

# THE IMPACT OF ARTIFICIAL INTELLIGENCE ON THE RIGHT TO PRIVACY -CONSTITUTIONAL LAW PERSPECTIVE

---

**Dr Ramesh Kumar Singh**

Assistant professor

Veer Kunwar Singh University, Ara Bihar

Posted at Maharaja Law College, Ara

Sub - Law

---

## ABSTRACT

**Aim:** This paper attempts to create an intersection that is associated between AI-related technologies and the basic right to privacy. It looks at a more focused area, specifically in India; challenges arising from AI domains such as surveillance, data mining, and facial recognition are examined while introducing a problem with India-the difficulty of ensuring and proving privacy protection at an individual level and in comparison with the parameters established by Indian law.

**Method:** The paper is based upon qualitative legal research methodology and a discussion of several constitutional provisions in case law through the relevant applicable legal frameworks and structures. It introduces Article 21 of the Indian Constitution, enshrining fundamental rights related to the right to life and liberty, and expounds upon and analyses landmark judgements like that in *K.S. Puttaswamy v. Union of India* (2017). The study also evaluates the Digital Personal Data Protection Act, 2023, and the draft Digital Personal Data Protection Rules, 2025, in comparison with international privacy regulations such as the General Data Protection Regulation of the European Union to determine their adequacy in addressing AI-related privacy concerns. Other ethical considerations, such as risks of surveillance and algorithmic discrimination, are also discussed.

**Results:** The analysis reveals that in spite of developmental benefits AI offers to society, an evaluation involving data collections, profiling, and mass surveillance still poses significant privacy risks. A comparison with Indian and international frameworks reveals gaps in the existing legal arrangements, and therefore, privacy protection needs to be stronger to overcome these challenges.

**Findings:** The study has identified that AI raises significant privacy concerns, particularly when it comes to mass surveillance, data profiling, and algorithmic bias. While the Digital Personal Data Protection Act, 2023, and the draft Digital Personal Data Protection Rules, 2025, provide some degree of legal protection, they fall short of being comprehensive in handling the risks of AI. This shows the need for better regulations and ethical governance mechanisms to ensure the development and deployment of AI technologies with respect to responsibility and protection of privacy rights.

**Conclusion:** In conclusion, this paper advocates for a balanced approach to AI development, emphasizing the protection of fundamental rights such as privacy through judicial oversight, robust ethical frameworks, and transparent legal mechanisms. Laws should encourage innovation while maintaining respect for individual privacy, ensuring AI systems are not misused to infringe upon citizens' rights.

**Keywords:** General Data Protection Regulation, Artificial Intelligence, Article 21, Indian Constitution, Right to Privacy, K.S. Puttaswamy v. Union of India, Privacy Protection

## 1. INTRODUCTION

AI has dramatically changed different aspects of human life and transformed various sectors like healthcare, finance, education, and governance (Stahl & Wright, 2018)<sup>1</sup>. The deployment of AI has immense benefits in terms of efficiency, automation, and decision-making; however, its use raises huge legal and ethical issues, mainly related to privacy rights (Cath et al., 2018)<sup>2</sup>. As AI systems are deepened in complexity, they can collect, process, and analyze vast amounts of personal data that often do not obtain explicit consent from the people involved (Villaronga, Kieseberg & Li, 2018)<sup>3</sup>. This has brought about widespread debate regarding whether existing legal frameworks are enough to protect fundamental rights to privacy. From facial recognition technologies to predictive policing and algorithmic surveillance, AI-powered tools have posed challenges that lie against constitutional protections, necessitating a reassessment of privacy laws as well as regulatory mechanisms (Roberts et al., 2021)<sup>4</sup>.

In a significant number of jurisdictions, the right to privacy has been established as a very important human right under constitutional law. Landmark legal decisions worldwide have settled that privacy forms an

---

<sup>1</sup> B. C. Stahl & D. Wright, Ethics and Privacy in AI and Big Data: Implementing Responsible Research and Innovation, 16 IEEE SEC. & PRIVACY 26 (2018).

<sup>2</sup> C. Cath et al., Artificial Intelligence and the 'Good Society': The US, EU, and UK Approach, 24 SCI. & ENG'G ETHICS 505 (2018).

<sup>3</sup> E. F. Villaronga, P. Kieseberg & T. Li, Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten, 34 COMPUT. L. & SEC. REV. 304 (2018).

<sup>4</sup> H. Roberts et al., The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation, in SPRINGER INTERNATIONAL PUBLISHING 47-79 (2021).

[www.ijesrr.org](http://www.ijesrr.org)

Email- [editor@ijesrr.org](mailto:editor@ijesrr.org)

integral part of dignity, autonomy, and personal liberty. But AI-based technologies undermine traditional interpretations of law around the concepts of privacy by allowing mass surveillance, data mining, and predictive analytics with minimal human oversight (Adams-Prassl, 2019)<sup>5</sup>. Today, governments, corporations, and other entities have access to personal information that has never been seen before, raising the specter of misuse, lack of transparency, and erosion of civil liberties. The question remains whether existing constitutional protections are enough to address the risks of AI or whether new legal frameworks must be developed to balance innovation and privacy.

Moreover, the issue of privacy impacts AI differently based on the divergent legal approaches. While many countries have tightened data protection in their laws; for instance, the European Union has the GDPR, others embrace a more minimalist approach to law (Amann et al., 2020)<sup>6</sup>. This differential calls for some form of agreement at the global legal level toward AI governance; otherwise, individuals' rights with regard to private information will get trampled through technological advancements. Moreover, constitutional courts are critical in the interpretation and enforcement of privacy rights in the age of AI. Judicial intervention will define the contours of privacy, set accountability mechanisms for AI-driven decisions, and create legal precedents that will shape future regulatory frameworks (Latonero, 2018)<sup>7</sup>.

As a given background condition, this research will explore the intersection of AI technologies and constitutional law at greater length (Perc, Ozer & Hojnik, 2019)<sup>8</sup>. It is going to identify what impact AI brings to the fundamental right to privacy, assess existing legal protections, and possible legal and policy measure suggestions on emerging challenges. This study attempts to contribute to the ongoing debate on AI regulation and constitutional safeguards by examining key judicial decisions, legislative developments, and ethical considerations (Safdar, Banja & Meltzer, 2020)<sup>9</sup>. As AI continues to evolve, legal scholars, policymakers, and technology developers must work together to ensure that privacy remains a protected and inviolable right in the digital age.

## 1.1 The Growing Influence of Artificial Intelligence on Privacy

The rapid growth of artificial intelligence (AI) in every facet has rapidly transformed the processing and recording of data, surveillance, and decision-making processes. Efficiency and innovation are promoted

---

<sup>5</sup> J. Adams-Prassl, What If Your Boss Was an Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work, 41 COMP. LAB. L. & POL'Y J. 123 (2019).

<sup>6</sup> J. Amann et al., Explainability for Artificial Intelligence in Healthcare: A Multidisciplinary Perspective, 20 BMC MED. INFORMATICS & DECISION MAKING 1 (2020).

<sup>7</sup> M. Latonero, Governing Artificial Intelligence: Upholding Human Rights & Dignity, 38 DATA & SOC'Y (2018).

<sup>8</sup> M. Perc, M. Ozer & J. Hojnik, Social and Juristic Challenges of Artificial Intelligence, 5 PALGRAVE COMM'NS 1 (2019).

<sup>9</sup> N. M. Safdar, J. D. Banja & C. C. Meltzer, Ethical Considerations in Artificial Intelligence, 122 EUR. J. RADIOL. 108768 (2020).

[www.ijesrr.org](http://www.ijesrr.org)

Email- [editor@ijesrr.org](mailto:editor@ijesrr.org)

through AI, but gathering, analyzing, and retaining massive amounts of personal data is a monumental issue regarding privacy. These technologies are often used in facial recognition, predictive analytics, and automated decision-making without explicit user consent, thus violating users' rights to privacy (Greenstein, 2022)<sup>10</sup>. These developments call for a review of the adequacy of existing legal and constitutional protections so that advances in AI do not compromise individual privacy and fundamental rights.

## 1.2 Constitutional Protection of Privacy Rights in the AI Era

Right to privacy is the fundamental part of Article 21 of the Indian Constitution, and it has been reaffirmed by the landmark judgment of *K.S. Puttaswamy v. Union of India* (2017). With the emergence of AI-driven surveillance and automated decision-making, there are new challenges to this right. Mass data collection, in the name of facial recognition, data profiling, and predictive analytics, happens in a way where there is little oversight and chances of infringement on privacy increase. These concerns give way to stronger legal safeguards that regulate the impact of AI on individual freedoms and privilege the protection of privacy under constitutional law.

## 1.3 Addressing AI-Related Privacy Risks: The Need for Legal Reforms

India's Digital Personal Data Protection Act, 2023, makes a huge stride in the world of data privacy regulation, yet it is totally silent on provisions related to AI, where a lot of concerns arise with issues like automated decision-making, profiling, and mass surveillance. For instance, regulations like GDPR implement more stringent conditions for AI-related accountability and transparency. Without explicit AI-related rules in India, there is legal protection lapse leading to an increase in privacy infringement risks. To protect individual rights, full legal reforms are required, such that AI technologies operate ethically and within constitutional privacy safeguards.

## 2. REVIEW OF LITREATURE

**Villaronga, Kieseberg, and Li (2018)** illustrated how artificial intelligence affects the right to forget. It showed the AI systems as retaining and processing large amounts of personal data long after an individual attempts to eradicate his digital footsteps. Their study points out how well AI remembered and

---

<sup>10</sup> S. Greenstein, Preserving the Rule of Law in the Era of Artificial Intelligence (AI), 30 ARTIFICIAL INTELLIGENCE & L. 291 (2022).

[www.ijesrr.org](http://www.ijesrr.org)

Email- [editor@ijesrr.org](mailto:editor@ijesrr.org)

reconstructed data created a problem that negated the current legal systems to effectively ensure privacy rights. The authors posited that despite the best intentions of the GDPR and other data protection regulations in providing more individual control over one's data, the technicality of AI presents a significant difficulty in enforcing compliance (Keskinbora, 2019)<sup>11</sup>.

**Contissa et al. (2018)** discussed the intersection of AI and privacy policies by designing Claudette, an AI-based system that aimed to evaluate the compliance of data protection policies in relation to the GDPR. They demonstrated how AI could be applied to automate the evaluation of privacy policies, potentially identifying violations and gaps in compliance. However, they pointed out that AI-based tools, despite enhancing transparency and regulatory oversight, introduced risks about bias, accuracy, and interpretability. The study indicated that while automated privacy policy assessment could help the regulatory body, it would not replace the judgment of human law (Contissa et al., 2018)<sup>12</sup>.

**Raso et al. (2018)** analyzed the wider relationship between AI and human rights, outlining potential opportunities as well as potential risks within the deployment of AI. Discussed was the same AI technology that had the potential to bring greater efficiency and innovation but would also pose a possible threat to the core rights, especially privacy. Such concerns included AI-driven surveillance, profiling data, and discriminatory decision-making that could weaken constitutional protections. It should be balanced as the regulatory approach that maximizes the benefits from AI while limiting the risks towards privacy and other human rights (Raso et al., 2018)<sup>13</sup>.

**Murdoch (2021)** analyzed the challenges posed by artificial intelligence in protecting health information, emphasizing that the risks associated with data breaches, unauthorized access, and ethical dilemmas have increased in AI-driven healthcare systems. The research pointed out that AI-based medical applications rely more on large amounts of data and raise questions on patient consent, data ownership, and regulatory compliance. Murdoch said, while AI would likely revolutionize health care with superior diagnostics and recommendation of treatments, the law currently is incapable of keeping pace with the developments of technology and was unable to adequately protect the individual's privacy rights (Murdoch, 2021)<sup>14</sup>.

---

<sup>11</sup> K. H. Keskinbora, Medical Ethics Considerations on Artificial Intelligence, 64 J. CLIN. NEUROSCIENCE 277 (2019).

<sup>12</sup> G. Contissa et al., Claudette Meets GDPR: Automating the Evaluation of Privacy Policies Using Artificial Intelligence, SSRN 3208596 (2018), <https://ssrn.com/abstract=3208596>

<sup>13</sup> F. A. Raso et al., Artificial Intelligence & Human Rights: Opportunities & Risks, BERKMAN KLEIN CTR. RES. PUB. 2018-6 (2018).

<sup>14</sup> Cath B. Murdoch, Privacy and Artificial Intelligence: Challenges for Protecting Health Information in a New Era, 22 BMC MED. ETHICS 1 (2021).

**Felzmann et al. (2019)** dived deep into the role of transparency in AI governance. The research focused on the tension between the obligations of legal transparency and the contextual concerns over AI decision making. Their work studied whether the existing obligations of legal transparency related to privacy laws, as enshrined in GDPR, could be sufficient in a more complex system of AI-driven systems. While the legal norms had demanded transparency, most AI models were "black boxes," leaving users unable to understand how a decision was arrived at. To improve AI transparency, the authors argued that improving legal compliance needed to be combined with the creation of user-friendly mechanisms that can facilitate meaningful explanations of AI-driven outcomes (Felzmann et al., 2019)<sup>15</sup>.

### 3. METHOD

This study adopts qualitative legal research as a methodology for the investigation into the effects of artificial intelligence on the right to privacy from the constitutional law viewpoint. The study is mainly doctrinal in approach, depending more on the analytical interpretation of constitutional provisions, judicial precedents, statutory frameworks, and international regulations on privacy.

#### 3.1 Research Design

It examines India's legal framework on the protection of privacy in the AI technology context, adopting a comparative legal analysis approach. This implies a detailed evaluation of Indian law, including the Digital Personal Data Protection Act, 2023, and draft Digital Personal Data Protection Rules, 2025, to analyze whether they provide adequate solutions for AI-driven privacy concerns. Given the rapid advancements of AI and its increased role in data processing, surveillance, and decision-making, this study conducts an evaluation of whether India's current legal provisions adequately safeguard individual privacy rights against the potential risks of AI.

To give a proper perspective, it draws comparisons to international legal frameworks, especially in the General Data Protection Regulation in the European Union. The General Data Protection Regulation is considered among the most strict data protection legislations in the world, so it sets higher standards for protecting data, keeping AI accountable and transparent. Using the GDPR for comparison, it identifies gaps in India's regulation of data, strengths, and areas that call for reform under India's privacy laws.

This comparative analysis is important for understanding how jurisdictions around the world approach AI-related privacy challenges and provides valuable insights into best practices that India can adopt. Through

---

<sup>15</sup> H. et al., Transparency You Can Trust: Transparency Requirements for Artificial Intelligence Between Legal Norms and Contextual Concerns, 6 BIG DATA & SOC'Y 2053951719860542 (2019).

[www.ijesrr.org](http://www.ijesrr.org)

Email- [editor@ijesrr.org](mailto:editor@ijesrr.org)

the differences highlighted in AI governance models, this study emphasizes that India needs to develop stronger legal mechanisms to regulate AI technologies and ensure that protection of privacy falls in line with global standards.

### 3.2 Sources of Data

The research has constituted secondary sources-constitutional provisions, case law analysis, legislative frameworks, international legal instruments, and academic literature as the foundation for this paper. A very relevant focus of discussion is made to Article 21 of the Indian Constitution that recognizes the right of privacy as the fundamental right in the Constitution of India. Through landmark judicial pronouncements, specifically *K.S. Puttaswamy v. Union of India* (2017), it enshrines this right.

It further critically discusses the legislative architecture, including that of the Digital Personal Data Protection Act, 2023 and the draft Digital Personal Data Protection Rules, 2025 for its adequacy in addressing issues related to the use of Artificial Intelligence for collecting and processing private data. Adopting a comparative approach, there is an understanding of international instruments, particularly from the European Union's General Data Protection Regulation. This would also be able to provide an avenue for India in understanding the most appropriate privacy rules.

Further, the study entails a literature review of peer reviewed journal articles and legal commentaries along with report regarding artificial intelligence, data protection, and constitutional law. That is why all possible impacts from AI towards rights of privacy and what legal frameworks regulate these present-day privacy aspects arising due to AI, therefore.

### 3.3 Methods of Analysis

The research employs doctrinal legal analysis, which pertains to interpreting legal texts, judicial rulings, and statutory provisions to analyze the impact of AI on the constitutional right to privacy. It bases its arguments by examining key judicial pronouncements and legislative enactments to find whether the current frameworks of law address the concerns raised by AI-driven technologies over the right to privacy.

Apart from the doctrinal analysis, a comparative legal approach is followed to evaluate India's privacy laws vis-à-vis international legal frameworks like the GDPR. The rationale behind such a comparative analysis is that this study would help identify legal gaps and areas requiring reform in the regulation of AI-related privacy risks. Drawing its insights from global best practices, the research will thus provide recommendations for improving India's legal approach to AI governance.

[www.ijesrr.org](http://www.ijesrr.org)

Email- [editor@ijesrr.org](mailto:editor@ijesrr.org)

It incorporates thematic analysis of the study for the identification of recurring concerns around AI and privacy. Key themes include mass surveillance, where AI-powered facial recognition and predictive policing pose risks to individual freedoms; data profiling, which raises concerns over unconsented data collection and potential misuse; algorithmic bias, which can lead to discriminatory outcomes affecting marginalized groups; and regulatory challenges, highlighting the lack of AI-specific legal provisions in India's data protection laws.

It thus deals with all the other relevant ethical concerns that arise with regard to the issues of state surveillance, algorithmic discrimination, and the relationship between national security and individual freedom. The paper suggests the necessity of responsible AI governance and seeks judicial oversight so that AI technologies do not become an instrument to infringe the constitutional framework. Transparency, accountability, and proper ethical deployment of AI are all in focus with regard to strong legal safeguards in a society run by AI to protect privacy.

## 4. RESULT

The crucial privacy risks in relation to AI research findings relate to data collection and profiling practices, which, through mass surveillance, raise alarming issues about individual privacy rights. As the technologies advance in AI, they allow the processing of massive datasets without apparently requiring or seeking explicit consent from a user, which poses a significant issue concerning privacy rights. Systems like facial recognition, predictive analytics, and algorithmic decision-making introduced by AI will result in invasive surveillance, further data exploitation, and violations of constitutional rights.

The comparative analysis of Indian and international legal frameworks shows that though India has been working to enhance data protection, its present legal framework still contains gaps over AI-specific privacy-related issues. The Digital Personal Data Protection Act, 2023, and the proposed Digital Personal Data Protection Rules, 2025, show a step in the right direction toward regulation of personal data. However, no clear provisions can be found with regard to the governance of AI, automated decision-making, or AI-based surveillance technologies. Instead, international law frameworks, specifically the General Data Protection Regulation by the European Union, have strict regulations over the processing of AI-driven data that focus on the principles of transparency, accountability, and rights for individuals.



These findings are categorized under distinct areas of concern, which include mass surveillance, data profiling, algorithmic discrimination, and regulatory challenges. The study concludes that although AI offers numerous societal benefits, unregulated deployment might pose serious risks to privacy. Therefore, Indian law and regulatory framework do demand urgent strengthening by adopting AI-related legal provisions, greater judicial oversight for governance, and alignment of policies with the finest global best practices in order to protect fundamental privacy rights.

**4.1 Privacy Risks Posed by AI Technologies**

The integration of AI across multiple domains raises significant privacy concerns, especially in areas like surveillance, data mining, automated decision-making, and predictive analytics. Facial recognition and mass surveillance systems through AI-powered applications undermine individual rights to privacy, while large-scale data mining usually takes place without explicit user consent. AI-driven decision-making also often results in biased outcomes and discrimination, while predictive analytics compromise personal autonomy and data security. This reflects the need for strong legal frameworks to address privacy risks associated with AI technologies.

**Table 1:** Privacy Risks of AI Technologies and Their Legal Implications

AI Domain	Privacy Concern	Legal Implication
Surveillance	Mass surveillance via AI-powered cameras and facial recognition	Potential violation of privacy rights under Article 21
Data Mining	Large-scale personal data collection without explicit consent	Breach of consent-based privacy protections
Algorithmic Decision-Making	AI-based profiling leading to biased outcomes	Risk of discrimination and lack of accountability
Predictive Analytics	Use of personal data for behavioral predictions	Threat to individual autonomy and data security

The findings indicate that AI-based technologies pose serious threats to privacy mainly because of a lack of transparency and inadequate user consent mechanisms. Mass surveillance, data mining, biased decision-making, and predictive analytics are common practices that pose significant privacy risks, as they often

operate outside the scope of legal oversight or accountability. Such urgent legal and ethical interventions are surely needed in order for AI applications to be brought within the limits of fundamental privacy rights, transparency standards, and user protection measures.

#### 4.2 Comparative Analysis of Legal Frameworks

A comparative analysis of Indian and international privacy laws suggests both strengths and weaknesses in their ability to handle AI-related privacy concerns. In this regard, the Indian legal framework, under which the Digital Personal Data Protection Act, 2023 was passed, fails to explicitly mandate governance of AI. International regulation, such as the General Data Protection Regulation by the European Union, is better positioned with its enhanced transparency, accountability, and AI-specific requirements. It does raise the urgent requirement for a strengthened legal architecture that can prevent potential privacy harms emanating from AI technologies for India.

**Table 2:** Comparative Analysis of Legal Frameworks Governing AI and Privacy

Legal Framework	Key Provisions	Effectiveness in Addressing AI Privacy Risks
Indian Constitution (Article 21)	Recognizes the right to privacy as part of the right to life and personal liberty	Lacks specific AI-related provisions
K.S. Puttaswamy v. Union of India (2017)	Established privacy as a fundamental right	No direct focus on AI regulations
Digital Personal Data Protection Act, 2023	Regulates data processing and mandates consent	Limited provisions on AI governance
Draft Digital Personal Data Protection Rules, 2025	Strengthens compliance mechanisms for data protection	Still in draft stage, lax enforcement clarity
General Data Protection Regulation (GDPR) – EU	Strict data privacy, AI accountability, and transparency mandates	More comprehensive compared to Indian laws

This analysis shows that though India has achieved a lot in data protection, its AI governance framework is relatively weak compared to international standards like the GDPR. The lack of AI-specific regulations, coupled with weak enforcement mechanisms, limits the effectiveness of existing privacy protections.

Unlike the GDPR which makes AI transparency, accountability, and data protection safeguards mandatory, India's current laws have a very inadequate provision of regulation over data processed and surveilled through AI-driven systems and decision-making processes.

### 4.3 Gaps in India's AI Privacy Protection

The Digital Personal Data Protection Act, 2023, is an important step in India's data privacy landscape, but it does not specifically talk about AI-driven data processing and automated decision-making. This has a regulatory gap that raises issues of accountability, transparency, and oversight in AI-driven technologies such as predictive analytics, algorithmic profiling, and large-scale data collection. Unlike the European Union, India does not have a specific framework for AI governance, while its data protection law is in an embryonic state. AI applications are thus, largely unregulated from a legal perspective.

One of the biggest concerns has been the integration of AI into surveillance technologies, such as facial recognition systems and predictive policing mechanisms, which often work with very little legal oversight. These technologies facilitate mass surveillance without explicit consent, raising severe violations of privacy and ethical concerns. The lack of clear legal safeguards increases the risk of misuse, bias, and discrimination. Thus, the urgent need is for comprehensive regulations of AI to balance technological advancement with fundamental privacy rights.

### 4.4 Proposed Regulatory and Ethical Recommendations

To mitigate privacy risks from AI, this research study proposes critical regulatory and ethical reforms to enhance AI privacy governance in India. These reforms comprise the introduction of AI-specific legal provisions to enhance oversight over the collection of data and automated decision-making, increased judicial and regulatory supervision to avert the abuse of AI-based surveillance, and transparency and accountability measures to be built for trust among the citizens. This will bridge the legal gaps and ensure that India has a robust framework that upholds individual privacy rights while fostering ethical AI innovation. Moreover, aligning Indian AI regulations with international best practices- like the GDPR-will help in filling this gap.

**Table 3:** Proposed Legal and Ethical Reforms for AI Privacy Governance in India

Recommendation	Expected Impact
----------------	-----------------

[www.ijesrr.org](http://www.ijesrr.org)

[Email- editor@ijesrr.org](mailto:editor@ijesrr.org)

Introduction of AI-specific legal provisions	Ensures better oversight of AI-based data collection and processing
Stronger judicial and regulatory oversight	Prevents misuse of AI in mass surveillance
Adoption of AI transparency and accountability measures	Enhances public trust and compliance with ethical standards
Alignment of Indian regulations with international best practices	Bridges the gap between domestic and global AI governance frameworks

Findings have shown that India, despite progress in data protection law, still lacks AI-specific legal safeguards that leave massive parts of privacy unaddressed. As a result, ensuring such provisions should benefit from implementing stronger regulations that specifically relate to AI-driven data processing, surveillance, and decision-making in curbing possible infringements. Ensuring such development, including ethical AI, is important for keeping pace with technological advancements while also protecting fundamental rights and is further assured by judicial oversight as well as transparent legal mechanisms. A holistic legal framework will ensure the protection of individual privacy while pushing towards the responsible use of AI technologies.

## 5. DISCUSSION

The impact of AI on the right to privacy poses a sophisticated legal and ethical challenge, which is especially pressing from the angle of constitutional law. AI technologies such as facial recognition, predictive analytics, and automated decision-making systems significantly impact the processing of personal data. Concerns relate to user consent, data security, and surveillance. The article will outline primary privacy risks brought about by AI and assess how the existing frameworks are able to provide protection of individual rights of privacy.

### 5.1 AI and Privacy Risks: Constitutional and Legal Implications

Substantially, these technologies are secretly in a position to pose risks to privacy. This includes the spectrum of mass surveillance, data mining, and algorithmic decision-making. With facial recognition technologies being increasingly deployed and predictive policing sanctioned, mass surveillance and misuse by state apparatuses raise rightful concerns. Left unchecked, the constitutional right to privacy- Article 21 of the Indian Constitution-may be infringed by such technologies, as exemplified in *K.S. Puttaswamy v.*

Union of India (2017) judgment firmly established privacy as a fundamental right, the rapid evolution of AI necessitates additional legal safeguards to prevent unauthorized data collection and surveillance abuses.

This means that AI-driven data profiling is further complicating privacy protection. Organizations can now collect and analyze vast amounts of personal information in ways that have not been fully understood by the users themselves, leading to discrimination in decision-making and ethical questions about bias and transparency in such automated processes. The lack of comprehensive legal provisions on AI thus exacerbates such risks, requiring stronger regulatory oversight.

## 5.2 Comparative Legal Analysis: India vs. International Standards

The comparative legal analysis brings out certain deficiencies of the Indian legal framework on privacy vis-à-vis AI governance. The Digital Personal Data Protection Act, 2023, while it is a massive step toward the enhancement of data protection, does not address AI-driven data processing and automated decision-making. The General Data Protection Regulation, European Union, while offering a much-needed larger legal framework for AI to be placed within this structure, regulates AI with a robust scale of transparency, accountability, and standards of data processing.

The GDPR requires organizations to be transparent, carry out AI impact assessments, and respect data subject rights. In contrast, India's legal framework does not have such provisions, which creates ambiguities in AI governance. Since there are no AI-specific regulations, the enforcement mechanisms are weak, and privacy protections are less effective in the country. By adopting global best practices, such as those embedded in the GDPR, India can bridge these gaps and establish a robust AI regulatory framework.

## 5.3 Addressing Regulatory and Ethical Challenges

One of the primary regulatory challenges in India is the lack of a dedicated AI governance framework. In contrast, the European Union has made efforts to incorporate AI oversight into its data protection laws. India continues to rely on general data protection provisions without specific AI accountability measures. This regulatory gap allows AI-driven surveillance and predictive analytics to operate without adequate legal oversight, thereby increasing the risk of privacy violations.

Its impact on ethical and privacy protection levels is also at par. For instance, while algorithmic bias and discrimination can still be present, AI processes tend to repeat societal prejudices during decision-making procedures. The opaqueness in AI algorithms introduces accountability issues with respect to unchallenged unfair or discriminatory outcomes. Only a complete reformation of existing laws that consider the

implementation of AI within all the boundaries but also in regards to the intrinsic privacy rights, will help settle these challenges.

## 5.4 Strengthening AI Governance: Recommendations

To address AI-related privacy risks, this study suggests key regulatory and ethical reforms that can be taken to improve AI governance in India:

1. Introduction of AI-Specific Legal Provisions: Explicit legal provisions should be incorporated within India's data protection laws to address AI-driven privacy risks, ensuring accountability in AI-based data processing and automated decision-making.
2. Intensifying Judicial and Regulatory Monitoring: Well-entrenched legal oversight is needed because AI should not be misused for mass surveillance and data gathering. The regulatory bodies need to clearly stipulate guidelines for monitoring AI applications.
3. Developing Transparency and Accountability Mechanisms: Adequate mechanisms need to be instituted in AI such that the decisioning process becomes transparent. Organizations have to publish AI impact assessments along with opportunities for individuals to contest any wrongful AI decision.
4. Alignment with Global Best Practices: India can align its AI regulatory framework with international standards such as the GDPR to enhance data protection mechanisms while fostering ethical AI innovation.

The findings reveal that while India has made progress in data protection, its legal framework remains insufficient to address the privacy challenges posed by AI. The absence of AI-specific legal safeguards leaves significant privacy vulnerabilities unaddressed, necessitating urgent reforms to ensure transparency, accountability, and ethical AI deployment. Strengthening India's AI governance model, incorporating judicial oversight, and aligning regulations with international best practices will be crucial in safeguarding fundamental privacy rights while promoting responsible AI innovation.

## 6. CONCLUSION

The rapid pace of artificial intelligence presents important challenges to the right to privacy and calls for urgent legal and regulatory interventions. This study has demonstrated that, although India has progressed in taking its steps toward securing data protection with frameworks such as the Digital Personal Data Protection Act, 2023, these measures are inadequate as regards AI-specific risks for privacy. AI technologies such as mass surveillance, data mining, predictive analytics, and decision-making algorithms that are not transparent, accountable, or consent-based provide immense threats to individual privacy. The

[www.ijesrr.org](http://www.ijesrr.org)

Email- [editor@ijesrr.org](mailto:editor@ijesrr.org)

general observation of the European Union's General Data Protection Regulation (GDPR) here makes the comparison to underscore the shortcomings in India's AI governance system and greater requirements for AI-specific regulations and enforcement mechanisms.

The development of AI should be approached with a balance. India should therefore strengthen its legal, regulatory, and ethical frameworks to reduce privacy risks. These reforms will involve the incorporation of AI-specific legal provisions, strict judicial and regulatory oversight, and greater transparency in AI-based decision-making. This will be made possible by bringing domestic regulations into line with international best practices, such as the GDPR. As technology advanced further with AI, fundamental rights in relation to privacy calls for preservation; violations of individual privacy cannot take place without curbs on technological progress. A sufficiently robust constitutional framework will be necessary to protect citizens from any kind of potential violation through the scope of AI, yet it will have to facilitate responsible and ethically advancing innovation in AI.

## REFERENCES

1. B. C. Stahl & D. Wright, Ethics and Privacy in AI and Big Data: Implementing Responsible Research and Innovation, 16 IEEE SEC. & PRIVACY 26 (2018).
2. B. Murdoch, Privacy and Artificial Intelligence: Challenges for Protecting Health Information in a New Era, 22 BMC MED. ETHICS 1 (2021).
3. C. Cath et al., Artificial Intelligence and the 'Good Society': The US, EU, and UK Approach, 24 SCI. & ENG'G ETHICS 505 (2018).
4. E. F. Villaronga, P. Kieseberg & T. Li, Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten, 34 COMPUT. L. & SEC. REV. 304 (2018).
5. F. A. Raso et al., Artificial Intelligence & Human Rights: Opportunities & Risks, BERKMAN KLEIN CTR. RES. PUB. 2018-6 (2018).
6. G. Contissa et al., Claudette Meets GDPR: Automating the Evaluation of Privacy Policies Using Artificial Intelligence, SSRN 3208596 (2018), <https://ssrn.com/abstract=3208596>.
7. H. Felzmann et al., Transparency You Can Trust: Transparency Requirements for Artificial Intelligence Between Legal Norms and Contextual Concerns, 6 BIG DATA & SOC'Y 2053951719860542 (2019).
8. H. Roberts et al., The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation, in SPRINGER INTERNATIONAL PUBLISHING 47-79 (2021).
9. J. Adams-Prassl, What If Your Boss Was an Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work, 41 COMP. LAB. L. & POL'Y J. 123 (2019).

[www.ijesrr.org](http://www.ijesrr.org)

Email- [editor@ijesrr.org](mailto:editor@ijesrr.org)

10. J. Amann et al., Explainability for Artificial Intelligence in Healthcare: A Multidisciplinary Perspective, 20 BMC MED. INFORMATICS & DECISION MAKING 1 (2020).
11. K. H. Keskinbora, Medical Ethics Considerations on Artificial Intelligence, 64 J. CLIN. NEUROSCIENCE 277 (2019).
12. M. Latonero, Governing Artificial Intelligence: Upholding Human Rights & Dignity, 38 DATA & SOC'Y (2018).
13. M. Perc, M. Ozer & J. Hojnik, Social and Juristic Challenges of Artificial Intelligence, 5 PALGRAVE COMM'NS 1 (2019).
14. N. M. Safdar, J. D. Banja & C. C. Meltzer, Ethical Considerations in Artificial Intelligence, 122 EUR. J. RADIOL. 108768 (2020).
15. S. Greenstein, Preserving the Rule of Law in the Era of Artificial Intelligence (AI), 30 ARTIFICIAL INTELLIGENCE & L. 291 (2022).