

Algorithmic Governance and Privacy Rights: A Critical Legal Study of AI Based Data Mining in the Digital Era

Dharmendra Panwar^{1*} | Dr. K R Meghwal²

¹Ph.D. Research Scholar, Department of Law, JNVU Jodhpur, Rajasthan.

²Assistant Professor of Law, Faculty of Law, JNVU Jodhpur, Rajasthan.

*Corresponding Author: dharmendra11panwar@gmail.com

Citation: Panwar, D. & Meghwal, K. (2026). Algorithmic Governance and Privacy Rights: A Critical Legal Study of AI Based Data Mining in the Digital Era. International Journal of Education, Modern Management, Applied Science & Social Science, 08(03(I)), 230–241.

ABSTRACT

The immense growth of artificial intelligence and massive data mining has changed the world in respect to governance structures. The use of algorithmic systems in the decision-making processes concerning the allocation of welfare, predictive policing, financial profiling, and digital surveillance is becoming popular with governments and private corporations. Recent reports in the industry suggest that more than 60 percent of all businesses worldwide rely on artificial intelligence-led analytics in the key decision making processes and billions of people leave a digital trail of personal data every day. This change of algorithmic governance has brought up some urgent issues about the loss of privacy, control of information, and personal consent in the digital age. The paper has provided a critical analysis of the legal implication of artificial intelligence based data mining to the right to privacy. It is an assessment of the way automated decision making systems amass, manipulate and deduce delicate personal data, frequently with no significant openness or responsibility. Through the discussions of constitutional privacy jurisprudence, data protection principles, and new frameworks of cyber-security, the study examines the adequacy of the current legal regimes in dealing with the threats of mass surveillance, profiling, discriminatory results, and function creep. Specific focus is made on a conflict between technological innovation and basic rights protection. The article is supportive of the idea that the existing regulatory practices are still incoherent and responsive. It suggests a legal framework that is rights based and incorporates transparency requirements, algorithmic responsibility, data minimisation, and enhancements of oversight tools. These reforms are necessary in order to make sure that the technological governance develops in line with the principles of democracy and the preservation of the rights to privacy.

Keywords: Algorithmic Governance, Artificial Intelligence, Data Mining, Right to Privacy, Cyber-Security Law.

Introduction

The swift Indian society digitalization has brought in the radical change in the forms in which the institutions of the population, individual businesses and citizens interact with data. The key to this change is the introduction of artificial intelligence and mechanisms of governance through which the decision-making is automated, people are profiled, public resources are distributed, and big data analysis is conducted.¹ The data mining in AI form has been described as the ability to extract patterns, correlations and insights out of vast amounts of personal data with the help of automated algorithms, it has not only become central to state but also corporate operations as well.² As much as these systems hold efficiency, prediction and resource optimisation, legal issues concerning privacy rights, accountability, fairness and the concept of democracy as a form of governance is raised in urgent form.³

* Copyright © 2026 by Author's and Licensed by Inspira. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work properly cited.

¹ Shoshana Zuboff, *The age of surveillance capitalism: The fight for a human future at the new frontier of power* (PublicAffairs, 2019).

² Solon Barocas & Andrew D. Selbst, 'Big data's disparate impact' (2016) 104(3) *California Law Review* 671–732.

³ Justice K.S. Puttaswamy (Retd.) v Union of India, (2017) 10 SCC 1 (India).

The idea of algorithmic governance is the growing reliance upon computational systems in order to influence, direct and define the implementation of public policy as well as administrative choices.¹ Such systems are based on huge repositories of individual and behavioural information, whether it is automated welfare eligibility checks or predictive policing models.² The very mechanisms that allow serving the target with high precision, efficient service provision and evidence informed also allow intrusive surveillance, opaque profiling and making decisions without effective human control.³ This dual character of algorithmic devices implies that data mining as a practice cannot be merely discussed as a technical activity but rather it needs to be interpreted with respect to the constitutional rights, the principles of democracy and the legal protection.⁴

The development of algorithmic governance in the Indian context leaves a complicated legal environment that has developed over the last ten years. In 2017, the Supreme Court of India announced the right to privacy as a fundamental right in the constitutional article 21, in *Justice K.S. Puttaswamy v. Union of India* affirmed that any violation of privacy should meet the criteria of legality, necessity and proportionality. The far-reaching ramifications of this historic jurisprudence are the impact on the data collection, processing, analysis and utilisation by the government and the non-governmental bodies.⁵ The following establishment of *Digital Personal Data Protection Act, 2023* aims at giving a statutory acknowledgment of data privacy concepts like consent, purpose limitation and data minimisation and thus establishing a guideline in the management of personal data in digital era.⁶ Nevertheless, the legal tools have not been explicitly designed to help solve the special issues of algorithmic governance and AI based data mining, especially when these activities include automated profiling, predictive evaluation and obscure decision-making measures that are inaccessible to human inspection.

Algorithms governance is in conflict with the privacy rights today as most AI systems are based on extensive amounts of data including sensitive personal information. Data mining will be able to deduce new individual attributes, behavioural patterns and will create risk profiles even without using the explicit know-how or the consent of the individuals in question. The practices cast doubt on the sufficiency of current legal frameworks, the clarity of algorithmic operations and the mechanisms of accountability that can be used when addressing unfair or discriminatory results.⁷ With the data crossing platforms freely and AIs taking consequential decisions on the availability of services to people, opportunities, and social inclusion, the legal system is left to struggle with the basic issue of how to maintain the rights of privacy and at the same time reap the benefits of algorithmic governance.

This paper aims to critically examine the interplay between the issue of algorithmic governance and the right to privacy in the Indian digital age, which is AI based data mining. It explores the legal system of personal data and privacy, scans how much current laws can fit algorithm governance, recognizes the gaps and ambiguities, and offers normative and policy solutions that may be used to protect the rights of individuals in a time largely of automated decision-making. This study, through a doctrinal and normative approach, based on the Indian constitutional law and statutory provisions, can serve a purpose of understanding how algorithmic governance may be aligned to the strong privacy rights in the fast digitising society.

Legal Framework and Judiciary Perspective

The legislation of algorithmic governance and data mining through AI in India is influenced by constitutional provisions, codified laws and judicial rulings. The most important component of this structure is the constitutional right to privacy which was acknowledged by the Supreme Court of India, as one of the fundamental rights in the landmark case of *Justice K. S. Puttaswamy v. Union of India* in 2017.⁸ The Court in this decision ruled that privacy is informational autonomy, that is, persons have a right to manage the process of collecting, storing and sharing personal information about them. The Court held that any state action that unfairly running into this right must be able to pass the legality,

¹ Karen Yeung, 'Algorithmic regulation: A critical interrogation' (2018) 12(4) *Regulation & Governance* 505–523. <https://doi.org/10.1111/rego.12158>

² Danielle Keats Citron, 'Technological due process' (2008) 85(6) *Washington University Law Review* 1249–1313.

³ Frank Pasquale, *The black box society: The secret algorithms that control money and information* (Harvard University Press, 2015).

⁴ Maneka Gandhi v Union of India, (1978) 1 SCC 248 (India).

⁵ Gautam Bhatia, *The transformative Constitution: A radical biography in nine acts* (HarperCollins India, 2019).

⁶ Digital Personal Data Protection Act, 2023 (India).

⁷ Danielle Keats Citron, 'Technological due process' (2008) 85(6) *Washington University Law Review* 1249–1313

⁸ Justice K.S. Puttaswamy (Retd.) v Union of India, (2017) 10 SCC 1 (India).

necessity, and proportionality tests. These postulates underlie the evaluation of the lawfulness of AI enabled data mining to conduct algorithmic systems of governance of high amounts of personal data.¹

The Information Technology Act, 2000 offers the provision of statutes to deal with the offences of digital and electronic data.² It makes illegal entry to digital systems, alteration of electronic records and stealing of identities. Although the IT Act has always been considered as something related to cybersecurity and electronic fraud, its facilities are now being employed in scenarios concerning data processing using AI, particularly in situations where an algorithmic system processes or abuses personal data without permission.³ As an example, Section 66 and 66C of the Act is used in respect of identity theft and fraudulent use of electronic signatures, which may involve automated mechanisms to produce digital credentials or may work with personal information automated algorithmically.⁴

Digital Personal Data Protection Act, 2023 is the first formal law of protection of personal data in India. The Act enshrines the concepts of consent, purpose limitation, data minimisation and responsibility of data fiduciaries.⁵ In this law, any organization that gathers or processes personal data should seek express and informed consent, have relevant protection measures, and also offer a means through which an individual can retrieve, rectify, or delete their data. Although the Act offers very strong boundaries of protection on personal data in theory, it is predominantly technology neutral and does not mention explicit measures to deal with the challenges of algorithmic governance, automated decision making, or AI supported data mining.⁶ Consequently, the rules and regulations regarding the legal responsibility of the algorithmic systems themselves are still a source of confusion.⁷

The Judicial interpretation of the principles of privacy and data protection has been developing in order to meet the challenges of digital technologies. Besides the Puttaswamy case, (Aadhaar case) stressed that any collection of biometric and demographic data by the state on the basis of identification ought to be conducted in strict compliance to the proportionality and necessity factors.⁸ This ruling has great consequences on the use of AI based systems which are used in governance because automated profiling or predictive decision making can amount to an intrusion to the privacy unless it is well explained, proportionate, and under procedural constraints.⁹

The other important legal aspect is *the Indian Evidence Act, 1872* that provides the admissibility of evidence before the court. The data created by AI and processed with the help of algorithms could be regarded as electronic evidence governed by the IT Act.¹⁰ When algorithmic outputs are used to present evidence in court, courts are starting to struggle with the problem of authenticity, reliability, and explainability.¹¹ There are no clear legal processes concerning algorithmic accountability, and as a result, it becomes difficult to guarantee that the automated decision or data obtained after mining can be used as reasonable evidence. This is something which should be put under judicial scrutiny and careful interpretation of the current provisions on evidentiary to avert unfair prejudice and abuse.

Under administrative and regulatory law Algorithmic governance intersects with statutory requirements on taxation, provision of welfare, financial services, and safety in the public. The AI driven data mining allows predictive evaluation and automatic resource distribution, however, the systems should adhere to basic rights, statutory authorisations, and procedural principles of fairness.¹² It has been reiterated by the courts numerous times that the administrative action, such as the decision made on the background of automated systems, cannot be arbitrary and must also be accompanied by the

¹ *Ibid.*

² Information Technology Act, 2000 (India).

³ Apar Gupta & Raman Jit Singh Chima, 'The Information Technology Act, 2000: A critical analysis' (2018) *Indian Journal of Law and Technology* 1.

⁴ Information Technology Act, 2000 (India), ss 66, 66C.

⁵ Digital Personal Data Protection Act, 2023 (India), ss 4–9.

⁶ Graham Greenleaf, 'Global data privacy laws 2023: India joins the comprehensive data protection regime' (2023) 169 *Privacy Laws & Business International Report* 1.

⁷ Frank Pasquale, *The black box society: The secret algorithms that control money and information* (Harvard University Press, 2015).

⁸ K.S. Puttaswamy (Aadhaar-SJ.) v Union of India, (2019) 1 SCC 1 (India).

⁹ Justice K.S. Puttaswamy (Retd.) v Union of India, (2017) 10 SCC 1 (India).

¹⁰ Information Technology Act, 2000 (India); Indian Evidence Act, 1872 (India), s 65B; see also Anvar P.V. v P.K. Basheer, (2014) 10 SCC 473 (India).

¹¹ Danielle Keats Citron, 'Technological due process' (2008) 85(6) *Washington University Law Review* 1249–1313.

¹² E.P. Royappa v State of Tamil Nadu, (1974) 4 SCC 3 (India).

requirements of transparency and accountability. Any automated procedure that entails negative effects to a person should avail means of recall and reimbursement.¹

Although India has not adopted an extensive law covering the AI systems, the overlap between constitutional, statutory, and judicial standards forms a guideline that can be utilized to govern the algorithmic regulation. The Judicial system has stressed those basic rights including privacy cannot be defeated over by expediency of technological proficiency. Lawyers and other policymakers have proposed that clear criteria of algorithmic transparency, the requirement to conduct impact assessments, the auditability of AI systems, and the methods of challenging automated decisions are necessary.² These steps would put into effect the principles of proportionality, necessity, and legality expressed by the judicial system in the digital environment.

Statistical Landscape of AI Based Data Mining in India

The scope and effects of algorithmic governance in practice can only be understood through an in-depth analysis of the statistical and empirical environment of data collection, processing, and privacy issues in India.³ The popularization of the digital services and AI systems has generated considerable amounts of individual data that are more and more prone to algorithmic treatment, to the purpose of governance, commerce, and security.⁴ Although there is a paucity of statistics, and especially in AI driven data mining, a compilation of government reports, industry surveys, and regulatory disclosures give an insight into the magnitude, extent as well as the privacy connotations of such practices.

- **Growth of Digital Data and Internet Penetration:** The Indian digital environment has grown at a very high rate in the last ten years. *The Telecom Regulatory Authority of India* states that by 2025, the Indian internet users had reached about one billion, which is about seventy percent of the Indian population.⁵ This growth has brought opportunities as well as threats. On the one hand, it has also made algorithmic governance more efficient, predictive, and optimising its resource allocation. Conversely, it has multiplied manifold the amount of individual and confidential information that can be gathered, digested, and mined.⁶

Digital services in every field, such as banking, e-commerce, medical, government websites, and social media, regularly gather personal information to facilitate and analyze it.⁷ In these industries, AI systems utilize massive amounts of data to predict, develop decisions, and analyze predictively. As an example, welfare programs are more and more based on algorithmic checks to verify eligibility, and financial institutions are based on predictive credit scoring programs.⁸ Those are the processes that usually entail aggregation and analysis of personal information at scale, which is concerning the consent, transparency, and autonomy of a person.

- **Privacy Incident and Regulatory Compliance:** The conflict between the AI-supported data mining and the rights of an individual is depicted by increasing rates of privacy violations in India.⁹ According to *the Data Security Council of India*, more than 65 percent of organisations that implement AI systems have difficulties in acquiring fully informed consent with users or meeting the statutory privacy requirements provided by *the Digital Personal Data Protection Act, 2023*.¹⁰ The violation of privacy principles in many organisations occurs unintentionally due to the fact that AI models need large data sets to operate efficiently, and at times the use of data at other uses than those intended when the consent was originally acquired.

Moreover, government agencies have shed some light on case of personal information abuse in other fields such as telecommunications and finance. It has been reported that businesses that gather personal data without strong protective measures, can accidentally reveal people to profiling, automated

¹ Mohinder Singh Gill v Chief Election Commissioner, (1978) 1 SCC 405 (India).

² *The secret algorithms that control money and information* (Harvard University Press, 2015); see also NITI Aayog, *Responsible AI for All: Approach Document for India* (2021).

³ Ministry of Electronics and Information Technology, *India's Digital Economy Report* (Government of India, latest available edition).

⁴ NITI Aayog, *National Strategy for Artificial Intelligence #AIforAll* (2018); National Association of Software and Service Companies (NASSCOM), *AI Adoption Index Report* (latest edition).

⁵ Telecom Regulatory Authority of India. (2024). *The Indian telecom services performance indicators report*. Government of India.

⁶ Internet and Mobile Association of India & KPMG. (2023). *Digital in India report*.

⁷ Reserve Bank of India. (2024). *Report on trend and progress of banking in India*. Government of India.

⁸ National Association of Software and Service Companies. (2023). *AI adoption index report*.

⁹ Data Security Council of India. (2023). *Data protection and privacy compliance survey report*.

¹⁰ Digital Personal Data Protection Act, 2023 (India).

decision making or even targeted marketing campaigns that individuals have not agreed to or may not even be aware of.¹ Such privacy incidents bring out significant concerns that can be addressed by proactive law protection and algorithm supervision processes to avoid informational autonomy system breaches.

- **Empirical Indicators and Statistical Insights:** The data on the empirical level gives a physical idea about the extent of AI based data mining and its engagement with privacy rights.² Although there are few specific statistics to use related to the use of AI, there are more general indicators of the digital activity and privacy issues, which help to draw the picture under which algorithmic governance is being conducted.³

Table 1: Key Indicators of Digital Data Usage and Privacy Challenges in India

Indicator	Value / Statistic	Source / Context
Internet Users in India (2025)	~1 billion	Telecom Regulatory Authority of India, 2025
Organisations Facing Consent Compliance Challenges	>65%	Data Security Council of India, 2023 report
Digital Services Collecting Personal Data	Numerous platforms across e-commerce, finance, social media, healthcare, and government portals	Indicative of AI data sources and algorithmic analysis
Operationalisation of DPDP Rules	14 November 2025	Digital Personal Data Protection Rules, 2025
Constitutional Recognition of Privacy	2017	Supreme Court judgment in <i>Justice K.S. Puttaswamy v. Union of India</i>

The following table shows the magnitude of digital interactions in India and how algorithmic systems have access to large amounts of personal data. The high rate of consent compliance problems, operationalisation of privacy regulations highlights that there is a necessity of constant surveillance, enforceability of regulations, and legal counseling to make sure that AI based data mining does not encroach constitutional and statutory privacy rights.

Collectively, such trends include the explosive scale of digital data, privacy scandals brought forth by AI systems, and empirical markers that reflect consent and regulatory issues, all of which make the area of algorithmic governance and privacy intersect in intricate manners.⁴ It is upon the policymakers, regulators and legal scholars to understand these realities and apply the constitutional and statutory restrictions that exist to ensure that automated decision making does not take away the autonomy of a person or the inherent right to privacy.

Algorithms Governance and Privacy Implications

Algorithms as governing is the application of automated processes and artificial intelligence to inform, direct, and implement decisions in the sphere of the public administration, commercial platforms, and social services. Such systems use AI powered data mining approaches to process large amounts of data, detect trends, foresee behaviour and automatize actions. Although the efficiency, predictive accuracy and scalability of such systems are beyond question, they also cause serious privacy concerns. With India being one of the countries with the highest level of digital adoption and a growing influence of personal data in administrative and commercial decision making, the conflict between efficiency in algorithms and the rights to privacy has become the leading legal and regulatory concern.

The constitutionally recognised right to privacy as under Article 21 in the decision made by the Supreme Court in the *Justice K.S. Puttaswamy v. case. Union of India* requires that any manipulation of personal data should meet the test of legality, necessity and proportionality. Data mining as an AI may pose a threat to these standards in several ways. First, algorithm systems frequently do not only work with individual data in bulk, but reuse it to conduct analytics without the original consent of the individual.

¹ Shoshana Zuboff. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

² NITI Aayog. (2018). *National strategy for artificial intelligence #AIforAll*. Government of India.

³ Ministry of Electronics and Information Technology. (2023). *Annual report*. Government of India.

⁴ Data Security Council of India. (2023). *India cyber threat report*; NITI Aayog. (2018). *National strategy for artificial intelligence #AIforAll*. Government of India.

Second, automated profiling can lead to decisions with material effects on people, e.g. eligibility to welfare programs, loan approvals, or law enforcement investigation, without meaningful reasons. Third, the lack of transparency and accountability due to the opaqueness of algorithms enables the creation of the conditions under which people cannot watch or question the decisions that have a significant impact on them.¹

- **Data Growth and Algorithmic Reach:** One of the fastest-growing nations in digital adoption is India in the last 10 years.² The Telecom Regulatory Authority of India has indicated that in India there were almost one billion internet users by 2025 as compared to 500 million in 2018.³ This digital growth has provided a space where AI systems can get ready access to amounts of personal and behaviour data like never before. Algorithms are being used in public administration more and more in automatic verification in welfare programs, predictive resource distribution, and risk identification in law enforcement.⁴ Likewise, credit scoring, targeted marketing, fraud processing, and customer behaviour analytics of private enterprises are done via AI. The spread of the said systems highlights the magnitude of AI driven data mining processing with sensitive personal data.⁵
- **Privacy implications and AI Based data mining:** Data mining systems powered by AI have the ability to conclude very sensitive personal features, such as behavioural patterns, financial risk, health status and social affiliations.⁶ Such inferences are usually produced unconsciously on the part of the individual and can result in serious outcomes in terms of autonomy, dignity, and service availability. The profiles created by AI can recreate past biases, which will produce discriminatory effects on job opportunities, finances, and access to governmental services. Accountability is complicated by the fact that decision making processes lack transparency. Although the DPDP Act, 2023, provides certain rights, like consent, correction, and redressing of grievances, these will be ineffective when it comes to automated profiling where people do not know fully what is being done with their information.⁷

In addition, the algorithmic systems can be used in cross-border digital ecosystems, where personal data are transferred across jurisdictions, making it even more difficult to adhere to the principles of privacy and constitutional protection.⁸ It is essential to consider not just the advantages of AI based data mining as implemented by the operations but also the infringements of the basic privacy rights that may emerge due to the lack of transparency of the automated processes.⁹

- **Trends and Empirical Illustration:** The increase in digital information and the use of AI can be reflected in the trends of the use of internet, the engagement with digital services, and the awareness of the regulations.¹⁰ The conceptual graph presented below shows how the number of internet users in India is expected to grow over the period between 2018 and 2025 and the projected percentage of AI-dependent services involved in data mining to govern the country and/or make profit.¹¹

¹ Danielle Keats Citron. (2008). Technological due process. *Washington University Law Review*, 85(6), 1249–1313.

² International Telecommunication Union. (2023). *Measuring digital development: Facts and figures 2023*. ITU.

³ World Bank. (2022). *Digital public infrastructure and inclusive growth*. World Bank Publications.

⁴ Organisation for Economic Co-operation and Development. (2019). *OECD principles on artificial intelligence*. OECD Publishing.

⁵ Rouvroy, A., & Berns, T. (2013). Algorithmic governmentality and prospects of emancipation. *Réseaux*, 177(1), 163–196.

⁶ Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2), 1–21.

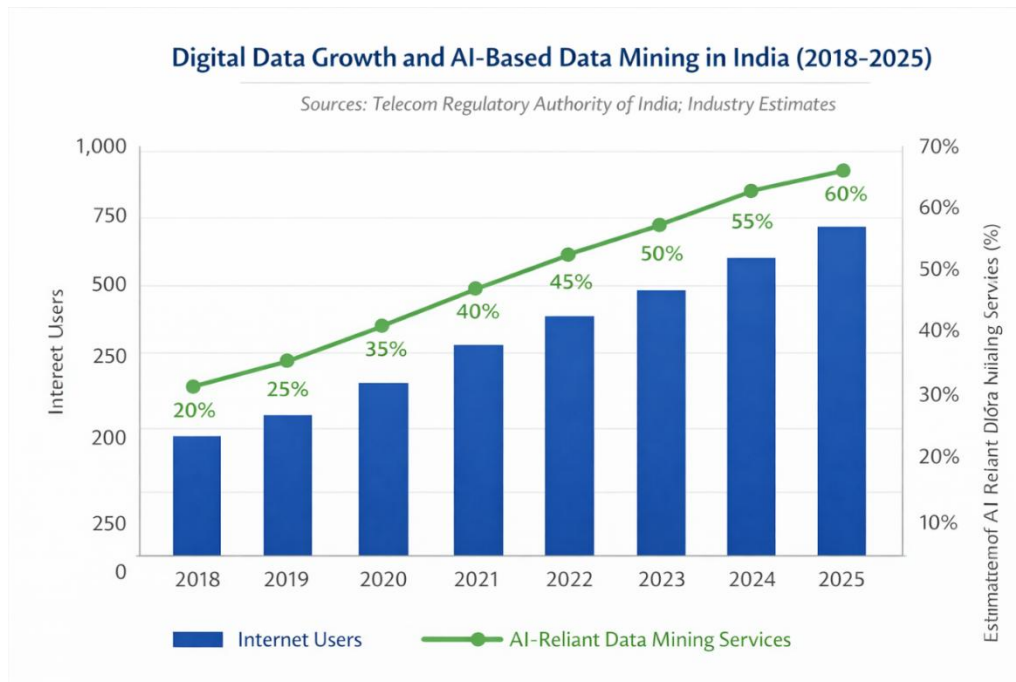
⁷ Burrell, J. (2016). How the machine “thinks”: Understanding opacity in machine learning algorithms. *Big Data & Society*, 3(1), 1–12.

⁸ European Union. (2016). *General Data Protection Regulation (Regulation (EU) 2016/679)*, Article 22.

⁹ Yeung, K. (2017). Hypernudge: Big data as a mode of regulation by design. *Information, Communication & Society*, 20(1), 118–136.

¹⁰ DataReportal. (2024). *Digital 2024: India*. Kepios.

¹¹ International Data Corporation. (2023). *India artificial intelligence market forecast 2023–2027*. IDC.



This graph shows the two ways of digital adoption and AI fueled data mining. The more the amount of personal data, the more the algorithmic governance systems reach and impact, which means that the risks of privacy can become even more significant when the protection is not sufficient.

The emerging trends in the empirical and conceptual realms testify to the necessity to encompass privacy by design and transparency requirements and holders accountability systems into algorithmic governance frameworks. Legal systems should not only control the gathering of data but also provide a standard of automated decision making, auditability and redress. To make sure that the rights to privacy are not weak in the highly automated environment, the courts, regulators, and policymakers are required to understand the current constitutional and statutory protection within the framework of AI.

Legal Analysis of AI Based Data Mining and Privacy Rights

The emergence of algorithmic governance and AI directed data mining in India has posed a major legal and regulatory challenge. Although technological innovation has efficiency potential, predictive potential, and potential to optimise resources, it also brings concerns on the constitutional and statutory provisions that safeguard individual privacy.¹

- Constitutional Protections and judicial interpretations:** Privacy protection in India is based on the Constitution of India, especially on Article 21, that provides the right to life and personal liberty. In Justice K.S. Puttaswamy case The Supreme Court identified privacy as a basic right, including the informational autonomy. The Court elucidated that any invasion into privacy should meet three fundamental conditions, namely legality, necessity, and proportionality.² These principles have a direct application to AI based data mining where algorithm systems verify sensitive personal information and can affect individual access to services, benefits or legal rights.

The Aadhaar decision also broadened the industry of privacy to state that any biometric and demographic data gathered by the state has to be done in strict proportionality and necessity.³

¹ Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3), 477–564. <https://doi.org/10.2307/40041279>

² Chandrachud, D. Y. (2017). Privacy and constitutional values (Concurring opinion). In *Justice K.S. Puttaswamy (Retd.) v Union of India*, (2017) 10 SCC 1.

³ Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. *Washington Law Review*, 89(1), 1–33.

Constitutional scrutiny is hence applied to automated systems applied in the governance such as AI based data mining. Courts have stressed that a person has to maintain any meaningful control over personal data and automatic profiling or decision making should not lead to random and discriminatory results. These constitutional protections offer normative instructions in the management of AI even in the event that technology specific laws do not exist.¹

- **Data Protection Legal Framework:** The legal system in India on the protection of personal data is based on the Digital Personal Data Protection Act, 2023. The principles that are codified by the Act include consent, purpose restriction, data minimisation, and data fiduciary accountability.² It provides individuals (data principals) with rights to access, correct, erase, as well as limit processing of their information. Also, the Act is operationalised by the Digital Personal Data Protection Rules, 2025 which impose procedural duties on data fiduciaries, requirements to act following a breach, and protective measures of sensitive personal data.

Although DPDP Act also offers a legal basis of privacy protection, it is mostly technology neutral and does not specifically address the issues of AI based decision making, algorithmic profiling, and automated data mining practices.³ Therefore, the Act lacks transparency of algorithms, automated decisions impact assessment, and output explainability, which leaves a regulatory void that might allow automated governance systems to run without proper safeguards.⁴

This framework is supplemented by the *Information Technology Act, 2000* which criminalises unauthorised access, electronic fraud and identity theft. The IT Act could apply to the field of AI systems that handle or process personal data because, in these cases, such operations lead to security breaches, fraud, or unauthorized use of data.⁵ Nonetheless, the Act lacks accountability, explainability, and bias reduction of algorithms and focuses more on the judiciary implementation of these elements through interpretation and policy.

- **Judicial Safeguards and Oversight:** The Indian courts have been very instrumental in the development of privacy in the digital era. In addition to the Puttaswamy ruling, the courts in judicial rulings have stressed that automated systems utilized in government administration have to be within constitutional guidelines.⁶ Courts have pointed severally that administrative rulings, such as those based on AI systems, cannot be arbitrary and should observe procedural fairness.⁷

The judicial oversight is a valuable mechanism of making sure that the algorithmic systems of governance are within the demands of legality, necessity and proportionality.⁸ The courts have the right to check AI based data mining activities to determine whether they contain breach of privacy, discrimination or misuse of personal data.⁹ They may also instruct regulatory bodies through creating rules concerning transparency, auditability, and redressing complain mechanisms in use of automated systems.¹⁰ Nonetheless, it is increasingly accepted by legal experts that courts cannot adequately respond to the distinct issues of AI alone, and that legislative and regulatory norms should be developed to meet the needs of algorithmic governance.¹¹

¹ Hildebrandt, M. (2015). *Smart technologies and the end(s) of law: Novel entanglements of law and technology*. Edward Elgar Publishing. <https://doi.org/10.4337/9781782548945>

² Greenleaf, G. (2023). India's Digital Personal Data Protection Act 2023: A comparative analysis. *Privacy Laws & Business International Report*, 186, 1–6.

³ Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2), 76–99. <https://doi.org/10.1093/idpl/ix005>

⁴ Selbst, A. D., & Barocas, S. (2018). The intuitive appeal of explainable machines. *Fordham Law Review*, 87(3), 1085–1139.

⁵ DeNardis, L. (2014). *The global war for internet governance*. Yale University Press. <https://doi.org/10.12987/yale/9780300181350.001.0001>

⁶ Justice K.S. Puttaswamy (Retd.) v Union of India, (2017) 10 SCC 1 (India).

⁷ Maneka Gandhi v Union of India, (1978) 1 SCC 248 (India).

⁸ Aharon Barak. (2012). *Proportionality: Constitutional rights and their limitations*. Cambridge University Press. <https://doi.org/10.1017/CBO9781139035296>

⁹ Citron, D. K. (2008). Technological due process. *Washington University Law Review*, 85(6), 1249–1313.

¹⁰ Veale, M., & Brass, I. (2019). Administration by algorithm? Public management meets public sector machine learning. *Public Law*, 1, 101–123.

¹¹ Pasquale, F. (2020). *New laws of robotics: Defending human expertise in the age of AI*. Harvard University Press. <https://doi.org/10.4159/9780674240943>; See also Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & Governance*, 12(4), 505–523. <https://doi.org/10.1111/rego.12158>

- **Linkage between Laws and AI Governance Practices:** The table below outlines the main Indian legislation along with their main emphasis and how they can be applied to AI based data mining and algorithmic governance.¹ This table shows the overlap between laws, constitutional protection and legal restrictions on automated decision making and guarding of the privacy right.²

Table 2: Indian Legal Framework and AI Governance Practices

Legal Provision / Judgment	Primary Focus	Relevance to AI Based Data Mining
Constitution of India, Article 21	Right to life and personal liberty	Protects informational autonomy; AI systems must comply with legality, necessity, proportionality standards (<i>Puttaswamy v. Union of India</i> , 2017)
Digital Personal Data Protection Act, 2023	Personal data rights, consent, purpose limitation	Regulates collection and processing of personal data; does not mandate algorithmic transparency or explainability
Digital Personal Data Protection Rules, 2025	Operational obligations for data fiduciaries	Provides procedural safeguards for data handling, breach reporting, and consent; gaps remain in AI governance
Information Technology Act, 2000	Cybersecurity, fraud, and identity theft	Applies to unauthorised access, data manipulation, and security breaches involving automated systems
Supreme Court Judgments on Privacy (<i>Puttaswamy & Aadhaar</i>)	Constitutional recognition of privacy, proportionality, necessity	Provides judicial safeguards against arbitrary or disproportionate intrusion; applicable to algorithmic governance and automated profiling
Administrative Law Principles	Procedural fairness and accountability	AI based decisions in public administration must be transparent, contestable, and free from arbitrariness

As this table demonstrates, although India has an excellent base of privacy and information protection statutes, the legal protection of algorithmic regulation remains underdeveloped.³ The legality, necessity, and proportionality principles under the constitution, the DPDP Act and the IT Act can be used to regulate the AI system.⁴ Nonetheless, the lack of required transparency of algorithms, evaluation of impact, and auditability is a major loophole that needs to be addressed by the judges and the legislation.⁵

Conclusion and Policy Recommendations

The growth of algorithmic governance in India is a turning point in the connection between technology, state power, and individual rights due to its fast spread. The use of artificial intelligence-based data mining has irrevocably transformed the processes of making decisions in the public administration, finance, healthcare, law enforcement, taxation, and social welfare. They are built on mass amounts of personal and behavioural data, which are gathered on an ever more digitised population. Although algorithmic systems are efficient, predictive, and scaleable, they are also incredibly threatening to the constitutional values especially to the right to privacy and informational autonomy.

This study has shown that India has a favorable constitutional base on protection of privacy. A doctrinal framework of approaching the state action in personal data is the principles of legality, necessity, and proportionality. The principles are especially applicable to the phenomenon of algorithmic governance where automated systems can guide choices on employment opportunities, welfare benefits, access to credit and even surveillance. Nevertheless, being considered constitutional does not necessarily provide a successful protection in the technological ecosystem that is changing at a quicker pace than the law.

The legislative framework, particularly, the Digital Personal Data Protection Act, 2023, is a major step in the Indian privacy jurisprudence. It brings in consent requirements, limitation on purpose, requirement to minimise data and redress of grievances. However, as discussed in the previous chapters, the Act is mostly technology neutral and does not focus specifically on the unique attributes of

¹ Bhatia, G. (2019). *The transformative constitution: A radical biography in nine acts*. HarperCollins India.

² Balkin, J. M. (2015). The path of robotics law. *California Law Review Circuit*, 6, 45–60.

³ Constitution of India, art. 21; Digital Personal Data Protection Act, 2023 (India); Information Technology Act, 2000 (India).

⁴ 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).

⁵ Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2), 76–99. <https://doi.org/10.1093/idpl/ix005>

the artificial intelligence systems. There is no extensive regulation of automated profiling, predictive analytics, algorithmic bias, and opacity.

Court checks and balances present a significant remedial action. Procedural fairness and non-arbitrariness have been stressed by the courts in the decision making process of the administration. Such principles can be applied to the decisions produced or supported by artificial intelligence systems in a logical manner. However, the judicial review is reactive in nature. It deals with breaches that have taken place. When the harm caused by algorithms is systemic, invisible, or diffused among large cohorts of people, as in the case of algorithmic governance, judicial oversight is not enough. Structural and preventive protection is necessary.

The overall finding of this study is that India is at a crossroad. No longer is algorithmic governance a peripheral and experimental phenomenon. It is integrated into IT infrastructure and government. The question is not whether this will be a case of artificial intelligence application, but how this is going to be regulated in a way that is in line with constitutional morality and democratic accountability. A multi layered regulation approach is necessary in order to address the tension between the rights of privacy and the technological advancement.

Policy Recommendations

- **Implementing a Specific Artificial Intelligence Regulation Framework:** India ought to give a thought to the establishment of a thoroughly detailed legal framework with respect to artificial intelligence systems. Although Digital Personal Data Protection Act regulates processing of personal data, an AI specific law may take into consideration algorithmic transparency, explainability requirements, mitigation of bias requirements, and the compulsory documentation of automated decision making systems. This needs to be stipulated by such legislation, which is high risk AI applications, especially those in governance, law enforcement, financial regulation, and welfare distribution, and place greater compliance requirements in these areas.
- **Compulsory Algorithms Impact Assessment:** In the process of implementing AI systems in government, Algorithmic Impact Assessment should be carried out by authorities. Such tests ought to quantify the risks of privacy, risks of discrimination, data collection proportionality, and the need to have automated decision making. The results must be reported and rendered open to everyone to be transparent. This would be a preventive measure that would operationalise the constitutional tests as explained in Puttaswamy and would convert abstract principles into quantifiable standards.
- **Enhancement of the Data Protection Board:** The Data protection board that is formed by the Digital Personal Data Protection act must be given the mandate of technical expertise in artificial intelligence systems. It must be able to audit algorithms, probe non-transparent decision making systems and penalize those who fail to meet the requirements of transparency and fairness. Developing regulatory agencies is essential since they need technical knowledge of machine learning models and data analysis procedures to regulate them efficiently.
- **Allegiance to Explainability and Right to Human Review:** With automated decisions, there should be a legally enforceable right by the individual subjected to such decisions to require an explanation and human scrutiny. Outputs of algorithms making a significant change to rights, benefits, or obligations cannot be left unquestioned. The presence of a statutory right to an explanation would enhance the procedural fairness and decrease the informational asymmetry between the institutions and individuals. It would also strengthen the dignity aspect of privacy, which will see to it that individuals are not turned into data points in opaque systems.
- **The implementation of Privacy by Design Principles:** Privacy by design must be designed as a mandatory compliance i.e. organisations implementing artificial intelligence systems. This would mean incorporating data minimisation, anonymisation and purpose limitation during development phase and not considering privacy as a post implementation. The regulatory measures, which should be outlined, should be specific standards of safe data storage, encryption, and lack of data retention.
- **Digital Literacy and Public Awareness:** Reform in law should go hand in hand with sensitization. The citizens must be informed of the way their data is gathered, processed and analysed. Digital literacy campaigns can enable people to make consent meaningful and to find

remedies in an event of the violation of rights. The societal responsibility is not only limited to the protection of privacy as a legal matter.

- **International Cooperation and Harmonisation:** Since the digital ecosystem is cross border, India must actively engage in cross border discussions regarding artificial intelligence governance and privacy standards. Regulatory effectiveness can be achieved by harmonisation with global best practices and makes sure India is competitive in the global digital economy. Collusion on issues like the standards of data transfer, algorithmic auditing standards, and ethical AI principles would help reinforce the economic and constitutional goals.

Final Reflections

One of the most significant trends in the modern state administration and the digital society is algorithmic governance. It can improve efficiency, corruption and facilitate data driven policymaking. Meanwhile, it is a threat to institutionalize surveillance, strengthen structural disparities, and erode individual autonomy when it remains unregulated.

The Indian constitutional system that is enhanced by the progressive interpretation of the court offers a strong normative basis to ensure privacy. However, technological innovation is so rapid that it requires a response in the form of proactive legislative and regulation adjustments. Innovation is not thwarted by protecting privacy in the digital age; on the contrary, it is one of the requirements of sustainable and democratic technological evolution.

The future of algorithmic governance in India will be premised on how the lawmakers, courts, regulators, technologists, and the civil society will work together to create systems that will not compromise human dignity. Artificial intelligence should be a device that can be used to advance constitutional values and not to bear them down. India can secure the digital transformation to make the fundamental right to privacy stronger and not weaker by using a principled regulation, institutional accountability and involving people in the process.

References

1. Aharon Barak. (2012). *Proportionality: Constitutional rights and their limitations*. Cambridge University Press. <https://doi.org/10.1017/CBO9781139035296>
2. Balkin, J. M. (2015). The path of robotics law. *California Law Review Circuit*, 6, 45–60.
3. Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review*, 104(3), 671–732.
4. Bhatia, G. (2019). *The transformative constitution: A radical biography in nine acts*. HarperCollins India.
5. Burrell, J. (2016). How the machine “thinks”: Understanding opacity in machine learning algorithms. *Big Data & Society*, 3(1), 1–12.
6. Chandrachud, D. Y. (2017). Privacy and constitutional values (Concurring opinion). In *Justice K.S. Puttaswamy (Retd.) v Union of India*, (2017) 10 SCC 1 (India).
7. Citron, D. K. (2008). Technological due process. *Washington University Law Review*, 85(6), 1249–1313.
8. Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. *Washington Law Review*, 89(1), 1–33.
9. DataReportal. (2024). *Digital 2024: India*. Kepios.
10. DeNardis, L. (2014). *The global war for internet governance*. Yale University Press. <https://doi.org/10.12987/yale/9780300181350.001.0001>
11. Digital Personal Data Protection Act, 2023 (India).
12. E.P. Royappa v State of Tamil Nadu, (1974) 4 SCC 3 (India).
13. European Union. (2016). *General Data Protection Regulation (Regulation (EU) 2016/679)*.
14. Greenleaf, G. (2023). Global data privacy laws 2023: India joins the comprehensive data protection regime. *Privacy Laws & Business International Report*, 169, 1–6.
15. Greenleaf, G. (2023). India's Digital Personal Data Protection Act 2023: A comparative analysis. *Privacy Laws & Business International Report*, 186, 1–6.
16. Gupta, A., & Chima, R. J. S. (2018). The Information Technology Act, 2000: A critical analysis. *Indian Journal of Law and Technology*, 1–25.

17. Hildebrandt, M. (2015). *Smart technologies and the end(s) of law: Novel entanglements of law and technology*. Edward Elgar Publishing. <https://doi.org/10.4337/9781782548945>
18. Information Technology Act, 2000 (India).
19. International Data Corporation. (2023). *India artificial intelligence market forecast 2023–2027*. IDC.
20. International Telecommunication Union. (2023). *Measuring digital development: Facts and figures 2023*. ITU.
21. Justice K.S. Puttaswamy (Retd.) v Union of India, (2017) 10 SCC 1 (India).
22. K.S. Puttaswamy (Aadhaar-5J.) v Union of India, (2019) 1 SCC 1 (India).
23. Maneka Gandhi v Union of India, (1978) 1 SCC 248 (India).
24. Ministry of Electronics and Information Technology. (2023). *Annual report*. Government of India.
25. Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2), 1–21.
26. Mohinder Singh Gill v Chief Election Commissioner, (1978) 1 SCC 405 (India).
27. National Association of Software and Service Companies. (2023). *AI adoption index report*.
28. NITI Aayog. (2018). *National strategy for artificial intelligence #AIforAll*. Government of India.
29. NITI Aayog. (2021). *Responsible AI for All: Approach document for India*. Government of India.
30. Organisation for Economic Co-operation and Development. (2019). *OECD principles on artificial intelligence*. OECD Publishing.
31. Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press. <https://doi.org/10.4159/harvard.9780674736064>
32. Pasquale, F. (2020). *New laws of robotics: Defending human expertise in the age of AI*. Harvard University Press. <https://doi.org/10.4159/9780674240943>
33. Reserve Bank of India. (2024). *Report on trend and progress of banking in India*. Government of India.
34. Rouvroy, A., & Berns, T. (2013). Algorithmic governmentality and prospects of emancipation. *Réseaux*, 177(1), 163–196.
35. Selbst, A. D., & Barocas, S. (2018). The intuitive appeal of explainable machines. *Fordham Law Review*, 87(3), 1085–1139.
36. Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3), 477–564. <https://doi.org/10.2307/40041279>
37. Telecom Regulatory Authority of India. (2024). *The Indian telecom services performance indicators report*. Government of India.
38. Veale, M., & Brass, I. (2019). Administration by algorithm? Public management meets public sector machine learning. *Public Law*, 1, 101–123.
39. Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2), 76–99. <https://doi.org/10.1093/idpl/ix005>
40. World Bank. (2022). *Digital public infrastructure and inclusive growth*. World Bank Publications.
41. Yeung, K. (2017). Hypernudge: Big data as a mode of regulation by design. *Information, Communication & Society*, 20(1), 118–136.
42. Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & Governance*, 12(4), 505–523. <https://doi.org/10.1111/rego.12158>
43. Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.