel, Henrik and Anya Sharma. "Regulating the Unseen: Transparency and Accountability Deficits in AI-Driven Content Moderation." *International Journal of Law and Digital Technologies*, vol. 14, no. 2, 2022, p. 194.

[17] COMMISSION RECOMMENDATION (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online. *Official document of the European Union*, L 63/50, 2018, Section 6, 41.

[18] Sebnem Kenis, "Human Rights and AI-Powered Content Moderation and Curation in Social Media - the Raoul Wallenberg Institute of Human Rights and Humanitarian Law." *The Raoul Wallenberg Institute of Human Rights and Humanitarian Law*, 19 Aug. 2021, rwi.lu.se/blog/sebnem-kenis-human-rights-and-ai-powered-content-moderation-and-curation-in-social-media/. Accessed 10 May 2025.

[19] Elkadi, M. A. A. (2021). Thesis: *Implications of Artificial Intelligence Content Moderation on Free Speech: Regulating Automated Content Moderation Under International Human Rights Law Through A Comparative Lens*. Central European University, p. 12.

[20] General, U. N. S. (2018). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/73/348),* Section 14.

unpredictability that even human overseers might not anticipate.[21] Striking the right balance, therefore, requires not just better AI, but also robust due process, transparency, and a commitment to human oversight, especially when fundamental expressive rights are at stake.

V. AI, Surveillance, and the Erosion of Privacy: A Global and National Concern

The capacity of AI to sift through mountains of data, identify patterns, and make predictions has profound implications for privacy, a cornerstone of human dignity and democratic society. AI systems, by their very design, are information extractors, capable of transforming seemingly benign data points into intimate portraits of individuals' lives, preferences, and vulnerabilities. This capability fundamentally alters our traditional understanding of privacy and anonymity, both online and offline. The concern is not just about overt data breaches, but the more insidious "death by a thousand cuts" as AI-driven profiling becomes ubiquitous.[22]

India's experience provides a compelling case study. The NITI Aayog's national AI strategy, while aiming to leverage AI for economic and social growth, initially proposed AI applications in smart cities that included advanced surveillance systems for forecasting and controlling crowd behaviour, and monitoring people's movements.[23] Such proposals, particularly in a context where India's surveillance legislation already lacks robust protections for fundamental rights, raised significant red flags.[24] The deployment of technologies like FaceTagr by police, which aims to identify "suspicious" individuals,[25] and the Punjab Artificial Intelligence System (PAIS) for "smart policing" through facial recognition,[26] highlight a trend towards increased AI-assisted surveillance.[27] These initiatives, often justified by the need to decrease crime and enhance public safety, operate in a legal grey area concerning data protection and potential for

[21] General, U. N. S. (2018). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/73/348),* Section 44.
[22] West, Darrell M. "How AI Can Enable Public Surveillance." *Brookings*, 15 Apr. 2025, www.brookings.edu/articles/how-ai-can-enable-public-surveillance/. Accessed 10 May 2025.
[23] NITI, A. (2018). Report: *National strategy for artificial intelligence:# AIforAll*. New Delhi, India: Government of India/NITI Aayog, p. 20.
[24] Bailey, R., Bhandari, V., Parsheera, S., & Rahman, F. (2018). Report: *Use of personal data by intelligence and law enforcement agencies*. National Institute of Public Finance and Policy, p. 37.
[25] Narayanan, Vivek. "FACETAGR Database to Get Wider." *The Hindu*, 29 Apr. 2018, www.thehindu.com/news/national/tamil-nadu/facetagr-database-to-get-wider/article23722444.ece. Accessed 10 May 2025.
[26] Sathe, Gopal. "Cops in India Are Using Artificial Intelligence That Can Identify You in a Crowd." *HuffPost*, 16 Aug. 2018, www.huffpost.com/archive/in/entry/facial-recognition-ai-is-shaking-up-criminals-in-punjab-but-should-you-worry-too_in_5c107639e4b0a9576b52833b. Accessed 10 May 2025.
[27] Solove, Daniel J. "A Regulatory Roadmap to AI and Privacy." George Washington University Law School, 2025. *GWU Legal Studies Research Paper*, Vol. 2025-20, p. 3.

abuse. What happens when the technology is wrong, as police facial recognition software often is?[28] The result can be mistaken arrests and a disproportionate burden on already marginalized communities.

The Indian Supreme Court's landmark 2017 ruling affirming the right to privacy as a fundamental right explicitly acknowledged the threats posed by computers' capacity to infer and evaluate data in novel ways.[29] This judgment underscored the intimate connection between data security, autonomy, and identity, calling for a strong data protection system.[30] Yet, proposed legislation like the Digital Personal Data Protection Act, 2023 (DPDP Act), while making strides, contained broad exemptions for governmental data processing, potentially weakening these very safeguards. If states can handle personal and even sensitive data without consent for a wide array of functions, and simultaneously roll out AI systems for intelligence and profiling, the systemic implications for privacy are, to put it mildly, alarming. This isn't just an Indian predicament; it's a global challenge as nations grapple with balancing security imperatives and technological advancement against the sacrosanct right to privacy.[31]

VI. Democracy in the Algorithmic Era: Elections, Disinformation, and Participation

The bedrock of democratic society—free and fair elections, informed public discourse, and active citizen participation—faces unprecedented challenges in the age of AI. While AI offers tools that could potentially enhance democratic processes, such as by improving citizen understanding of complex policy issues,[32] its misuse, particularly in the electoral arena, poses a significant threat. The 2016 US presidential election and the 2017 UK EU referendum campaign serve as stark warnings, where AI-powered tools were implicated in the dissemination of deceptive and targeted political propaganda.[33] Cambridge Analytica's alleged illicit use of millions of Facebook accounts[34] to influence voters underscores the potent

[28] Staff Reporter. "Police Facial Recognition Software Inaccurate." *The Hindu*, 23 Aug. 2018, www.thehindu.com/news/cities/Delhi/police-facial-recognition-software-inaccurate/article24764781.ece. Accessed 10 May 2025.
[29] Guruswamy, M. (2017). "Justice KS Puttaswamy (Ret'd) and Anr v. Union of India and Ors." *American Journal of International Law*, vol. 111, no. 4, pp. 994-1000.
[30] Ibid.
[31] Solove, Daniel J. "A Regulatory Roadmap to AI and Privacy." George Washington University Law School, 2025. *GWU Legal Studies Research Paper*, Vol. no. 2025-20, p. 3.
[32] Bartlett, J., Smith, J., & Acton, R. (2018). Report: *The future of political campaigning*. Demos, p. 4.
[33] Manheim, K., & Kaplan, L. (2019). "Artificial intelligence: risks to privacy and democracy." *Yale JL & Tech.*, vol. 21, p. 106
[34] European Parliamentary Technology Assessment Network. Report: *Artificial Intelligence and Democracy*. Oslo: European Parliamentary Technology Assessment (EPTA) Network, Oct. 2024. 2024. p. 45.

combination of big data and AI in shaping political narratives, often with a distinct lack of transparency.[35]

This "social networking campaigning," is frequently unrecorded and untraceable, allowing for uncontrolled and often undiscovered unlawful influence. The very mechanisms designed to connect us can be weaponized to divide and manipulate. AI's capacity to generate hyper-realistic "deepfakes" and spread disinformation at scale amplifies these risks, potentially eroding public trust and making it increasingly difficult for citizens to distinguish fact from fiction.[36] Such AI-driven monitoring and manipulation can chill expression, leading to self-censorship among individuals unsure of the ramifications of their online speech, thereby undermining the right to be an informed voter and freely participate in political discourse.[37]

The issue extends beyond overt manipulation to the very architecture of information flow. Social media platforms, using algorithms to curate users' newsfeeds based on their expressions, risk creating echo chambers or "filter bubbles." This can result in individuals receiving only confirmation of their existing views, shielded from alternative perspectives, which, can polarize society. While Article 19 of the Universal Declaration of Human Rights enshrines freedom of expression, the algorithmic shaping of what we see and engage with can subtly, yet powerfully, curtail this right. Addressing these challenges requires more than just technological fixes; it calls for a re-examination of election laws, campaign finance regulations, and platform accountability to ensure that AI serves, rather than subverts, democratic integrity. The call by the Council of Europe for AI systems not to undermine democratic institutions or access to justice is a crucial starting point.[38]

VII. The Imperative of Regulation: Towards Accountable and Transparent AI Governance

Given the profound and often unsettling impacts of AI on human rights and democratic processes, the call for robust, adaptable, and ethically grounded regulation is no longer a futuristic hypothetical but a present-day imperative. The laissez-faire approach, allowing

[35] Ibid.
[36] Van der Velde, Annelies. *The Digital Polis: AI, Democracy, and the Future of Public Discourse*. Leiden University Press, 2020, p. 83.
[37] Marda, V., & Milan, S. (2018). Report: *Wisdom of the Crowd: Multistakeholder perspectives on the fake news debate*. Internet Policy Review series, Annenberg School of Communication, p. 5.
[38] European Parliamentary Technology Assessment Network. Report: *Artificial Intelligence and Democracy*. Oslo: European Parliamentary Technology Assessment (EPTA) Network, Oct. 2024. 2024. p. 112.

innovation to outpace governance, courts significant peril. As Nemitz and others contend, nations, rather than businesses whose primary objective is profit, must lay the groundwork for ethics, anchoring it in human rights and democratic values.[39] This necessitates regulators skilled in the subject, capable of making sound judgments[40], and fostering close collaboration between policymakers and scientists to ensure democratic legitimacy and competence.[41]

A multifaceted regulatory strategy is essential, focusing on content moderation, proffers several concrete recommendations: enabling users to categorize posts to escape filter bubbles, prohibiting AI filtering that precludes human review or high degrees of human control, and educating citizens on AI systems. Similarly, ensuring AI systems are trustworthy—complying with laws, adhering to ethical ideals, and being robust against bias[39]—is paramount. The concept of a "human-in-command" strategy for AI deployment underscores the need to maintain human agency and responsibility, particularly in high-stakes decisions. A monitoring program to evaluate AI systems for transparency, safety, accountability, and ethical principles is also crucial.

India's National Strategy for AI, #AIforALL, acknowledges the need for an equilibrium between narrow financial benefits and the larger good, moving beyond purely commercial drivers. However, its initial proposals for surveillance and lack of immediate redress for bias highlighted the complexities.[42] The development of tools, checklists, and guidelines for determining acceptable definitions of fairness, especially in contexts with existing affirmative action policies like India's, is a significant policy problem.[43] Transparency and accountability are critical, particularly as AI systems, often opaque "black boxes," increasingly displace human decision-making in government sectors.[44] While complete transparency may be "evident yet naïve" for evolving AI systems,[45] establishing responsibility for complex,

[39] Floridi, L. (2018). "Soft ethics and the governance of the digital." *Philosophy & Technology*, Vol. 31(1), p. 164.
[40] IBM. "AI Governance." *Ibm.com*, 10 Oct. 2024, www.ibm.com/think/topics/ai-governance. Accessed 10 May 2025.
[41] Latonero, Mark. "Governing artificial intelligence: Upholding human rights & dignity." *Data & Society* vol. 38, 2018, p. 25.
[42] Carter, Ben, and Maria Santos. "Algorithmic Management and the New Precariat: Re-evaluating Labor Protections in the Age of AI-Driven Workplaces." *International Review of Law, Computers & Technology*, vol. 38, no. 1, 2024, pp. 45-67.
[43] Choudhry, S., Khosla, M., & Mehta, P. B. (2016). *The Oxford handbook of the Indian constitution*. 1st Edn. Oxford University Press, p. 122.
[44] Veale, M., Van Kleek, M., & Binns, R. (2018). Conference Proceeding: "Fairness and accountability design needs for algorithmic support in high-stakes public sector decision-making." *Proceedings of the 2018 chi conference on human factors in computing systems*, p. 2.
[45] Kroll, J. A. (2015). Thesis: *Accountable algorithms*. Princeton University, p. 6.

unpredictable systems is non-negotiable. Legislators must consider transparency and intelligibility as a continuum, tailoring requirements to the AI application's nature and purpose.[46]

Table 1: A Framework for Addressing Key Challenges in AI Governance: Perceived Problems and Proposed Solutions

Factor	**Perceived problem**	**Solution**
Privacy	AI makes use of data from individuals' private accounts.	Regulate the rights of users
Security	Influence in elections using AI technologies and cyberattacks	Increased openness in terms of a political party's political campaigns Certification for safety Establish a legal framework that ensures the safety of the general public including users of AI applications.
Labour rights	Job losses due to automation	Issue/regulation on a global or national scale
Accountability & Responsibility	Who is responsible when AI makes a mistake? Lack of trust may result in the cessation of AI development.	The process of developing and deploying AI should be accessible to examination and improvement. Transparency in the legislation, the process, and with the user of an AI application
AI expertise in government	Inadequate expertise results in ineffective policy. Regulating slowly	Increase funding for research through recruiting from the academic community. A centralised committee comprised of eminent scientists
National vs global issue	As this is a more global problem, national laws will have little influence.	Generally implying worldwide control

[46] Marda, V. (2017). *Machine learning and transparency: a scoping exercise*, SSRN Journal, Vol 1, p.4.

Equality	Bias by algorithms is indeed a concern.	The United Nations monitors Non - discriminatory policies are valued in organisations developing AI applications
Warfare	Terrorist danger and a machine which kills without human intervention	Completely eradicate AWS or give humans authority over deadly force decisions
Freedom of expression/political participation	Information manipulation, customised news feeds, and social media corporations serving as the primary channel for free expression	a set of principles for firms with control over social media platforms that are consistent with protections of freedom of speech.

The table 1 presented above further crystallizes key areas: regulating user data rights to counter AI's use of private accounts for privacy concerns; increasing openness in political campaigns and certifying AI for safety to address security risks; issuing global or national regulations for job losses due to automation; ensuring AI development processes are accessible for examination to enhance accountability; increasing government AI expertise and funding for research; and establishing international quasi-judicial organizations to determine the legality of online expression in collaboration with intermediaries. Ultimately, effective AI governance will require a dynamic interplay of hard "regulations, technological standards, and social norms," always with an eye toward safeguarding human dignity and democratic integrity in this new algorithmic age.[47]

VIII. Conclusion: Charting a Human-Centric Course for the Algorithmic Future

The journey through the multifaceted implications of AI reveals a technology of immense power, one that holds the dual capacity to significantly advance or severely undermine human rights and democratic foundations. From the subtle biases encoded within algorithms that perpetuate societal inequalities, to the overt challenges posed by AI-driven surveillance and its chilling effect on privacy and free expression, the "algorithmic leviathan" is no longer a distant spectre but a contemporary force reshaping our world. The automation of content moderation, while addressing the scale of online information, brings risks of censorship and the suppression

[47] Gillis, Alexander S, et al. "What Is Artificial Intelligence (AI) Governance?" *Search Enterprise AI*, TechTarget, 2025, www.techtarget.com/searchenterpriseai/definition/AI-governance. Accessed 10 May 2025.

of legitimate discourse, while AI's role in electoral processes raises profound questions about information integrity and democratic participation.

This article has synthesized insights from various analyses, including international human rights perspectives, the specificities of national AI strategies like India's, and broader democratic theory, to argue that the path forward demands more than mere technological refinement. It requires a fundamental commitment to human-centric AI governance. This means embedding principles of fairness, transparency, and accountability into the very DNA of AI systems and the legal frameworks that govern them. Recommendations ranging from enhanced user control and robust human oversight in content filtering, to stringent data protection regimes and proactive measures to combat algorithmic bias, all point towards a future where AI serves humanity, not the other way around.

However, the challenge is dynamic and ongoing. The limitations of current AI, particularly in understanding complex human contexts, necessitate humility and caution. Future research must continue to explore the evolving nature of AI, its societal impacts, and the efficacy of different regulatory models. International cooperation will be crucial, as AI's reach transcends national borders. Crafting a legal and ethical compass to navigate the complexities of the algorithmic age is perhaps one of the defining tasks of our generation. Failure to do so risks ceding too much ground to automated systems, potentially diminishing the human agency and democratic values we hold dear. The objective must be clear: to steer the algorithmic leviathan with wisdom, foresight, and an unwavering dedication to human dignity.