
ARTIFICIAL INTELLIGENCE AND INFORMATIONAL PRIVACY: TOWARDS A CONSTITUTIONAL FRAMEWORK FOR ALGORITHMIC GOVERNANCE IN INDIA

Dr. Malay Kumar Behera, Recognized as 'Star' & 'Domain Scholar' in "Patents and IPR"
by NPTEL IIT Madras

Gunnam Bhaskar Rao, Research Scholar, PG Dept. of law, Sambalpur University

ABSTRACT

Artificial intelligence (AI) is rapidly transforming the relationship between individuals, markets, and the State. In India, algorithmic systems increasingly influence welfare delivery, policing, financial services, employment, healthcare, education, digital identity, content moderation, and public administration. These developments generate substantial constitutional concerns because contemporary AI systems do not merely process information supplied by individuals; they aggregate, infer, predict, classify, and generate information about them. The resulting privacy risks therefore extend beyond conventional notions of data collection and disclosure to encompass profiling, behavioural prediction, surveillance, inferential privacy, and automated decision-making. This article examines whether India's constitutional framework is capable of regulating these emerging forms of informational power.

The article adopts a doctrinal and comparative methodology, analysing Article 21 and related fundamental rights, the Supreme Court's privacy jurisprudence, particularly *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), *K.S. Puttaswamy (Aadhaar-5J.) v. Union of India* (2019), *Maneka Gandhi v. Union of India* (1978), and *Anuradha Bhasin v. Union of India* (2020), alongside the Digital Personal Data Protection Act, 2023 and contemporary international approaches including the European Union's Artificial Intelligence Act. It argues that India's constitutional privacy doctrine should be understood as a form of algorithmic constitutionalism, capable of imposing substantive and procedural limits on both governmental and, in appropriate circumstances, private algorithmic power. The article proposes a constitutional framework based on legality, legitimate purpose, necessity, proportionality, data minimisation, algorithmic transparency, explainability, human oversight, non-discrimination, independent auditing, procedural fairness, and effective remedies. It concludes that India's emerging AI governance regime should not rely exclusively upon sectoral regulation or consent-based data protection but should place constitutional

rights at the centre of algorithmic governance.

Keywords: Artificial Intelligence, Informational Privacy, Article 21, Constitution of India, Algorithmic Governance, Digital Personal Data Protection Act, Proportionality, Surveillance, Automated Decision-Making, AI Regulation.

1. Introduction

Artificial intelligence has moved from the domain of experimental computing into the infrastructure of contemporary social, economic, and governmental life. Machine-learning systems are capable of analysing enormous datasets, identifying patterns, making predictions, generating content, ranking individuals, and supporting or automating decisions previously made by human actors. In India, the expansion of digital public infrastructure, biometric identification, financial technology, platform-mediated services, and data-driven governance creates particularly significant opportunities for AI deployment.

Yet the benefits of AI coexist with a profound transformation of informational power. Traditional privacy law largely conceptualised the problem as one of collecting, storing, using, or disclosing personal information. Artificial intelligence complicates that model. An algorithm may derive sensitive information from apparently innocuous data, infer personality characteristics, predict behaviour, determine creditworthiness, identify relationships, or classify individuals without the individual ever directly providing the inferred information.

The constitutional significance of this transformation is considerable. Privacy is no longer concerned only with secrecy. It concerns the conditions under which an individual can maintain autonomy, dignity, identity, decisional freedom, and control over personal information. The Supreme Court of India expressly recognised these dimensions in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), holding privacy to be a constitutionally protected fundamental right.

The emergence of AI therefore raises a fundamental question: **Can India's existing constitutional and statutory framework adequately constrain algorithmic power, or does AI require a new constitutional approach to informational privacy?**

This article argues that the Constitution already contains the normative resources necessary for such a framework. However, these resources must be operationalised through legislation,

administrative safeguards, judicial review, independent oversight, and technical accountability mechanisms.

The central thesis is that **Article 21, read with Articles 14 and 19, should be interpreted to impose constitutional constraints on high-impact algorithmic decision-making, particularly where AI systems affect bodily integrity, personal autonomy, equality, livelihood, reputation, liberty, or access to public services.**

2. Research Questions and Methodology

This article addresses four principal questions:

1. What constitutional protections does Indian law currently provide against AI-enabled invasions of informational privacy?
2. Is the Digital Personal Data Protection Act, 2023 sufficient to address the distinctive risks posed by AI?
3. How should constitutional principles of legality, proportionality, equality, and procedural fairness apply to algorithmic decision-making?
4. What institutional framework should India adopt for constitutionally compliant AI governance?

The article employs a **doctrinal legal methodology**, examining constitutional provisions, judicial decisions, legislation, governmental policy documents, and relevant academic scholarship. A comparative dimension is incorporated through consideration of international approaches, particularly the European Union's risk-based regulatory framework.

The objective is not to advocate wholesale transplantation of foreign AI regulation into India. Rather, comparative law is used to identify regulatory principles that can be adapted to India's constitutional and institutional context.

3. Artificial Intelligence and the Transformation of Informational Privacy

3.1 From data collection to data inference

The privacy problem associated with AI is fundamentally different from the traditional data-

protection problem.

A conventional database may contain a person's name, address, telephone number, financial information, or biometric identifier. AI systems, however, can combine multiple datasets and generate additional information through inference.

For example, seemingly unrelated data concerning a person's purchasing behaviour, geographic movements, online activity, social connections, and device usage may enable an algorithm to infer health conditions, political preferences, economic status, religious affiliation, or behavioural tendencies.

Consequently, privacy protection cannot be restricted to information that an individual consciously disclosed.

The important constitutional question becomes not merely:

Who possesses my data?

but also:

What may institutions legitimately infer about me, and what decisions may they make on the basis of those inferences?

This is particularly significant because algorithmic inferences can be inaccurate, discriminatory, or impossible for individuals to contest.

Recent scholarship similarly identifies AI as an "inference infrastructure" in which privacy risks arise from profiling, prediction, surveillance, and generative systems rather than simply from conventional data storage (Rathi & Tyagi, 2026).

3.2 Informational privacy and autonomy

In *Puttaswamy* (2017), the Supreme Court recognised informational privacy as an important dimension of the constitutional right to privacy. The Court's reasoning linked privacy with dignity, autonomy, liberty, and individual choice.

This constitutional conception has particular relevance to AI.

An individual subjected to continuous algorithmic classification may experience a reduction in meaningful autonomy even when no physical intrusion occurs. If a system predicts that an individual is financially risky, medically vulnerable, politically radical, or otherwise undesirable, the resulting classification can affect opportunities and social participation.

AI thus transforms privacy from a passive right against unwanted disclosure into an active constitutional interest in **control over informational identity and algorithmic treatment**.

4. The Constitutional Foundations of AI Governance in India

4.1 Article 21 and privacy

Article 21 provides that no person shall be deprived of life or personal liberty except according to procedure established by law. Indian constitutional jurisprudence has progressively transformed Article 21 from a narrow procedural guarantee into a substantive protection of dignity and liberty.

In *Maneka Gandhi v. Union of India* (1978), the Supreme Court established that legal procedures affecting personal liberty must satisfy standards of fairness and non-arbitrariness. This principle is highly relevant to automated governmental decision-making.

The constitutional recognition of privacy was conclusively established by the nine-judge bench in *Puttaswamy*.

The judgment conceptualised privacy as encompassing several dimensions, including bodily, spatial, decisional, and informational privacy.

For AI governance, informational privacy is particularly important because algorithmic systems operate fundamentally through information.

4.2 Articles 14 and 15: Algorithmic equality

Privacy cannot be separated from equality.

Article 14 prohibits arbitrary State action and guarantees equality before the law and equal protection of the laws. AI systems may reproduce historical discrimination embedded in training data, produce disparate outcomes, or use proxy variables that indirectly reproduce

prohibited characteristics.

For example, an algorithm that excludes applicants based upon geographic location may indirectly disadvantage communities associated with caste, class, religion, or ethnicity.

The constitutional issue therefore extends beyond privacy to **algorithmic discrimination**.

An AI system used by the State should consequently be subject to heightened scrutiny where it creates differential effects upon constitutionally protected groups.

Articles 15 and 16 provide additional protection against discrimination in specified contexts, particularly in education and public employment.

4.3 Article 19 and informational freedom

AI also affects Article 19 rights.

Algorithmic content recommendation and moderation can influence freedom of speech and expression. Automated surveillance may create a chilling effect on political expression. Predictive policing can disproportionately target communities, affecting their ability to participate freely in public life.

Accordingly, AI governance cannot treat privacy as an isolated right.

The constitutional framework should recognise an **interdependent relationship between privacy, equality, speech, liberty, and dignity**.

5. The Puttaswamy Proportionality Framework

The most important constitutional tool for evaluating AI-related State action is proportionality.

The Supreme Court in *Puttaswamy* articulated a structured approach to restrictions on privacy. Broadly, State interference should satisfy requirements concerning:

1. legality;
2. legitimate State aim;

3. rational connection between the measure and its objective;
4. necessity;
5. proportionality between means and ends; and
6. procedural safeguards against abuse.

This framework provides a constitutional methodology for evaluating AI deployments.

Consider AI-powered facial recognition used for policing. The existence of a public-security objective cannot by itself establish constitutional validity. The State should demonstrate:

- a clear legal basis;
- a legitimate objective;
- evidence that facial recognition contributes materially to that objective;
- consideration of less intrusive alternatives;
- limits on collection and retention;
- safeguards against misuse;
- mechanisms for correcting false matches; and
- independent oversight.

The proportionality principle therefore transforms AI regulation from a question of technological enthusiasm into a question of constitutional justification.

6. The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act) represents a major development in India's data-protection architecture.

It establishes a statutory framework governing the processing of digital personal data and creates obligations for data fiduciaries and rights for data principals.

The Act is significant because AI systems frequently depend upon large-scale personal-data processing.

However, its relationship with AI governance requires careful examination.

First, data protection is not identical to algorithmic governance.

An algorithm may produce harmful consequences even when the underlying data processing is technically lawful.

For example, a person may provide data lawfully, but an algorithm may subsequently use that information to generate a discriminatory risk score.

Second, consent is an inadequate solution to structural algorithmic power.

AI ecosystems frequently involve complex processing chains that individuals cannot realistically understand. The informational asymmetry between individuals and organisations can make formal consent an insufficient safeguard.

Third, inferential privacy remains difficult.

The central problem is not merely what data are collected but what information is inferred and how such information is used.

Fourth, high-impact automated decision-making requires procedural safeguards.

A comprehensive AI framework should address explanation, contestability, human review, impact assessment, and accountability in circumstances where algorithmic decisions significantly affect individuals.

Thus, the DPDP Act should be regarded as **one component of India's AI-governance architecture rather than its complete constitutional solution.**

7. AI, Surveillance and the Indian State

AI has the potential to dramatically expand State surveillance capabilities.

Traditional surveillance requires human investigators and therefore encounters practical

limitations of scale. AI can automate identification, correlation, pattern recognition, and behavioural prediction.

Facial-recognition systems, predictive policing, automated traffic monitoring, biometric systems, and large-scale data analytics can create persistent infrastructures of observation.

The constitutional danger lies in the possibility of moving from targeted surveillance to **continuous population-level monitoring**.

The Supreme Court's decision in *K.S. Puttaswamy (Aadhaar-5J.) v. Union of India* (2019) demonstrates the constitutional sensitivity surrounding large-scale identity infrastructures. The Court's analysis illustrates that technological efficiency cannot automatically justify extensive data collection.

AI intensifies this concern because biometric information can be combined with other datasets to produce detailed behavioural profiles.

A constitutionally legitimate surveillance framework should therefore require:

- specific statutory authority;
- defined purposes;
- necessity;
- narrowly tailored deployment;
- limited retention;
- independent authorisation where appropriate;
- auditability;
- judicial or independent review;
- transparency reports; and
- effective remedies.

8. Algorithmic Decision-Making and Administrative Law

The administrative State increasingly relies upon computational systems.

AI can determine or influence eligibility for welfare programmes, allocation of resources, fraud detection, tax administration, immigration processing, recruitment, policing, and public-sector decision-making.

This raises an important administrative-law principle:

A public authority should not escape constitutional responsibility merely because a decision has been delegated to an algorithm.

If an administrative decision violates Article 14 or Article 21, the use of technology cannot immunise that decision from judicial review.

Algorithmic systems should therefore be understood as instruments of administrative power rather than autonomous substitutes for constitutional accountability.

8.1 Reasoned decision-making

Administrative law traditionally values reasoned decisions.

Where an algorithm materially affects an individual's rights or interests, the individual should ordinarily be able to understand:

- what decision was made;
- what factors materially influenced it;
- what data were relied upon;
- whether automated processing was involved; and
- how the decision can be challenged.

This does not necessarily require disclosure of proprietary source code.

There is an important distinction between **source-code transparency** and **decision transparency**.

Constitutional accountability generally requires sufficient information to understand and

contest a decision, while legitimate trade secrets and cybersecurity concerns may justify withholding technical details.

9. The Problem of Algorithmic Bias

AI systems are not inherently neutral.

Bias may enter an algorithm through:

1. biased training datasets;
2. incomplete datasets;
3. historically discriminatory institutional practices;
4. inappropriate proxy variables;
5. model design choices;
6. optimisation objectives; or
7. deployment environments.

In India, algorithmic bias has special constitutional implications because social inequalities frequently intersect with caste, gender, religion, language, region, disability, and economic status.

An AI system trained on historically unequal outcomes may reproduce those inequalities while appearing mathematically objective.

The constitutional principle of equality therefore requires more than prohibiting explicitly discriminatory variables.

Regulation should address **disparate impact and proxy discrimination**.

High-impact AI systems should be subjected to algorithmic impact assessments capable of identifying potential discriminatory effects before deployment and throughout the system lifecycle.

10. Generative AI and Informational Privacy

Generative AI creates an additional category of privacy risk.

Large language models and multimodal systems may be trained or fine-tuned using enormous collections of text, images, audio, and other information. They can also generate synthetic representations of real individuals.

Three issues deserve particular attention.

10.1 Training data

The use of personal information for model training raises questions concerning lawful processing, purpose limitation, legitimate interests, consent, and individual rights.

10.2 Memorisation and extraction

Models may sometimes reproduce information contained within training or contextual data. This creates potential risks to confidential and personal information.

10.3 Synthetic identity

Deepfakes and AI-generated representations can undermine privacy, reputation, dignity, and autonomy.

The constitutional analysis should therefore extend beyond conventional personal-data processing to include **synthetic representations and inferential information**.

11. Comparative Lessons from the European Union

The European Union's AI Act adopts a risk-based model distinguishing different categories of AI systems and imposing stronger obligations upon higher-risk applications.

Its significance for India lies less in direct transplantation than in demonstrating that AI governance can move beyond traditional data-protection law.

The EU approach emphasises:

- risk classification;
- prohibited practices;
- high-risk system obligations;
- transparency;
- human oversight;
- documentation;
- conformity assessment; and
- institutional enforcement.

The EU General Data Protection Regulation also contains important principles concerning data minimisation, purpose limitation, transparency, and automated decision-making.

India can draw from these approaches while adapting them to its own constitutional structure and developmental requirements.

India should avoid a regulatory model that makes compliance so costly that beneficial innovation becomes inaccessible, particularly for smaller firms and public-interest technologies.

A proportionate, risk-based model is therefore preferable.

12. Towards a Constitutional Framework for Algorithmic Governance

This article proposes an eight-part constitutional framework.

12.1 Legality

Government deployment of high-impact AI should have a clear statutory basis.

Executive convenience or broad administrative powers should not substitute for legislation where AI materially interferes with fundamental rights.

12.2 Legitimate purpose

AI systems should be deployed only for constitutionally legitimate purposes.

The State should articulate the precise objective rather than rely upon broad claims such as "efficiency" or "public interest."

12.3 Necessity

The State should demonstrate that AI deployment is necessary to achieve the identified objective.

Less intrusive alternatives should be considered.

12.4 Proportionality

The expected public benefit must be balanced against the severity and probability of rights infringement.

A technically sophisticated system is not constitutionally justified merely because it is effective.

12.5 Data minimisation

AI systems should process only information reasonably necessary for their stated purpose.

Mass collection simply because future analytical uses are possible should be presumptively disfavoured in high-risk governmental applications.

12.6 Algorithmic transparency

Individuals affected by consequential AI decisions should receive meaningful information concerning the existence and operation of automated decision-making.

Transparency should be calibrated according to risk rather than requiring universal disclosure of source code.

12.7 Human oversight and contestability

Where AI materially affects fundamental rights, meaningful human review should remain available.

Human oversight must, however, be substantive rather than merely ceremonial. A human decision-maker who automatically accepts an algorithmic recommendation without independent assessment provides little constitutional protection.

12.8 Independent accountability

High-risk AI systems should be subject to independent auditing and impact assessment.

A future Indian AI regulatory architecture could combine:

- sector-specific regulators;
- a central coordinating authority;
- independent technical auditors;
- data-protection institutions;
- parliamentary oversight; and
- judicial review.

13. Algorithmic Impact Assessments

India should consider mandatory **Algorithmic Impact Assessments (AIAs)** for high-risk governmental and private-sector systems.

An AIA could assess:

Dimension	Core Question
Privacy	What personal/inferred information is processed?
Equality	Could the system produce discriminatory outcomes?

Dimension	Core Question
Necessity	Is AI genuinely required?
Accuracy	What are the system's error rates?
Explainability	Can affected persons understand decisions?
Security	Can data or models be compromised?
Human rights	What fundamental rights may be affected?
Remedies	Can affected persons challenge outcomes?

Such assessments should occur before deployment and periodically thereafter.

The lifecycle approach is important because AI systems may change when datasets, models, objectives, or deployment environments change.

14. The Right to Explanation and the Right to Contest

One of the most significant constitutional implications of algorithmic governance is the emergence of a possible **right to contest automated decisions**.

The right should not necessarily require a universal constitutional entitlement to a complete technical explanation.

Instead, individuals should receive a meaningful explanation proportionate to the impact of the decision.

For high-impact decisions, this may include:

- the principal reasons for the outcome;
- relevant categories of data;
- significant factors considered;
- the role of automated processing;
- avenues for human review; and

- mechanisms for correction.

Such safeguards are closely connected to natural justice.

An individual cannot meaningfully challenge an adverse decision if the State merely states that "the algorithm determined the outcome."

15. Privacy by Design and Constitutional Technology

Constitutional compliance should not depend exclusively on ex post judicial remedies.

Privacy and rights protection should be incorporated into system design.

This could include:

- privacy-preserving architectures;
- data minimisation;
- differential privacy where appropriate;
- encryption;
- access controls;
- federated learning;
- secure deletion;
- audit logs;
- bias testing; and
- model monitoring.

The concept may be described as "**constitutional technology by design.**"

The underlying idea is straightforward: fundamental rights should be embedded in technological architecture rather than added after harm occurs.

16. Challenges to the Proposed Framework

A constitutional framework must also acknowledge competing interests.

16.1 Innovation

Excessive regulation could inhibit technological innovation. India's regulatory model should therefore distinguish between experimental, low-risk applications and systems capable of significantly affecting fundamental rights.

16.2 State capacity

Regulation requires technical expertise. Indian regulators and courts may require specialised AI expertise, independent laboratories, and interdisciplinary institutions.

16.3 Trade secrets

Transparency requirements must balance accountability against legitimate intellectual-property interests.

16.4 National security

AI may be used for defence and intelligence. Nevertheless, national security should not automatically eliminate constitutional scrutiny. Rather, appropriate confidential oversight mechanisms should be developed.

16.5 Federalism

AI regulation intersects with areas governed by both the Union and the States. A coherent framework should therefore accommodate India's federal structure.

17. Judicial Review as the Constitutional Backstop

Courts will remain essential to India's AI-governance architecture.

The judiciary can apply established constitutional doctrines to novel technological circumstances.

Three doctrines are particularly significant.

First: arbitrariness

Algorithmic decision-making that lacks rational standards or produces manifestly arbitrary outcomes may violate Article 14.

Second: proportionality

Intrusive AI applications affecting privacy or liberty must satisfy the proportionality standard.

Third: procedural fairness

Individuals should have meaningful opportunities to challenge consequential decisions.

The advantage of constitutional adjudication is technological neutrality. Courts need not determine whether a particular machine-learning architecture is scientifically optimal. They can instead ask whether the State has exercised power consistently with constitutional standards.

18. Toward an Indian Model of Algorithmic Constitutionalism

India should avoid choosing between two simplistic alternatives:

innovation without regulation and regulation without innovation.

A constitutional approach offers a third possibility: **rights-compatible innovation.**

Such an approach would recognise AI as a form of institutional power and would subject that power to constitutional principles.

The Indian model should therefore rest on five interconnected pillars:

Constitutional rights → risk classification → procedural safeguards → institutional accountability → effective remedies.

This approach would permit beneficial AI applications while placing stronger restrictions on systems that threaten fundamental rights.

Importantly, the framework should be technologically neutral. Constitutional rules should not become obsolete whenever a new model architecture emerges.

19. Conclusion

Artificial intelligence presents India with an unprecedented governance challenge. The problem is not simply that machines process more personal data than before. The deeper transformation lies in the capacity of algorithmic systems to **infer, predict, classify, rank, surveil, and influence individuals at extraordinary scale.**

India's constitutional jurisprudence already provides a powerful foundation for confronting this challenge. *Puttaswamy* constitutionalised privacy and recognised informational privacy as integral to dignity and autonomy. *Maneka Gandhi* strengthened the requirements of fairness and non-arbitrariness. Article 14 provides a constitutional basis for confronting algorithmic discrimination, while Article 19 protects against technological practices that may chill expression and participation.

The DPDP Act, 2023 is an important component of this emerging architecture, but it cannot by itself constitute a complete AI-governance regime. Data protection addresses an essential part of the problem, while algorithmic governance must additionally address inference, automated decision-making, discrimination, explainability, human oversight, surveillance, and institutional accountability.

India should consequently develop a constitutional framework for algorithmic governance based upon legality, legitimate purpose, necessity, proportionality, data minimisation, transparency, human oversight, equality, independent auditing, and effective remedies.

The most important conceptual shift is to recognise that **algorithmic power is constitutional power when exercised by the State, and potentially rights-affecting private power when deployed in essential or high-impact domains.**

The future of Indian privacy law should therefore move beyond the question of who controls personal data. It should address the broader question of **who controls the systems that transform personal information into decisions about human beings.**

That is the central constitutional challenge of artificial intelligence in India.

REFERENCES:

Bhandari, V., & Bailey, R. (2025). Evolution of privacy jurisprudence in the Supreme Court of India: Evaluating the impact of *Puttaswamy*. *National Law School of India Review*, 36(2). <https://repository.nls.ac.in/nlsir/vol36/iss2/7/>

European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). *Official Journal of the European Union*, L119, 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

Góra-Błaszczkowska, A., et al. (2026). Artificial intelligence in judicial systems: Constitutional frameworks and democratic safeguards in Poland and India: A comparative governance analysis. *European Proceedings of Politics and International Relations*. <https://ojs.academicon.pl/eppism/article/view/11084>

Jain, A., & Anand, A. (2025). Tracing the constitutional journey of data privacy in India: From *Puttaswamy* to the Draft DPDP Rules, 2025. *SSRN Electronic Journal*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5283949

Majithia, J., & Bhatia, S. (2025). Artificial intelligence legislation in India: A comparative legal analysis with the European Union Artificial Intelligence Act. *Panjab University Law Review*. <https://pulr.puchd.ac.in/index.php/pulr/article/view/370>

Maneka Gandhi v. Union of India, (1978) 1 SCC 248 (India).

Ministry of Electronics and Information Technology. (2023). *Digital Personal Data Protection Act, 2023*. Government of India.

Mohapatra, D., Pattanaik, S., Mishra, A. R., et al. (2026). Data privacy and artificial intelligence in the digital society: A comparative analysis of legal frameworks for personal data protection. *Journal of Law, Information & Science*. <https://jlisjournal.com/index.php/jlis/article/view/62>

Nath, S., & Dhar, R. (2026). An analysis of the Digital Personal Data Protection Act 2023. *Christ University Law Journal*. <https://journals.christuniversity.in/index.php/culj/article/view/7550>

Raghuwanshi, T., & Maheshwari, C. (2025). Regulating artificial intelligence in the era of data protection: A comparative legal analysis of the European Union and Indian frameworks. *International Journal of Legal Science and Innovation*. <https://ijlsi.com/article/view/regulating-artificial-intelligence-in-the-era-of-data-protection-a->

comparative-legal-analysis-of-the-european-union-and-indian-frameworks

Rathi, G., & Tyagi, S. (2026). Artificial intelligence as an inference infrastructure: Recasting the right to privacy across surveillance, profiling and generative systems in India. *Lex Gazette*.<https://lexgazette.com/wp-content/uploads/2026/08/Manuscript-Artificial-Intelligence-As-An-Inference-Infrastructure-Gayatri-Rathi.pdf>

Sarankumar, R. (2025). An analysis of the role of the Indian Constitution in protecting digital rights and AI governance. *International Journal of Legal Science and Innovation*.
<https://ijlsi.com/article/view/an-analysis-of-the-role-of-the-indian-constitution-in-protecting-digital-rights-and-ai-governance>

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 SCC 1 (India).

Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India).

United Nations Educational, Scientific and Cultural Organization. (2021). *Recommendation on the ethics of artificial intelligence*. UNESCO.

United Nations General Assembly. (2024). *Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development* (A/RES/78/265). United Nations.

World Economic Forum. (2024). *Presidio AI framework: Embedding AI governance into organisational practice*. World Economic Forum.

Yadav, A. K. (2025). Issues and challenges in the protection of right to privacy in the era of artificial intelligence: An overview. *Indian Journal of Integrated Research in Law*, 5.
<https://ijirl.com/wp-content/uploads/2025/06/>