ARTIFICIAL INTELLIGENCE AND THE DECLINE OF PRIVACY AND FREEDOM IN THE DIGITAL AGE

Tania Dasgupta, St. Xavier's University, Kolkata

ABSTRACT

This research paper, titled "Artificial Intelligence and the Decline of Privacy and Freedom in the Digital Age," discusses how the rapid growth of Artificial Intelligence influences basic human rights, such as the rights to privacy and freedom. The main objective of this study will be to examine how AI technologies (data analytics, facial recognition, predictive algorithms, and surveillance systems) collect and process personal information and use it in ways that can threaten individual autonomy and freedom of expression. The central argument of this research is that although AI confers enormous benefits in efficiency, communication, and problem solving, without guardrails of ethical considerations, its intrusive practices can substantially interfere with private life, manipulate human conduct, and even engender mass surveillance by governments and corporations alike. The research question guiding this study is: How does the increasing use of AI technologies contribute to the erosion of privacy and freedom, and what ethical measures can ensure the protection of human rights in the digital age? This paper follows a doctrinal methodology, combining critical analysis of existing laws, international conventions, judicial decisions, and scholarly writings on related subjects of privacy, data protection, and human rights. It examines the applicability of legal instruments like the UDHR, ICCPR, GDPR, and related national legislations to assess their adequacy in responding to the emerging threats posed by AI. Through comparative legal insights, the research underlines existing gaps in the current legal protection and the need for more robust accountability mechanisms affecting AI developers and users. This work is significant because it contributes to the current global debate on how technological progress can or should be balanced against human rights. In this context, the pressing need for ethics-driven governance, transparent policy on AI, and legally binding safeguards to prevent abuse of technology is absolutely indispensable. Ultimately, this research is meant to foster a rights-based approach toward AI development, ensuring that innovation does not come at the cost of human dignity, freedom, and privacy.

Keywords: Artificial Intelligence, Privacy, Freedom, Human Rights, Surveillance

I. INTRODUCTION

"Surveillance is permanent in its effects, even if it is discontinuous in its action." — Michel Foucault, Discipline and Punish: The Birth of the Prison (Foucault, 1975)

In the 21st century, artificial intelligence (AI) has evolved from a scientific goal to a powerful element of everyday life, significantly integrated into various sectors such as healthcare, finance, and social media. While AI promises advancements in efficiency and personalization, it also raises deep concerns regarding individual liberties, primarily around privacy. The ability of AI to collect and analyze data poses existential threats to privacy and freedom, particularly within constitutional democracies like India. The rise of AI presents challenges to foundational rights enshrined in the Indian Constitution, such as the right to privacy, as recognized by the

Supreme Court in the case of Justice *K.S. Puttaswamy v. Union of India* (Justice K.S. Puttasawmy (Retd.) vs Union of India, 24 August 2017). AI systems not only risk violating informational privacy but also threaten personal autonomy through influencing decisionmaking subtly, raising serious questions about transparency and human agency.

This research paper examines the intersection of AI and the diminishing of privacy rights in India, focusing on whether current legal protections are sufficient to uphold dignity, autonomy, and democratic involvement. It highlights the urgent need for stronger legal safeguards alongside the rapid adoption of AI technologies, which may inadvertently compromise the freedoms they aim to enhance. The evolving regulatory framework in India, including the Digital Personal Data Protection Act and new AI policies, offers some protection but remains limited.(Mishra)

Moreover, the integration of AI into the judiciary, such as through case-management systems, has led to concerns regarding accountability and bias. The paper reviews constitutional law, scholarly discussions, and legislative responses while providing case studies from governance and justice sectors to illustrate the challenges posed by AI. It also assesses global legal frameworks, including the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the General Data Protection Regulation, identifying gaps that necessitate enhanced accountability for AI-related developments. A key conclusion emphasizes the need for ethical governance, clear policies, and enforceable legal measures to ensure that technological advancements enhance rather than undermine privacy, dignity, and freedom in the digital age.

II. UNDERSTANDING ARTIFICIAL INTELLIGENCE IN THE DIGITAL AGE

AI is an advanced system that simulates human intelligence, emphasizing capabilities like data learning, pattern recognition, and decision-making. A central aspect is machine learning, which uses algorithms that improve over time through training on extensive datasets for better prediction and relational discovery. Deep learning, inspired by the structure of the brain, employs multi-layered neural networks to process complex data relationships, facilitating functions like image recognition and natural language processing. Predictive analytics is vital, employing historical and real-time data for tasks such as risk assessment and behavioral predictions. The efficacy of AI relies heavily on large datasets, which enhances generalization and prediction accuracy but raises significant privacy concerns related to the handling of sensitive personal information. AI is classified into "weak AI," tailored to specific tasks without general intelligence, and "strong AI," which would possess human-like cognitive capabilities. Autonomous systems can operate independently, raising questions about legal, ethical, and constitutional implications due to reduced human oversight. The trend of shifting from humancentered decision-making to algorithmic systems across various sectors presents challenges to constitutional democracy by questioning transparency, accountability, and potential biases inherent in such automated processes. This reliance on algorithms risks undermining democratic principles like equal protection and due process. (David Leslie, 2022)

A comprehensive understanding of AI encompasses technical subjects such as machine learning, deep learning, and predictive analytics, alongside critical legal considerations. Many scholars advocated for the evolution of constitutional frameworks to adequately address the implications of algorithmic governance on privacy, individual freedoms, and adherence to democratic norms, especially as decision-making shifts increasingly towards automation.

III. THE CONCEPT AND CONSTITUTIONAL PROTECTION OF PRIVACY IN INDIA

The right to privacy in India has evolved into a fundamental right, protected by the Constitution, despite the term not being explicitly mentioned. This right involves individuals' ability to control their personal choices, information, and interactions without unwarranted intrusion from the State or private entities. It is rooted primarily in Article 21 (The Constitution of India), which safeguards the right to life and personal liberty, suggesting that an expansive interpretation of personal liberty encompasses a range of rights essential for a dignified life. Privacy is crucial for dignity, as it allows for personal choices without public intrusion, thus enabling other fundamental rights enshrined in Articles 14 (The Constitution of India) and 19 (The Constitution of India)concerning equality and freedom of expression.

The landmark judgment in Justice *K. S. Puttaswamy v. Union of India (2017)* confirmed privacy as a fundamental right under the Constitution. A unanimous nine-judge bench interpreted privacy as integral to human dignity, closely linked to the principles of Articles 21, 14, and 19 (The Constitution of India). The judgment noted that advancements in technology necessitated stronger constitutional protections, with the court pursuing safeguards that would permit justified encroachments upon privacy as long as they meet tests of legality, necessity, and proportionality. Puttaswamy emphasizes three critical facets of privacy: physical privacy, decisional autonomy, and informational privacy. Physical privacy pertains to bodily integrity and protection against unwanted physical intrusion, ensuring individuals retain control over their physical selves. Decisional autonomy protects individuals' rights to make personal choices regarding intimate matters, such as marriage, reproductive rights, and family life, free from State interference. Informational privacy, increasingly significant in the digital age, refers to individuals' control over their personal data, as information can reveal intimate aspects of life through digital footprints left across various platforms. (Justice K.S. Puttasawmy (Retd.) vs Union of India, 24 August 2017)

However, the rapid advancement of artificial intelligence (AI) poses a substantial threat to informational privacy. AI systems often operate without individuals' knowledge or consent, collecting vast amounts of personal data that can be used for surveillance, control, and commercial exploitation. These technologies compromise the ability of individuals to manage their personal information, especially as they blur the lines between private and public life, tracking behavior without adequate legal hurdles or informed consent. The Puttaswamy judgment mandates that any privacy intrusion must adhere to constitutional tests, yet AI's implementation frequently bypasses these safeguards, creating vulnerabilities and potential misuse of personal data. (Mishra)

The rise of AI technologies raises concerns about encroachments on physical privacy, influences on decisional autonomy, and severe risks to informational privacy. Ultimately, it threatens to dilute individual freedoms, emphasizing the urgent need for robust legislative and protective measures to safeguard the constitutional right to privacy in India's evolving digital landscape. (Vijayalakshmi)

IV. AI AND THE DECLINE OF HUMAN FREEDOM

At the forefront of constitutional rights are the fundamental protections for individual freedom and dignity as outlined in Articles 19 and 21 of the Constitution. Article 19 guarantees freedom of speech and expression, while Article 21 has been interpreted to include privacy, personal autonomy, and informational self-determination. (The Constitution of India) However, the rise of artificial intelligence (AI) technologies challenges these rights by undermining autonomy, suppressing genuine free speech, and manipulating individual choices through algorithmic nudging and targeted content. (Kaur, 2025)

As AI personalizes content, it may significantly shape users' beliefs, particularly vulnerable groups like young users, potentially threatening the plurality critical for a thriving democracy. The opaque nature of AI algorithm decision-making further complicates these issues, making it difficult to identify and contest biases that exacerbate existing inequalities, especially in countries like India with deeply embedded structural disadvantages. AI systems can reflect societal biases in crucial areas like credit ratings and employment, leading to systemic discrimination. (Teo, 2024)

Moreover, traditional anti-discrimination measures inadequately address the unique challenges posed by algorithmic biases, which can harm marginalized groups in subtle ways. This exacerbates threats to justice and equality, necessitating comprehensive oversight, transparency, and accountability in AI to protect the constitutional guarantees of dignity, equality, and liberty for vulnerable communities. Urgent regulatory intervention is required to combat potential automated discrimination that could act as a tool of systemic oppression in the digital era. (Sumitra, 2025)

V. AI GOVERNANCE IN INDIA: EXISTING LEGAL AND POLICY FRAMEWORK

The AI governance framework in India lacks a comprehensive statute, relying on existing laws that create regulatory gaps. The Digital Personal Data Protection Act, 2023 (DPDP Act) is a significant advancement, establishing a personal data management framework emphasizing informed consent and personal rights, aligning with global privacy standards similar to European regulations. It enhances protections for sensitive health data and builds trust in digital health services. However, the DPDP Act has limitations, including a narrow scope, reliance on unnotified rules, and concerns about the independence and enforcement capability of the proposed Data Protection Board (DPB), potentially constraining transparency and public oversight, particularly under the Right to Information Act, 2005 (RTI Act).

The Aadhaar Act, 2016, despite being upheld by the Supreme Court, raises concerns about biometric data misuse and identity theft risks, especially with amendments allowing application to private entities. The earlier Information Technology Act, 2000, aimed at cyber security and personal information but did not provide adequate data protection, with its amendments being reactive rather than proactive regarding data privacy rights. (Ms. Mohita Yadav, 2025)

The National Strategy for Artificial Intelligence, launched by NITI Aayog in 2018, envisions AI benefits in sectors like agriculture and healthcare but is criticized for lacking enforceable measures. Judicial efforts to use AI for improving court efficiency indicate progress, yet highlight ongoing regulatory gaps. Currently, there's no specific AI law in India, leading to a lack of binding standards for algorithmic accountability and transparency. Existing data protection and cyber laws do not address unique issues posed by AI, such as bias and discrimination. The absence of independent audits and transparent mechanisms poses significant risks as AI technologies expand. Despite progress represented by the DPDP Act and strategic frameworks, the lack of robust AI-specific legislation leads to oversight and accountability gaps, undermining individual rights and exacerbating structural inequalities. For a fair and trustworthy AI ecosystem, India needs regulations focused on algorithmic transparency, impact assessments, rights to explanation, accountability frameworks, independent oversight, and public engagement. (Rakesh, 2025)

VI. COMPARATIVE GLOBAL APPROACHES TO AI REGULATION

The global regulatory landscape for artificial intelligence (AI) demonstrates diverse approaches, offering insights for India's AI governance structure. The European Union (EU) presents a comprehensive model with its General Data Protection Regulation (GDPR) and the upcoming AI Act, imposing strict obligations for transparency, data minimization, explicit consent, and accountability, alongside a risk-based assessment system requiring human oversight for high-risk AI systems. In contrast, the United States adopts a fragmented approach, leveraging the Algorithmic Accountability Act and state privacy laws like the California Consumer Privacy Act, mandating audits for high-impact automated tools and guaranteeing rights against unfair automated decisions. The UK fosters an innovation-friendly regulatory environment with sector-specific oversight that promotes responsible AI development without stifling progress. Conversely, China's interventionist model enforces strict regulations on algorithmic recommendations and facial recognition technologies aimed at ensuring social stability and state security. (Bidhuri, 2025)

These global frameworks impart key lessons for India, highlighting the necessity of enforceable transparency requirements, mandatory human reviews in critical sectors (e.g., healthcare, policing, welfare), and data minimization as essential obligations. Clear rights for citizens to seek explanations and corrections against automated decisions are also crucial. This analysis correlates with international human rights standards, such as the Universal Declaration of Human Rights and the International Covenants on Civil and Political Rights, which emphasize privacy, expression freedom, and equality, all impacted by AI-driven profiling. (Pouya Kashefi, 2024)

Additionally, the UN Guiding Principles on Business and Human Rights call for states to shield against corporate harms, necessitating human rights due diligence within algorithmic systems. Soft law standards from the OECD and UNESCO highlight fairness, accountability, and oversight in AI use. Despite India's Constitution safeguarding privacy and personal liberty under Article 21, and ensuring equality under Articles 14 and 15, there is currently no comprehensive legal framework ensuring algorithmic transparency or accountability for developers. Therefore, India can bolster its AI regulatory framework by integrating lessons from these comparative models and aligning them with international human rights commitments to foster trustworthy, people-centered AI ecosystems. (Bidhuri, 2025)

VII. CASE STUDIES HIGHLIGHTING AI-DRIVEN RISKS IN INDIA

Indranil Mullick & Ors. v. Shuvendra Mullick (2025) – CCTV Surveillance in a Residential House

In 2025, the Calcutta High Court faced a case where co-inhabitants of a house questioned the fitting of CCTV cameras inside a shared residence without their permission. In that dispute, the court set aside an earlier order of the city-civil court that had refused an injunction against running such cameras. The High Court held that setting up CCTV cameras in a residential area without the consent of all co-occupants was a violation of the fundamental right to privacy. ([lawfultalks.net][1]) The Supreme Court of India, on appeal, upheld the judgment of CHC and confirmed that any hidden video surveillance in private homes - without residents' consent - breaches constitutionally protected privacy. This case illustrates concretely that modern video/biometric surveillance-even "ordinary" CCTV-is subject to constitutional scrutiny under the right to privacy.

While this is not, strictly speaking, "AI used by the State," it represents an important judicial recognition of privacy harm via technological surveillance - which, when upgraded to AI-based face recognition or mass CCTV + analytics, would carry still greater risks. (Indranil Mullick and Ors. vs. Shuvendra Mullick, 2025)

Akhilesh Kumar Kandasamy v. State of Tamil Nadu - Ongoing challenge, filed 2023.

A petition was filed by Mr. Akhilesh Kumar Kandasamy in August 2023 before the Madras High Court, contesting the Tamil Nadu Police's deployment of Facial Recognition Technology (FRT) throughout the state, with a focus on Chennai. The petitioner argues that this deployment lacks consent, occurs covertly, and is not supported by any statutory framework, failing to meet the proportionality and necessity criteria established by the Supreme Court in the landmark case K.S. Puttaswamy (Retd.) v. Union of India (2017).

The concerns raised in the petition include the assertion that the Tamil Nadu police began utilizing FRT as early as 2021-2022 through a mobile application linked to an existing state database of images housed in the State Data Center. While the State attempts to justify its actions using the old Police Act and the Code of Criminal Procedure, the petition challenges this justification, asserting that general laws cannot effectively replace a dedicated legislative framework specifically addressing mass biometric surveillance.

As a result, the Madras High Court has issued a notice to the State and is set to consider the petition. This legal challenge directly questions the legality and constitutionality of deploying AI-based facial recognition by police in India, invoking fundamental constitutional rights related to privacy, equality, and dignity. (Akhilesh Kumar Kandasamy vs State of Tamil Nadu, 2023)

Welfare-Algorithm Exclusion Cases — e.g. from The Reporters' Collective investigation (2024):

In January 2024, The Reporters' Collective, with support from the Pulitzer Center, published a significant investigative series titled "Algorithms of Exclusion," which revealed how the Government of Telangana utilized an algorithmic profiling system called the "Samagra Vedika" platform to create comprehensive profiles of citizens for determining welfare benefits eligibility. The report highlighted substantial errors within the algorithm, which resulted in the wrongful exclusion of many individuals in genuine need, including widows, slum dwellers, and daily wage workers. Specific instances included individuals misclassified as asset owners, such as a car, or incorrectly recorded as deceased in state databases, leading to the abrupt loss of pensions. A notable case featured a 67-year-old widow denied subsidized food due to an algorithmic error. Officials often refused to amend these mistakes, treating the algorithmic decisions as infallible. Though these instances have not been adjudicated in court, they represent grave violations of fundamental rights, including dignity, equality, and access to essential entitlements, caused by opaque and unreliable algorithmic decision-making. (Tapasya, 2024)

VIII. AI IN PREDICTIVE POLICING AND CONSTITUTIONAL RISKS

AI in Predictive Policing and Constitutional Risks highlights significant constitutional issues arising from the use of Facial Recognition Technology (FRT) by police forces, as illustrated in the Kandasamy petition. The landmark Puttaswamy decision established that privacy is a fundamental right under Article 21, necessitating that state invasions meet legality, necessity, and proportionality criteria. Lawyers and civil rights advocates note that many FRT deployments occur without clear legislation, are non-transparent, and lack essential safeguards like data retention limits. The mass scanning enabled by FRT can deter free expression, assembly (Article 19), and liberty (Article 21). Wrongful identifications may threaten fair trial rights, undermining the presumption of innocence (Article 14), prompting calls from various organizations for a halt on mass FRT until appropriate legal and institutional safeguards are established. Additionally, AI in welfare systems poses risks of exclusion and discrimination against vulnerable communities. Investigations reveal that algorithms determining eligibility for welfare benefits can result in severe deprivation when misclassifications occur, infringing on rights to equality, non-discrimination, and livelihood (Articles 14, 15, and 21). The decisionmaking process remains opaque, leaving marginalized groups, who often lack resources and digital literacy, without recourse against algorithmic errors. This scenario cultivates a discriminatory environment under a facade of neutrality, raising ethical issues concerning justice, dignity, and equity.

The role of AI in judicial processes also warrants caution due to potential risks to due process and accountability. Although there is limited public documentation of AI usage in Indian courts, discussions surrounding its implications are intensifying. Concerns persist that AI tools can function as "black boxes," leading to decisions that lack transparent reasoning, violating the fair hearing tenet of Article 21. Furthermore, biases in AI training data may entrench systemic injustices, especially impacting marginalized populations. The push for efficiency amid a backlog of cases raises the risk that reliance on AI may compromise fairness and individual rights without proper regulatory oversight and a robust constitutional framework. Overall, the integration of AI across these domains in India requires significant attention to transparency, accountability, and the protection of fundamental rights. (R, 2025)

IX. INTERNATIONAL HUMAN RIGHTS FRAMEWORK AND AI

Discussion of artificial intelligence in the context of international human-rights law identifies critical normative frameworks related to privacy, liberty, dignity, and accountability, comparing India's constitutional provisions with global standards. The UDHR, ICCPR, and ICESCR provide foundational human rights protections, emphasizing the indivisibility and interdependence of all rights. The UN Guiding Principles on Business and Human Rights outline the responsibilities of states and enterprises to uphold these rights in AI systems, ensuring non-infringement on privacy, freedom of expression, and due process.

AI-ethics frameworks, such as the OECD Principles and UNESCO Recommendation, highlight the necessity for AI systems to respect human rights, ensuring fairness, transparency, and accountability throughout their life cycles. These global standards are especially pertinent as AI technologies impact fundamental rights. Scholars advocate for human rights impact assessments and the integration of technical safeguards alongside legal protections.

In India, while Article 21 safeguards life and personal liberty, the recognition of a "right to privacy" marked a notable alignment with international human rights standards, signified by the Supreme Court's decision in K.S. Puttaswamy v. Union of India (2017). However, gaps remain; privacy is not explicitly contained in the Constitution, leading to reliance on judicial interpretation. Despite a normative framework around privacy and AI, the lack of comprehensive data protection legislation presents a significant constitutional challenge.

To align with international human rights standards, India must enact robust data protection and AI governance laws, establishing independent oversight, ensuring transparency and accountability, and embedding core values such as fairness and informed consent in AI deployment. (Agarwal, 2025)

X. ETHICAL CHALLENGES IN AI DEPLOYMENT

The rapid deployment of AI systems across various sectors presents significant ethical challenges, particularly in relation to the principles of fairness, accountability, transparency, responsibility, and explainability (FATRE). Fairness is compromised when AI models replicate or exacerbate societal biases, especially since many are trained on data reflecting historical prejudices. This is critical in diverse societies, like India, where socio-economic, cultural, and linguistic disparities exist. Biased algorithms can lead to discriminatory impacts in crucial areas such as hiring, credit access, healthcare, and social welfare, thereby jeopardizing social equity. Transparency and explainability are undermined by the opacity of many AI systems, often described as "black-box" models. When decision-making processes are not interpretable, it complicates auditing and rectifying potentially harmful outcomes, such as wrongful denial of social benefits or healthcare misdiagnoses. This ambiguity raises questions about accountability: it may be unclear whether liability lies with developers, deployers, or operators. There is also an evident power imbalance among large technology firms that create and employ AI, governing bodies that regulate or utilize these systems, and everyday citizens adversely affected by AI decisions. Such dynamics risk consolidating power and decision-making into the hands of a few, risking the erosion of democratic accountability. The deployment of AI not only reflects social structures but may also deepen inequalities, exploit labor, and perpetuate structural biases.

Additionally, AI usage risks undermining individual autonomy and facilitating manipulation. When opaque algorithms govern access to essential services like jobs and healthcare, individuals may lose control over substantial aspects of their lives. There is also a potential for governments or powerful entities to leverage AI systems for influence or surveillance, exacerbating digital inequality among varying societal strata, particularly impacting those with limited access to resources, education, or digital literacy.

Thus, neglecting CPU principles in AI deployment can lead to the persistence and intensification of social injustices, compromising individual agency, diminishing public trust, and centralizing societal power instead of democratizing technological benefits. (OwusuBerko, 2025)

XI. NEED FOR A COMPREHENSIVE AI REGULATORY FRAMEWORK IN INDIA

In order to establish an effective AI-law or policy framework for India, it is crucial to ensure algorithmic transparency and explainability in AI systems deployed across governance, public services, policing, welfare, justice, and decision-making processes. This necessitates that the underlying logic, data inputs, and criteria of decisions made by these AI systems are accessible for independent scrutiny and comprehensible to affected individuals. The framework must include the establishment of an autonomous regulatory body, free from direct executive influence, comprised of diverse stakeholders such as technical experts, civil society members, representatives of marginalized communities, and legal scholars. This body would be responsible for auditing AI systems, ensuring compliance with the established norms, mandating corrections or suspensions when risks are identified, and imposing penalties for misuse or discrimination.

Furthermore, it should grant specific rights to citizens, including the right to explanation, allowing individuals to request clear justifications for decisions made about them; the right to correction, giving the ability to contest and amend any incorrect or biased data utilized by the AI; and the right to opt-out of purely automated decision-making, particularly in circumstances involving fundamental rights or entitlements. The policy must incorporate ethical guidelines that are enforceable by law, establishing mandatory standards such as fairness, nondiscrimination, proportionality, privacy protection, data minimization, and accountability rather than leaving compliance as a voluntary measure. Given the significant implications of AI in critical sectors like justice, policing, and welfare, it is essential to implement mandatory human oversight mechanisms. While AI can provide analytical support or recommendations, the final decisions impacting individuals' liberty, access to justice, welfare rights, or fundamental rights must rest with human decision-makers, who should have the authority to review, contextualize, and, if necessary, override AI-generated outputs. This comprehensive regulatory framework aims to enhance human competencies and effectiveness through AI while upholding constitutional principles surrounding justice, dignity, equality, and accountability.

XII. CONCLUSION

In conclusion, this research paper reveals that the rapid advancement of artificial intelligence (AI) within India's digital realm presents both significant opportunities and serious dangers to the core values of privacy, dignity, liberty, and equality as enshrined in the Indian Constitution. While AI offers prospects for efficiency, economic growth, and innovation, the research illustrates that, without robust safeguards, AI systems are increasingly compromising the three pivotal aspects of privacy identified in *Justice K.S. Puttaswamy v. Union of India*: physical privacy, decisional autonomy, and informational privacy. Instances of this erosion include intrusive CCTV surveillance within residences, unregulated police facial recognition techniques, opaque algorithmic welfare programs leading to societal exclusion, and AI-driven content curation that influences individual choices, all of which showcase how AI can covertly undermine essential constitutional protections under Articles 14, 19, and 21.

The analysis confirms that these threats are not merely hypothetical but are currently impacting citizens' rights and freedoms. A comparison of India's disjointed legal framework—overseen primarily by the limited Digital Personal Data Protection Act and various sector-specific regulations—with international regulatory frameworks like the EU's General Data Protection Regulation (GDPR), China's algorithm regulations, and the human-rights guidelines provided by organizations such as the UN, OECD, and UNESCO, points out significant deficiencies in India's strategy. The nation currently lacks enforceable measures for algorithmic accountability, transparency, fairness, explainability, human oversight, and effective avenues for remedy, allowing AI systems to function as "black boxes" free from democratic accountability, thereby perpetuating social disparities and undermining due process.

Thus, the findings indicate an urgent need for India to establish a comprehensive AI regulatory framework rooted in constitutional values and shaped by global best practices. Such a system should ensure algorithmic transparency, independent regulatory oversight, enforceable ethical obligations, and explicitly defined rights for individuals, including the rights to explanation, correction, and protection against automated decision-making. Furthermore, it is essential for India to require human oversight in critical areas like policing, welfare, and justice to guarantee that technology enhances, rather than replaces, human judgment and responsibility. Ultimately, the paper asserts that the future development of AI in India must prioritize not only innovation but also the steadfast safeguarding of human dignity, autonomy, equality, and democratic freedom. A rights-based, accountable, and transparent governance model for AI is imperative for India to ensure that technological advancements bolster—rather than undermine—the constitutional foundation of the nation.

XIII. SUGGESTIONS

1. It is desirable that India enacts a specific and detailed AI law that demarcates how artificial intelligence can be used by both the State and private companies.

   Moreover, such a law is required to address issues peculiar to data collection, automated decision-making, surveillance systems, and algorithmic discrimination, so that AI does not violate the constitutional rights granted under Articles 14, 19, and 21.

2. The government needs to enact strict regulations that will enforce algorithmic transparency and explainability in regard to all AI systems used in public decision-making.

   That means a person should be able to comprehend how this AI system came up with a particular decision, based on what data, and if the decision was biased or unbiased.

3. An Independent National AI Regulatory Authority, with full legal powers to monitor, audit, and penalize misuse of AI, should be established in India.

   This body should be free of any government or corporate influence and should include a wide variety of technical experts, legal scholars, representatives from civil society, and members from the most marginalized communities to hear all voices.

4. Legal rights such as the right to explanation, right to correction of data, and right to challenge or opt out of automated decisions should be provided to the citizens.

   These rights will enable them to protect themselves from wrongful profiling, biased decisions, and other harmful data practices.

5. Application of AI systems in sensitive domains such as policing, welfare delivery, and the judiciary should be done only under strong human oversight and accountability.

No fully automated tool should be able to make final decisions about a person's liberty, welfare benefits, or legal rights without a responsible human reviewing and validating the outcome.

6. Mass surveillance technologies, such as facial recognition, predictive policing, and analytics linked to CCTV should be strictly curtailed by the government.

   These tools should be deployed only after passing strict tests of legality, necessity, and proportionality, as required by the Puttaswamy judgment.

7. The introduction of any high-risk AI systems by a government or private entity shall be preceded by Mandatory AI Impact Assessments.

   Such scrutiny should analyze the individual impacts on privacy, equality, autonomy, and freedom, and must be subject to public disclosure for transparent purposes.

8. The law should enforce strict data minimization rules, so AI systems collect and use only the minimum amount of personal data necessary for a task.

   This will decrease unwarranted surveillance, reduce data leaks, and protect individuals from intrusive profiling.

9. This could take the form of governmental and company-level regulations around regular algorithmic audits that identify and eliminate biases harmful to marginalized groups. Audits of this kind would help ensure that the functioning of AI does not perpetuate existing social inequality and discriminate based on caste, gender, religion, or economic standing.

10. Public institutions should set up clear grievance-redressal mechanisms through which people can report AI-related harms and receive swift remedies.

    Any forms of wrongful welfare exclusion, incorrect facial recognition, or discriminatory automated decisions that citizens may face must have means of appeal that are accessible.

11. India should adopt international human rights standards-including those from the UDHR, ICCPR, OECD, and UNESCO AI Ethics Recommendations-into its domestic AI governance.

    Such alignment will reinforce accountability, equity, and human dignity within AI governance.

12. Educational and awareness programs should be put in place to help citizens understand how AI systems use their data and how they can exercise their rights.

    Greater public digital literacy will reduce manipulation, protect autonomy, and better enable people to challenge harmful AI practices.

13. Private companies and public authorities operating AI systems should be legally bound to make a public declaration of the purpose, risks, and sources of data feeding them. This kind of transparency will build trust and allow independent review of potential harms before they occur.

14. AI systems that impact political opinion, public debate, or social media content must be managed in such a way to avoid manipulation and protect democratic freedom.

    Rules should preclude any forms of algorithmic nudging and micro-targeting that distort freedom of expression or influence voting behaviour without users' awareness.

15. India should establish strict policies to ensure the use of AI in ethical ways in healthcare, finance, education, and employment to avoid discrimination and promote human dignity.

16. Sector-specific standards, such as fairness testing, informed consent, and periodic reviews, will help AI benefit society without undermining individual rights.

REFERENCES

Agarwal, S. (2025). ARTIFICIAL INTELLIGENCE AND THE RIGHT TO PRIVACY: A CONSTITUTIONAL CHALLENGE FOR INDIA. *Indian Journal of Law and Legal Research, VII*(IV).

Akhilesh Kumar Kandasamy vs State of Tamil Nadu, WP 24338/2023 (Madras High Court September 1, 2023).

Bidhuri, H. (2025). Regulating Artificial Intelligence in India: Bridging the Legal Vacuum. *International Journal of Law, 11*(4), 112-114.

David Leslie, C. B. (2022, February 6). Human rights, democracy, and the rule of law assurance framework for AI systems . europe: The Coucil of Europe's Ad Hoc Committee on Artificial Intelligence.

Foucault, M. (1975). *Discipline and Punish, The Birth of the Prison.* New York: s Surveiller et Puntr: Neusmce de Ia pruonby.

Indranil Mullick and Ors. vs. Shuvendra Mullick, SLP(C) 12384/2025 (Supreme Court of India May 11, 2025).

Justice K.S. Puttasawmy (Retd.) vs Union of India, Writ Petition (Civil) No. 494 of 2012 (Supreme Court of India August 24, 24 August 2017).

Kaur, R. (2025). Algorithmic Bias and Constitutional Safeguards in the Indian Judiciary: A

Critical Analysis of AI Integration in Legal Adjudication. *International Journal of Law Management and Humanities, 8*(4). https://doij.org/10.10000/IJLMH.1110679

Mishra, P. (n.d.). The Constitutional Right to privacy in India and challenges posed by Artificial Intelligence. *Indian Journal of Law and legal Research, VII*(IV).

https://www.ijllr.com/post/the-constitutional-right-to-privacy-in-indiaand-challenges-posed-by-artificial-intelligence

Ms. Mohita Yadav, D. A. (2025). Indian Privacy laws and the need for reform in the light of Artificial Intelligence. *International Journal of Social Science Research (IJSSR), 2*(3).

https://doi.org/10.70558/IJSSR.2025.v2.i3.30364

Owusu-Berko, J. K. (2025). Algorithmic bias, data ethics, and governance: Ensuring fairness, transparency and . *World Journal of Advanced Research and Reviews, 25*(2). https://doi.org/10.30574/wjarr.2025.25.2.0571

Pouya Kashefi, Y. K. (2024). Shaping the future of AI: balancing innovation and ethics in global regulation. *OXFORD ACADEMIC Uniform Law Review, 29*(3), 524-528.

R, K. (2025). PREDICTIVE POLICING AND CONSTITUTIONAL MORALITY: AN

EVALUATION OF AI-BASED CRIME FORECASTING TECHNOLOGIES IN

INDIA. *LawFoyer International Journal of Doctrinal Legal Research, 3*(2). https://doi.org/10.70183/lijdlr.2025.v03.75

Rakesh. (2025). Why we need Data Protection Laws for AI in India. *DE FACTO LAW JOURNAL, 1*(1).

Sumitra, P. S. (2025). FREEDOM OF SPEECH IN THE DIGITAL AGE: CHALLENGES OF ALGORITHMIC CENSORSHIP AND AI MODERATION. *Lex Localis, 23*(26). https://doi.org/10.52152/84jfyc65

Tapasya, K.S. (2024, January 24). *ALJAZEERA*. aljiazeera.com.

https://www.aljazeera.com/economy/2024/1/24/how-an-algorithm-denied-food-tothousands-of-poor-in-indias-telangana

Teo, S. A. (2024). Artificial intelligence and its ‘slow violence’ to human rights. *Springer*.

https://doi.org/10.1007/s43681-024-00547-x

The Constitution of India. (n.d.).

Vijayalakshmi. (n.d.). *Informational Privacy and Data Protection In India.* Asian Law and

Public Policy Review. https://doi.org/10.55662/ALPPR.2019.402