AI GOVERNANCE IN INDIA: A CRITICAL EXAMINATION OF DIGITAL RIGHTS, CONSTITUTIONAL SAFEGUARDS AND LEGAL ACCOUNTABILITY

Anu, PhD Research Scholar, School of Law, Sushant University, Gurugram

Dr. Himadari S Dey, Assistant Professor, Sushant University, Gurugram

ABSTRACT

Artificial intelligence currently determines how individuals access information, services and decisions from institutions. The influence of this technology raises questions about how the law can hold those who control such power accountable under the constitution. In this article I investigate if the developing governance framework in India protects digital rights and offers ways to fix harm caused by artificial intelligence. It applies to a qualitative doctrinal method to examine constitutional guarantees, court decisions, laws plus official policies. To assist this analysis, the text includes a comparison of two international instruments. The discussion distinguishes between constitutional duties, laws that the state has passed but not fully started, secondary regulations and governance principles that lack binding force.

I argue that protecting privacy does not solve the problems of unfair classification, hidden decision processes, or deception. Privacy laws do not address how companies spread responsibility across long supply chains. India uses a strategy that focuses on innovation and treats different industries separately - this method is flexible, but it is only legitimate if the state provides rules for fair procedures but also ways for citizens to complain. In response, I propose a framework for constitutional accountability - this framework connects the requirement for a legal basis, the balance of interests, equal treatment and clear explanations. It also requires that a human reviews decisions and that victims receive a fix for their injuries. The specific recommendations include tests to see how important uses of technology affect society. There must be records that allow independent experts to check the system. On top of this the state must use safeguards when it buys technology. Responsibility is assigned to the party who controls risks that they can predict.

Keywords: Artificial intelligence governance; digital rights; constitutional safeguards; algorithmic accountability; informational privacy; equality; India.

1. Introduction

Artificial intelligence is a concern for constitutional law when organizations use the technology to perform actions. The predictions from those systems result in legal effects if they determine how individuals receive government welfare, employment, school admissions, banking services or freedom from detention. The leaders of institutions sometimes characterize the tools as helps for decision making but the employees often accept the results without change. There is a need for oversight to focus on where the actual power to decide resides and the results of those choices, instead of the name the manufacturer gives to a software package.

The government of India must ensure that the country gains advantages from artificial intelligence in a way that aligns with the rules of a democracy and the transparency of a marketplace. To use the technology for translating languages, managing office tasks plus searching for data can make services available to more citizens and lower the amount of repetitive work - but the same functions allow for the categorization of individuals for the purpose of exclusion, the creation of false personas and the making of choices that the subjects cannot easily challenge. It is a mistake to view technology as having no inherent bias but also it is also a mistake to view every use of the software as a threat to safety[1].

In this article I argue that a functional regulatory system must connect the power of an institution to specific legal obligations and practical ways to fix harms. The promises regarding "responsible AI" result in actual legal protections only when a person can learn that artificial intelligence significantly changed the outcome of an important decision. To ensure this the person must be able to see the reasons for the choice, fix any facts that are not true and ask a separate authority to review the case again.

This concept of Digital Rights is used here purely as an umbrella term to describe the existing rights and proposed measures that seek to protect digital rights. This does not mean that India has a comprehensive statutory list of digital rights[2].

The discussion then moves from constitutional underpinnings to looking at what statutory

[1] Press Info. Bureau, Gov't of India, India AI Governance Guidelines (Feb. 15, 2026), https://www.pib.gov.in/Pressreleaseshare.aspx?

[2]Ministry of Elecs. & Info. Tech., Gov't of India, Notification G.S.R. 843(E), Gazette of India, Extraordinary, pt. II, sec. 3(i), No. 757 (Nov. 13, 2025), https://www.meity.gov.in/static/uploads/2025/11/c56ceae6c383460ca69577428d36828b.pdf.

coverage exists and how accountability can be improved. A constitutional accountability mechanism is proposed following the journey of implementing a system to providing redress to individuals. This provides a baseline process that can apply across different sectors. This should not however be seen as the only option as a new regulator or a comprehensive AI Act may be implemented.

2 Research Problem and Objectives

There can be a gap between diffuse legal enforcement and concentrated technological risk. When an individual suffers harms caused by an automated decision, there can be multiple parties involved who will have control over one of the many sources of error in the system. This can include the implementing organisation, third-party supplier, generic model supplier and several data suppliers. While there may be categories in the law imposing obligations on certain parties, there may be a lack of ability for the claimant to gather the necessary evidence. The aims of this study were to identify constitutional principles that govern the use of consequential AI, identify the extent and gaps in data protection and digital governance laws within India, evaluate barriers to attribution, explainability and remedies and create practical and proportionate protections.

3 Research Questions

- What principles of privacy, equality and natural justice should be considered when evaluating consequential AI use within India?
- Which areas of harms will current digital regulation cover and which areas need new obligations or co-ordination between parties?
- How can accountability be distributed between the AI value chain to ensure different obligations are placed based on the level of control?
- What level of protections would be required to ensure effective constitutional protection for an impacted individual?

4 Research Methodology and Scope

This is a qualitative legal doctrinal and normative study. This means a range of constitutional

provisions, case law, legislation, commencement notices, secondary legislation and official governance documents were studied. Priority was given to primary sources. Materials were chosen for their connection to privacy, equality, freedom of expression, natural justice, regulatory accountability and remedies. The main policy documents used were NITI Aayog's responsible AI methodology, India AI Governance Guidelines and official guidance documents.[3]

The research was carried out in three parts. First, identifying the legal status and protections of each document. Then, analysing whether these protections would be sufficient for hypothetical consequential use cases. Finally, creating recommendations for reform for areas that do not fully provide accountability or remedies. The use cases are hypothetical to show potential issues with the law. There is no specific information about any consequential uses within India or findings from a dataset. 'Should'/'proposed' indicates what the author believes should be done. Where the law currently exists, the document and its legal status is mentioned.

The comparative element only looks at the governance provided by the examples of the European Union AI Act and UNESCO Recommendation. This is not an extensive comparison between jurisdictions and does not assume any foreign laws apply within India. No interviews, surveys, experiments or quantifiable data was taken so it cannot be identified how common discriminatory systems are, how expensive compliance will be or prove causation.

The cut-off date for the legal research was 25th October 2026. Any provisions not yet commenced have been assessed based on their current design. This should not be assumed to be enforceable. This is particularly the case for the Digital Personal Data Protection Act, 2023. Only the documents indicated have been mentioned. This is not an extensive list of all requirements across all sectors.[4]

5 Review of Related Research and Governance Literature

The 2021 NITI Aayog approach document outlines the key principles of responsible AI including safety, equity, inclusivity, privacy, transparency, and accountability. This is useful to note as it demonstrates that there is a social aspect to AI system quality. However, while

[3] Ministry of Elecs. & Info. Tech., India AI Governance Guidelines (2025), https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc2025115685601.pdf
[4] NITI Aayog, Responsible AI for All: Approach Document for India, Part 1—Principles for Responsible AI (Feb. 2021), https://www.niti.gov.in/node/326

there are guiding principles within public policy, it still needs to be translated into a process to ensure those seeking to bring a claim against an organisation can do so. The key consideration is how to translate these guiding principles into procedures that can be enforced.

The India AI Governance Guidelines and Government explanation both support the innovation driven approach, with cross sectoral principles and collaboration through the AI Governance Group. The guidelines have been released by the Ministry of Electronics and Information Technology in November 2025. This includes the focus on accountability throughout the value chain and collaboration through the AI Governance Group and expert bodies. While this is an encouraging direction for public policy, the level of protection will be determined based on the authority, resources and process. Just because an entity is mentioned within a policy does not mean that it has statutory authority.

The UNESCO Recommendation (2021) outlines that AI ethics should be aligned with human dignity, human rights and responsibility across a life cycle.[5] The EU AI Act demonstrates how risk-based governance can be applied to categories different types of AI usage and document and oversee. This is useful as it helps to identify the processes carried out by the institution. However, as this is a recommendation it does not have the same legal force as the others.[6]

Overall, it becomes clear that whilst there is agreement on the need for fairness and accountability, there are still unclear processes to implement. This article will explore how to link a process that can be applied to individuals to an auditing process at an organizational level.

6 Constitutional Foundations of AI Governance

6.1 Equality

There are a number of constitutional principles relating to equality through Articles 14, 15 and 16.[7] These set out protections against inequality and discrimination when the state uses AI. This means that if an entity uses AI to classify, they should ensure they have a lawful reason

[5]UNESCO, Recommendation on the Ethics of Artificial Intelligence (Nov. 23, 2021), https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence
[6]Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L 1689), arts. 9–15, 26–27, https://eur-lex.europa.eu/eli/reg/2024/1689/oj.
[7] INDIA CONST. arts. 14–16.

for doing so. Simply saying they rely on statistical correlation will not protect them from a constitutional challenge.

For example if an organisation develops a model that determines suitability based on continuous employment, this may disadvantage those who have had interruptions to their employment due to caring responsibilities. Similarly if location or education is used as a proxy for social deprivation. Simply knowing that they have caused an unequal outcome will not be enough. The nature of the protection, the entity involved, the justification and evidence must be considered.

To ensure a meaningful audit, the entity should consider whether the variable they have chosen to target is truly aligned with the lawful aim. If the model is developed to determine similarity to previous successful applicants, then this may just reinforce previous preferences. Also, a high overall accuracy may hide inaccuracies for certain groups. Public entities should therefore try to justify why their criteria are suitable, consider any disparity and provide a way to re-consider.

6.2 Privacy

In Justice K. S. Puttaswamy (Retd.) v. Union of India, [2017] 10 SCC 1 the Supreme Court recognised the right to privacy as being protected within the Constitution. This has been further discussed by the supreme court linking it to dignity, freedom and autonomy.[8] This can be used to ensure that when the state uses AI, there is consideration of the legal authority, legitimate aim, proportionality and protections in place. However, this did not create a specific code for AI and does not give a general right to source code.

The doctrine can be implemented by ensuring that data collected for one purpose cannot be used for every predictive purpose. Any new surveillance or profiling systems should be considered with regard to their specific public aim, less invasive options, retention and access. Just because the information is technically available does not mean it should be provided without a reasoned justification. Particularly if combining regular data means that inferences can be made that were never disclosed.

[8]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India); Justice K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 S.C.C. 1 (India).

6.3 Freedom of Expression

AI governance can also relate to the conditions of freedom of expression in the public. In Anuradha Bhasin v. Union of India [2020] 3 SCC 637 the court discusses how the Constitution protects freedom of expression and trade through the internet. This can be applied to AI through analogy. There is no excuse for the administration to not provide justification for any restrictions.[9]

While systems can be developed to detect harmful synthetic media, there is a risk of incorrect classifications of satire, art and documentation. This can still be protected by ensuring there are procedures in place to ensure there is a difference between unlawful and artificially generated. The constitutional consideration is that there should be justification, proportionality and protection for any restrictions. Also ensuring there is a meaningful way for the individual to challenge.

6.4 Fairness

Within constitutional law there is a precedent set through Maneka Gandhi v. Union of India [1978] 1 SCC 248 that there should be fair processes in place when affecting personal liberty.[10] This can be applied to AI to ensure that there is no right to object if the individual cannot identify the error or reasoning. A meaningful hearing should be provided where they can engage with the true reason.

A meaningful human review should not simply involve someone pressing approve. There should be authority to change the outcome, access to the relevant data and time to consider the objection. If staff are only rewarded for speed or agreeing with the system, there may be little real oversight. This should be considered if an entity claims that they have human involvement to ensure their process is safe.

6.5 Public and Private Power

The constitutional considerations will most directly apply to the state. The private entity will need to be analysed based on the constitutional principles and any statutory, contractual,

[9] Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India).
[10] Maneka Gandhi v. Union of India, (1978) 1 S.C.C. 248 (India); Madhyamam Broad. Ltd. v. Union of India, 2023 S.C.C. OnLine S.C. 366 (India).

consumer or other considerations. A private company cannot be treated as being the same as the State. However, if a public authority purchases or outsources an AI service they will still be accountable for their decisions. Therefore the way they purchase should ensure they have the data and access required to perform their public duties.

7 India's Emerging Regulatory Landscape

7.1 Data Protection

The Digital Personal Data Protection Act, 2023 sets out a framework for digital personal data. This includes fiduciary obligations and rights for individuals. Within the legislation there are additions for Significant Data Fiduciaries, specific exemptions and an enforcement body through the Board. There is no general right to explanation for all automated decisions or general prohibition of consequential decisions being made solely by automation.[11]

It is important to consider the commencement of the legislation. G.S.R. 843(E) (13 November 2025) will cause specific provisions to take effect when published. After one year specific provisions will also take effect and most substantive processing obligations and individual rights will take effect eighteen months after being published (13 May 2027). At the time of researching this article the provisions taking effect after one year have not yet taken effect. The provisions taking effect after eighteen months will be considered as they have been enacted. The Digital Personal Data Protection Rules, 2025 should be read alongside their commencement provisions.[12]

Overall it can be seen that data protection cannot provide all governance for AI. There may be a reason to object to a decision as it may be unfair in its aim, inference or consequence even if the data is accurate. Conversely if there is an inaccurate prediction this does not constitute a breach of data protection. A thorough framework should include tests for lawful processing and justifiable decisions.

7.2 Synthetic Information

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code)

[11] Digital Personal Data Protection Act, No. 22 of 2023, §§ 3, 8–13, 17–18, 29, 33 (India)
[12]Ministry of Elecs. & Info. Tech., Gov't of India, Digital Personal Data Protection Rules, 2025 (2025), https://www.meity.gov.in/documents/act-and-policies/digital-personal-data-protection-rules-2025-gDOxUjMtQWa

Amendment Rules, 2026 were notified on 10 February 2026. They came into force on 20 February 2026. This covers synthetically generated information and specific exemptions for regular or genuine activities. [13]

While this demonstrates targeted consideration to content related harms, it does not solve issues with AI supported recruitment, clinical assistance or public administration. Also not all AI developers will be intermediaries and the legal responsibility will depend on their role and the provision being used. This shows that the remedy should be applied to the actual activity.

7.3 Guidance

Guidance can be useful to ensure consistent terminology, testing and collaboration. The flexibility will help sectors adapt to changes in systems. However, the extent to which it provides protection will depend on the legal basis. Voluntary guidance, contractual procurement conditions, statutory rules and judicial directions will all have different consequences. Compliance with one should not be seen as compliance with others.

If using the AI for consequential purposes, the institution should have a public record of the requirements that are mandatory, who is overseeing compliance and where to complain. A coordination body can help overcome any overlap. However this is not a remedy. The institution should be designed to ensure there is an authority that can investigate, request information and enforce correction based on a true legal mandate.

8 Accountability Issues Through the Value Chain

8.1 Liability

AI can be split across a number of organisations. The provider may have control over how the model is designed, the vendor may have control over how it is configured for a sector, the deployer could be setting the threshold and the operator may ignore the warning. The correct consideration should be to think about who had control over the risk, what information they had and if their actions contributed to the harm. If every issue is blamed on the final user there will be no consideration of the choices made by those up the chain.

[13]Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Feb. 10, 2026) (India).

This article suggests there should be differing responsibilities. The provider should document any material limitations and support investigations into proven issues. The deployer should ensure it is suitable for their use, staff are trained and results are monitored. The public authority should be responsible for ensuring their decisions are lawful and fair. These are suggested considerations and are not mandatory. The claimant must prove a cause of action under the relevant law.

8.2 Evidence

The individual may only know that their application has been refused. The entity will have details of the inputs, model version, threshold, instructions and any reviews. Without proper disclosure procedures the individual will not know if there was an issue with the data, unlawful criteria or misuse. If detailed evidence is required to gain access to the relevant data this may mean there is no remedy.

This can be overcome by having proportionate retention of data. The data should be labelled with the version, relevant inputs, outcome and any material human intervention. The data should only be retained for specific purposes and by law. Regulators and the courts should have appropriate means to investigate confidential information whilst protecting legitimate security and commercial interests. It is not always necessary or sufficient to publish source code.

8.3 Individual and Systemic

Whilst an individual may appeal and this can rectify an issue with one rejection, it will not expose any repeated errors affecting a whole group of people. Whereas a systemic audit can improve future outcomes but may not provide any remedy for the injured party. This should be considered within the governance. If there are repeated complaints then an investigation should be carried out. If there are systemic failures then decisions that have been materially impacted should be reviewed where possible.

Reforms should also be made to ensure that there is a difference between sanction, compensation, correction and prevention. A sanction to an organisation does not necessarily mean compensation for the individual and correcting the data does not necessarily mean they have been compensated for their lost opportunity. The correct remedy will depend on the forum and legal basis. Future legislation or authorised sectoral measures should specify what remedial

action should be taken at an organisational level and for the individual.

9 Proposed Constitutional Accountability Framework

This framework is prescriptive. It includes 6 elements to ensure that the institution considers the following points:

1. Legality and Purpose

Identify the authority, lawful purpose and the actual decision the AI will be involved in. Explain why the system is suitable to complete this task and if there was a less invasive and/or less exclusionary method.[14]

2. Impact

Consider the foreseeable impact on privacy, equality, freedom of expression and essential opportunities. Consider testing relevant languages and populations. Identify any unacceptable uses and note any uncertainties. This should be updated if there are material changes to the system.[15]

3. Transparency

Inform the individual of any material involvement of AI. If there is a consequential adverse decision then there should be usable reasons. The explanation should highlight the key factors and what steps can be taken to correct. Providing the claimant with hundreds of pages of technical information is not useful.[16]

4. Accountability

Ensure there is an competent reviewer with the ability to change the outcome and access to the evidence. This should be available to those with limited digital access.

[14] INDIA CONST. arts. 14, 21; Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
[15]Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), 2024 O.J. (L 1689), arts. 9, 27 (EU) (comparative illustration).
[16]Maneka Gandhi v. Union of India, (1978) 1 S.C.C. 248 (India); Madhyamam Broad. Ltd. v. Union of India, 2023 S.C.C. OnLine S.C. 366 (India)

5. Traceability

Ensure proportionate data is retained, authorised investigation and consideration of the effectiveness of the remedial action. Audit should consider the specific task and circumstances of use. Avoid providing a general certificate of ethical quality. The auditor should disclose what they have covered, any limitations and conflicts of interest.[17]

6. Remedial Action

Identify who is responsible, the forum and what remedy is available. If the decision is causing disruption to an essential service urgent remedial action may be required. Aggregate complaint data should be considered to identify any recurring failures.[18]

The framework should be proportionate to the consequence. If the AI is being used for regular drafting support then there is no need to impose the same requirements as if it has a material impact on liberty or essential benefits. The risk should be considered based on severity, scale, vulnerability and whether it can be reversed. Even a simple classification rule may require close consideration if it has serious consequences.

10 Implementation

Public procurement can be used to immediately implement. Contractual requirements should include documentation, evaluation access, cooperation with incidents and an exit plan. Authorities should avoid purchasing systems that will prevent them from providing reasons or relevant data. This will provide additional protection but should not be seen as replacing the legal consideration.

Sectoral regulators should define the requirements for performance and review based on the circumstances. Having a standard baseline will ensure consistency across sectors. Technical bodies will develop testing methods. It is important to ensure the roles are separated. An organisation promoting adoption should not have sole judgement on if a contested use has sufficient protections in place. Independent review and publishing reasons can help provide

[17] UNESCO, Recommendation on the Ethics of Artificial Intelligence ¶¶ 50–52 (Nov. 23, 2021) (nonbinding recommendation), https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence
[18]INDIA CONST. arts. 32, 226 (constitutional remedies); Digital Personal Data Protection Act, No. 22 of 2023, §§ 8–13, 18 (India)

credibility.[19]

Smaller organisations may need to share evaluation facilities, contract templates and practical guidance. Proportionate implementation will reduce unnecessary duplication but serious risks should not be ignored. Publicly supported testing can increase access to compliance expertise. Particularly if deploying in regional languages or for applications to marginalised communities.

Any proposed sandboxes should have a defined time frame, entry criteria, monitoring and exit criteria. They should not be seen as an excuse to ignore constitutional obligations. Consider whether those involved can identify and rectify any failures.

11 FINDING

Based on the doctrinal analysis there are four main findings. Firstly constitutional principles can be used to assess public use of AI however they need to be translated into processes and evidence to be effective for individuals. Secondly there needs to be a clear distinction between enactment, commencement and guidance. This will avoid overstating the current level of protection. Thirdly data protection and content regulation will address some key aspects but will not answer all the questions around discriminatory decisions and liability. Lastly responsibility will be most feasible if it is based on control over the risk and linked to investigation and remedies.[20]

The main argument against is that adding additional processes may slow down deployment and benefit larger companies. This is a valid argument and requiring a full assessment for every low consequence use would be a waste of resources. This can be addressed by focusing on binding protections for consequential situations, providing common compliance tools and simplifying the requirements for easily reversible decisions. The regulator should also ensure they are being proportionate with their requirements.

Another argument is around trade secrets and security. If there is no limit to disclosure then sensitive systems may be exposed and manipulated. However this should not mean there is no explanation. There could be a graduated approach to disclosure to ensure the individual has the

[19] Ministry of Elecs. & Info. Tech., India AI Governance Guidelines (2025), https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc2025115685601.pdf (policy guidance, not an independently enforceable procurement mandate).
[20]INDIA CONST. arts. 14, 21; Digital Personal Data Protection Act, No. 22 of 2023 (India)

relevant reasons but the court or authorised investigator can look at the protected technical information. The real consideration is what information is needed for effective investigation and who it should be provided to.[21]

These findings are prescriptive. This article does not show that any of the proposed audit methods will remove bias or that a specific structure will ensure compliance. Empirical research should be carried out to consider the outcome of complaints, effectiveness of review, error patterns in subgroups and cost of implementing protections in different sectors.

12 CONCLUSION

AI governance within India should be considered based on whether the institution can justify consequential uses and provide effective remedies to those affected. Constitutional protection is still relevant as decisions will be mediated through models, vendors or automated interfaces. Just because technical processes have been outsourced does not mean the entity cannot be identified.

India has an emerging framework that can provide a basis for coordinated and contextual governance. However the principles within policy should have a pathway for implementation. The constitutional accountability framework proposed will ensure there is a lawful purpose, impact, explanation, review, traceability and remedy. The most important practical consideration is that the institution using AI has the ability to understand and rectify the consequences they are responsible for. Innovation will be more sustainable if those affected can challenge errors and the institution can learn from them.

[21] Madhyamam Broad. Ltd. v. Union of India, 2023 S.C.C. OnLine S.C. 366 (India)

REFERENCES:

- Government of India, Ministry of Law and Justice, Legislative Department. The Constitution of India. Articles 12, 14–16, 19, 21, 32 and 226. Official editions: https://legislative.gov.in/constitution-of-india/.

- NITI Aayog. (2021). Responsible AI for All: Approach Document for India, Part 1—Principles for Responsible AI. https://www.niti.gov.in/node/326.

- Ministry of Electronics and Information Technology. (2025). India AI Governance Guidelines. Official policy document: https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc2025115685601.pdf.

- Press Information Bureau, Government of India. (2026). India AI Governance Guidelines. Official explanatory account. https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=2228315&lang=2&reg=48.

- Digital Personal Data Protection Act, 2023, Act No. 22 of 2023. Sections 3, 8–13, 17, 18, 29 and 33. https://www.indiacode.nic.in/bitstream/123456789/22037/1/a2023-22.pdf. Read subject to the commencement notification in reference [6].

- Ministry of Electronics and Information Technology. (2025). Notification G.S.R. 843(E), dated 13 November 2025, under section 1(2) of the Digital Personal Data Protection Act, 2023. Gazette of India, Extraordinary, Part II, Section 3(i). https://www.meity.gov.in/static/uploads/2025/11/c56ceae6c383460ca69577428d36828b.pdf.

- UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence, adopted 23 November 2021. https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence.

- European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 (Artificial Intelligence Act). Particularly Articles 9–15, 26 and 27, read with the applicable version and commencement provisions. https://eur-lex.europa.eu/eli/reg/2024/1689.

- Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (nine-judge bench). See also the Supreme Court's discussion of the privacy ruling in Justice K. S. Puttaswamy (Retd.) v. Union of India, (2019) 1 SCC 1, judgment dated 26 September 2018. Official later judgment: https://api.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf. The AI applications in this article are the author's analysis, not holdings in these cases.

- Anuradha Bhasin v. Union of India, (2020) 3 SCC 637. Judgment dated 10 January 2020. https://api.sci.gov.in/supremecourt/2019/28817/28817_2019_2_1501_19350_Judgement_10-Jan-2020.pdf.

- Maneka Gandhi v. Union of India, (1978) 1 SCC 248. For subsequent Supreme Court treatment of procedural fairness and natural justice, see Madhyamam Broadcasting Ltd. v. Union of India, 2023 SCC OnLine SC 366, judgment dated 5 April 2023. https://api.sci.gov.in/supremecourt/2022/6825/6825_2022_1_1501_43332_Judgement_05-Apr-2023.pdf. AI-specific procedural proposals in this article are normative applications.

- Ministry of Electronics and Information Technology. (2025). Digital Personal Data Protection Rules, 2025. Official publication page: https://www.meity.gov.in/documents/act-and-policies/digital-personal-data-protection-rules-2025-gDOxUjMtQWa.

- Ministry of Electronics and Information Technology. (2026). Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E), dated 10 February 2026. Gazette of India, Extraordinary, Part II, Section 3(i). https://www.meity.gov.in/static/uploads/2026/02/f55fe52418b03f58b0669f6a8bc03b6d.pdf.