Artificial Intelligence And Digital Governance: Emerging Legal Challenges In India

Pooja[1], Deeksha Chaudhary[2], Ananya Rastogi[3]

[1]Assistant Professor of Law at KCC Institute of Legal & Higher Education, Greater Noida, India. Email-piyushikohli7@gmail.com
[2]Assistant Professor of Law at KCC Institute of Legal & Higher Education, Greater Noida, India. Email-shailychaudhary1991@gmail.com
[3]Assistant Professor of Law at KCC Institute of Legal & Higher Education, Greater Noida, India. Email-ananya20rastogi@gmail.com

Abstract
The use and emergence of Artificial Intelligence (AI) and new digital technologies are changing how governments, businesses and public institutions provide services, manage information and make decisions. The growing adoption of these technologies does carry a number of legal issues related to privacy, data protection, transparency, accountability, non-discrimination, cybersecurity and content created by artificial intelligence, which can add to the Innovation and Efficiency and human-centric digital transformation of the Industry 5.0 paradigm. The issues raised here highlight the need for a sustainable development of technologies that is built on digital governance, which is responsible and legally accountable. This paper analyses the new legal hurdles that are being raised with the implementation of AI in India's e-governance system. In particular, it reviews the effectiveness of current legal and policy frameworks to tackle privacy and data protection, algorithmic accountability, transparency, discrimination, cybersecurity and the regulation of synthetically generated information. The study has a doctrinal and analytical legal research methodology. It explores the Constitution of India, the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (amended) and other judicial decisions and Government of India policy documents on responsible AI. The National Strategy for Artificial Intelligence and the NITI Aayog's Responsible AI framework are reviewed to gain insight into India's changing stance on the responsible development of technology. The paper suggests that India's governance policy on AI needs to consider the technological progress along with the constitutional principles and individual rights and public accountability. It proposes a rights-oriented as well as risk-sensitive framework emphasising transparency, human oversight, data protection, accountability and also effective grievance redressal.

Keywords: Artificial Intelligence, Digital Governance, Responsible AI, Data Protection, Algorithmic Accountability, Privacy, Cyber Law, AI Regulation.

1. INTRODUCTION

Artificial Intelligence (AI) is one of the most significant technological advances of the current digital age; its applications span public administration, healthcare, finance, education, employment, business and social and economic life in general. AI systems have become more proficient at handling vast amounts of data, detecting patterns, producing content and aiding decision-making, offering opportunities for innovation and digital transformation. Simultaneously, the use of AI presents numerous privacy, data protection, transparency and accountability, discrimination, cybersecurity and even responsibility questions. These concerns are especially relevant when AI-powered technology could have an impact on an individual's rights or have implications for how citizens, businesses, and public authorities interact with each other or public services.

AI tools and solutions should also be considered as part of the technology shift that is part of the Industry 5.0 adoption. The Industry 5.0 approach is more focused on human-centricity, sustainability and resilience, going beyond just automation and technological efficiency (European Commission, 2021). In the broader picture, responsible innovation entails that technology development should go hand in hand with suitable ethical, institutional and legal protections. The overall theme of the present conference "Innovation and Entrepreneurship for Sustainable Business in the Industry 5.0 Era" gives the general thematic background for the discussion of the relationship between technological innovation and governance and sustainability. Its sub-theme on Legal aspects of Artificial Intelligence and digital transformation also offers a useful interdisciplinary context to scrutiny of the legal issues arising from AI and digital transformation.

Artificial Intelligence governance has emerged in India through a mix of ad hoc laws, subordinate law, constitutional principles, judicial decisions, and government programs.In India, governance around Artificial Intelligence has not been created by one complete law, but rather through amalgamation of the existing laws, sub-ordinate

laws, constitutional principles, judicial decisions, and government programmes. AI has been recognised as one of the key technological advancements for India in the National Strategy for Artificial Intelligence (NITI Aayog, 2018) and the applications of AI have been discussed in various sectors such as healthcare, agriculture, education, smart cities, and infrastructure, as well as the ethical and regulatory concerns of the development and use of AI. The strategy thus set a crucial precedent for India's future policy debates on AI.

The policy strategy that emerged then about the concept of responsible Artificial Intelligence. The Principles for Responsible AI (NITI Aayog, 2020) outlined by NITI Aayog involved the following principles: safety and reliability, equality, inclusivity and non-discrimination, privacy and security, transparency, accountability and protection of positive human values. These principles show that there are more than just technical aspects to consider in assessing AI's impact on governance, and that the impacts of AI use will need to be considered for individuals, institutions and society. NITI Aayog also highlighted that the risks associated with AI may vary from context to context and application to application and advocated for a calibrated and context-specific approach to the governance of AI (NITI Aayog, 2020).

This developing regulatory regime is an integral part of India's existing information-technology regime. The Information Technology Act, 2000 is the main legislation which covers some of the matters related to electronic governance and regulation of information technology in India. The Act also gives legal recognition to electronic records and electronic signatures and also includes provisions related to electronic governance, intermediary responsibilities and offences relating to computer systems and electronic information (The Information Technology Act, 2000). As a result, the bill was passed before the emergence of current generative AI and other advanced AI tools, but a number of its provisions are still applicable to the current digital landscape where AI tools are created and used.

Data protection is another key aspect of AI governance. AI systems may involve the collection, processing, analysis or use of substantial quantities of data, including data relating to identifiable individuals. The Digital Personal Data Protection Act, 2023 provides a statutory definition for the processing of digital personal data and acknowledges the importance of balancing the individual's right to protection of their personal data with the need to process personal data for lawful purposes. The Act also imposes responsibilities on Data Fiduciaries and grants rights and protection for Data Principals for the processing of digital personal data (The Digital Personal Data Protection Act 2023). However, the relationship between data protection and AI also brings to the fore several questions on lawful processing, consent, legitimate uses, data governance, individual rights and organisational accountability.

The regulatory landscape is also starting to reflect concerns over the risks arising from content created using AI and synthetic content. India's intermediary regulatory regime was amended with the introduction of the provisions of synthetically generated information in the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026. The Ministry of Electronics and Information Technology (MeitY) notified the amendments and they became effective on 20th February 2026 (MeitY, 2026). The creation or manipulation of synthetic information shows the need for digital regulation to meet technological capabilities that can generate or modify audio, visual and audio-visual information, which can seem authentic or synonymous with real persons or events (MeitY, 2026).

The constitutional aspect of the governance of AI is also important. AI-powered technology could include comprehensive data collection, profiling, facial recognition, automated assessment, and other data processing which could impact individual autonomy and privacy. The Supreme Court of India in Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017 declared that the right to privacy is a constitutionally protected right and established the link with the guarantees of life, personal liberty and other fundamental freedoms under Part III of the Constitution. The judgment also held that privacy is not absolute, and that the interference of the State with privacy has to meet constitutional requirements such as legality, a legitimate State aim and proportionality (K.S. Puttaswamy (Retd.) v. Union of India, 2017).

In this backdrop, the present paper delves into the new legal issues pertaining to the AI and digital governance domain in India. The paper emphasizes, among other points, privacy and data protection, algorithmic transparency and accountability, discrimination, cyber security, AI-generated content and synthetically generated content and the overall need for responsible technological innovation. Uses doctrinal and analytical legal research skills and considers legislation, subordinate legislation, judicial decisions and government policy documents. The goal isn't to judge the current framework as completely satisfactory or unsatisfactory for India, but to assess its ability to address new issues raised by AI

and to determine if there are gaps in the existing rights and institutional protections that need filling. This paper argues that a balanced governance framework for AI in India must be principled, balancing technological innovation with legal accountability. Technological advancement should be encouraged but innovation should be subject to a framework that safeguards constitutional values, privacy, data protection, equality, transparency, human control over technology and effective accountability. This is aligned with the human-centric paradigm of Industry 5.0, as well as the overall goal of responsible innovation (European Commission, 2021).

ARTIFICIAL INTELLIGENCE, DIGITAL GOVERNANCE AND RESPONSIBLE INNOVATION

Artificial Intelligence (AI) is broadly defined as a technology area focused on systems that can learn, sense, reason, solve problems, and make decisions, which are traditionally attributed to human intelligence. According to the NITI Aayog National Strategy on Artificial Intelligence, AI is defined as intelligent machines that carry out cognitive functions like thinking, perceiving, learning, problem-solving and decision making (NITI Aayog, 2018). AI systems can generate outputs that affect decisions or actions without using the typical rule-based logic that is employed in computer programs, which makes this understanding relevant to legal analysis.

Machine Learning (ML) is an important method of AI, in which systems learn patterns from data and then apply those patterns to making predictions, classifications or other output. The legal significance of machine learning is not only that it is technically able to process data, but also that the quality and nature of the data used to train or operate such systems can affect the results (or outputs) of their use. As such, data quality, bias, reliability, transparency and accountability questions arise when machine-learning systems are adopted in situations that impact individuals.

Generative AI are applications of AI that can create new content such as text, images, audio, video, or other output from a prompt or input from a user. AI has become more relevant to the legal world thanks to generative AI, which can produce content that looks like real-world and/or human-created text. With the advent of AI-generated and synthetically generated content, there has also been a rise in concerns about authenticity, misinformation, privacy, IP, and the responsibility for digital content. India's regulatory response has begun to tackle these concerns, including in the recently amended Information Technology Rules, 2026, on synthetically generated information (MeitY, 2026).

In this paper, AI is thus not just a technological solution, but a system that, when applied, may have legal implications. The legal significance of AI is especially pertinent in contexts where its output has an impact on government decision-making, access to services, commercial arrangements, the handling of personal data, or the information context in which people exercise their rights.

Digital governance is a broad term for the application of digital technology and data within government to enhance public administration, policy making, service delivery and government-citizen relations. Digital-by-design government, a data-driven public sector, government as a platform, openness, and user-driven approaches and proactive service delivery are among the dimensions of digital government identified by the OECD (2021). A data-driven public sector values data as strategic resource in policy making, service delivery, organisational management and innovation and acknowledges the significance of integrity, openness and fairness in governance (van Ooijen et al., 2019).

Digital governance is not simply about converting paper-based government services to online services. It also involves the application of digital infrastructure, databases, platforms and data-analysis tools to develop and execute public policies, provide services and interact with citizens. Electronic government is being recognized in the Information Technology Act, 2000 under the provisions of electronic records, electronic signatures, and use of electronic records and electronic signatures by the government agencies (The Information Technology Act, 2000).

Data-driven administration is a part of today's digital governance. Data may be used for government institutions to detect patterns, evaluate needs, and create and inform decisions about public services. The OECD defines a data-driven public sector as one in which data is managed as a strategic asset, mechanisms are put in place to ensure its availability, access, sharing and reuse for better decision making and service delivery (OECD, 2021).

Digital governance also transforms the citizen-government communication. While digital platforms can enable more direct access to public services and more direct communication with the government, these platforms can also raise issues of accessibility, privacy, security, transparency and accountability. Therefore, technological efficiency is not sufficient to fully evaluate an effective digital governance. A robust and well-argued framework for digital governance needs to reflect the following questions: are digital systems working in line with the principles of fairness, accountability and protection of individual rights?

AI AND DIGITAL GOVERNANCE

The use of AI in digital governance is another development in the realm of data-centric governance. The importance of this connection is that in the future, AI could play a role in the decision-making process without it being the official decision-maker in law. An administrative authority may be legally liable for a decision based on an assessment, prediction or recommendation made by an AI system.A legally responsible administrative authority may use an AI system to make an assessment, prediction or recommendation, without losing its legal responsibility for the decision. This creates an important distinction between the technological assistance as well as legal responsibility.

The first question then is one of accountability: If an AI-assisted decision is responsible for harm or an incorrect outcome, then the question of responsibility is not solely about the technology itself. In the context of the relevant legal enquiry, the institution or person in charge of the deployment of the system, the way in which it was used, the quality of the data and the level of human control should be taken into account. The framework for Responsible AI by NITI Aayog acknowledges accountability as one of the guiding principles of responsible AI and discusses the responsibilities of various stakeholders associated with the AI systems (NITI Aayog, 2021).

The second concern is with accuracy and reliability. An AI system might generate a result that is technically feasible, but may not be suitable for the specific situation. In the Responsible AI framework by NITI Aayog, comprehending how an AI system works is related to safe and reliable deployment and they also state that an AI system could be dependent on spurious correlations in underlying data, resulting in large errors in deployment (NITI Aayog, 2021).

The third concern is explainability, as well as challenge of decisions. An AI system that is not easily understood can make it hard for impacted people to see why a specific result is being generated. The “black box” issue with certain deep-learning models, and its association with issues of trust, auditing, liability, maintenance and compliance with sector-specific requirements is identified by NITI Aayog (NITI Aayog 2021).

The fourth issue is regarding the personal data. AI systems could rely on large amounts of data, and if this data is digital personal data, then processing of this data becomes applicable to the data-protection framework in India. The Digital Personal Data Protection Act, 2023 explicitly aims to regulate processing of digital personal data, while affirming the interest of the individual in the protection of personal data and the need to process personal data for lawful purposes (Digital Personal Data Protection Act, 2023).

The use of AI in digital governance in turn raises a series of legal issues on responsibility, accuracy, transparency, contestability and data protection. The responses to these questions are important when AI is utilized where individuals' rights or entitlements, opportunities, or access to services are impacted.

RESPONSIBLE INNOVATION AND INDUSTRY 5.0

AI governance can be addressed with the appropriate normative approach of responsible innovation. Responsible innovation aims to consider the impact of technology development not only with regard to efficiency and economic gains, but also to broader implications for persons and society. According to NITI Aayog's Responsible AI, the governance of AI in India must be innovative, yet include governance of potential risks and be rooted in India's legal and regulatory environment (NITI Aayog, 2021).

The shift to the Industry 5.0 paradigm drives this human-centred approach to further. According to the European Commission (2021), Industry 5.0 can be characterized as three key pillars: human-centricity, sustainability and resilience, and going beyond the focus on efficiency and productivity as its only goals.

This is a knowledge that directly relates to the theme of the present conference. Industry 5.0, as stated in the conference brochure, is a transition to human-centric, sustainable and resilient industrial systems, and includes areas such as AI, Digital Transformation, Data-driven decision-making and Responsible Innovation among its subjects of inquiry. Data privacy, digital governance and legal aspects of AI and emerging technologies are explicitly featured in its Law, Governance, Public Policy and Responsible Innovation sub-theme.

In essence, good governance of AI should not be seen as a barrier to innovation. Instead, the right protection measures can help to foster trustworthy technological development and set expectations for transparency, accountability, privacy, safety and non-discrimination. According to NITI Aayog's Responsible AI framework, there are seven principles: safety and reliability; equality; inclusivity and non-discrimination; privacy and security; transparency; accountability; and protection and reinforcement of positive human values (NITI Aayog, 2021).

The conceptual link between AI, digital governance and responsible innovation can then be summarized as follows: AI offers technological tools; digital governance offers institutional and administrative environment; responsible

innovation offers a normativity framework for the deployment of digital tools in a way that is attentive to human welfare, rights and accountability. The relationship is the conceptual point of departure to look at the changing legal framework in India in the next section.

In 2018, the National Strategy for Artificial Intelligence (AI) was released by NITI Aayog, laying a strong institutional basis for India's policy dialogue with Artificial Intelligence. The policy was focused on the vision of "AI for All" and explored the possibilities of how AI can be used in areas such as health care, agriculture, education, smart cities and smart mobility and transportation (NITI Aayog, 2018).

But most importantly, the National Strategy for AI is a policy strategy, and not a statute on AI. It highlights challenges in the implementation of AI and separately addresses issues of ethics, privacy, security and Artificial Intelligence, acknowledging the need to consider legal and ethical issues along with the development of technology (NITI Aayog, 2018).

This strategy is thus relevant to this research as it is an early statement of India's stance on the development of AI, acknowledging the relevance of risks as well as opportunities.

THE RESPONSIBLE AI FRAMEWORK OF NITI AAYOG AND ITS IMPORTANCE FOR INDIA'S AI ROADMAP

Later, NITI Aayog formulated its Towards Responsible AI for All approach. The first part (2021) aimed to set out general ethical guidelines for designing, developing and using AI in India, and explicitly included these principles within the Indian legal and regulatory context (NITI Aayog, 2021).

The seven principles of Responsible AI outlined in the framework are: Safety and reliability; Equality; Inclusivity and non-discrimination; Privacy and security; Transparency; Accountability; and Protection and reinforcement of positive human values (NITI Aayog, 2021).

NITI Aayog's efforts have further underscored the need for a context-dependent, calibrated approach to AI risks and the absence of a blanket regulatory response to all AI uses. (NITI Aayog, 2021)

The principles are especially relevant to digital governance since the use of AI by government can entangle decisions that impact citizens and their personal data and access to public goods and services. The Responsible AI framework thus serves as an invaluable policy yardstick to assess the legal sufficiency of India's developing AI governance framework.

INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act, 2000 is still a key element of the Indian statute book for information technology and e-governance. The long title of the Act is, 'The Information Technology Act, 2000, for the legal recognition of transactions through electronic data interchange and other electronic communications, and for facilitating the filing of documents with government agencies'.

The Act has provisions on electronic governance, electronic signature, attribution and acknowledgement of electronic records, penalties and compensation, offences and intermediary liability, etc. (The Information Technology Act, 2000).

A key legal inquiry with respect to AI is not just whether the Information Technology Act "regulates AI." The issue, instead, is how much the current technology neutral statutory framework can address harms or legal issues from using AI. Some activities may already be covered by the existing law, additional regulation or even new policy creation may be necessary for some questions specific to AI. This is crucial, as it prevents the misrepresentation of the IT Act as being a blanket AI law, or as irrelevant to AI governance.

THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 (DPDP ACT, 2023)

The Digital Personal Data Protection Act, 2023 (DPDP Act) is of significant importance in the context of AI systems handling digital personal data. The main aim of the Act on the processing of digital personal data is to ensure that digital processing be carried out in a way that respects individuals' right to protect their personal data while also enabling the lawful processing of personal data (Digital Personal Data Protection Act, 2023).

The Act introduces a framework between Data Principals and Data Fiduciaries, along with the responsibilities and rights regarding the processing of digital personal data (Digital Personal Data Protection Act, 2023).

Its importance to AI is that AI systems can access personal data at various points in their development and/or deployment process. But it is not always the case that a personal data is always a part of an AI system. The analysis of the law should therefore be based on the fact of processing of digital personal data in the scope of the Act in the case of the particular AI application.

As a result, the DPDP Act plays a significant role in the legal landscape in which issues related to privacy, data governance, and responsible AI use can be explored in India.

RULES, IT AND GENERATED INFORMATION

One of the recent developments is the amendment

of Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 in February, 2026. The Rules have been updated by incorporating amendments relating to Synthetically Generated Information (SGI) and the Gazette notification dated 10 February 2026 has been issued along with the updated FAQs and subsequent corrigenda (MeitY, 2026).

This is a crucial development to showcase India's digital regulatory ecosystem adapting to technological advances like AI-generated and AI-altered content for 2026. The development is especially significant for the way digital platforms are regulated and the duties of synthetic content.

The development in this paper should thus be considered as a signpost of the gradual evolution of an issue-driven regulatory approach to AI-related risks under the existing digital legal framework rather than a signpost of a comprehensive India-specific AI law. This is significant to the accurate evaluation of India's emerging AI governance framework.

The National Strategy for AI, the Responsible AI framework, the Information Technology Act, the Digital Personal Data Protection Act and the ongoing IT Rules elaborate that India's AI governance framework is evolving in the multiplicity of legal and policy tools instead of a single comprehensive AI statute. This raises the question: If there are constitutional principles and judicial review to consider, are these instruments adequate to respond to the particular legal challenges that arise from AI-enabled digital governance?

CONSTITUTIONAL AND FUNDAMENTAL RIGHTS DIMENSIONS OF AI GOVERNANCE

Artificial Intelligence (AI) has come into direct constitutional relevance if it is used in a manner that impacts upon privacy, equality, freedom of expression, dignity or the fairness of governmental decision making. While there is no dedicated article on AI in the Constitution of India, the principles laid down in Article 14, 19, and 21 are key to assess AI-enabled governance. The problem, then, is not the legality of the use of AI, but is the use of AI consistent with constitutional rights, legality, fairness and accountability.

Right to Privacy under Article 21

The Supreme Court's landmark decision in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) is the constitutional basis for AI privacy. In Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017, a nine judge Bench of the Supreme Court unanimously declared that privacy is a fundamental right guaranteed by the Constitution and is interlinked with liberty, dignity and autonomy of the individual. The ruling is of particular importance in the context of AI governance, as modern AI systems are capable of analyzing vast amounts of data and drawing patterns or inferences about humans.

The processing of data based on artificial intelligence can include profiling, prediction, automated analysis and the aggregation of data from various sources. This processing may impact individuals' informational privacy without their knowledge, even if the original information is seemingly mundane. The constitutional concern then is not just related to whether information has been collected, but also how it is processed and used after it is collected (Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017).

This becomes a major concern with regard to the use of surveillance and facial-recognition technologies powered by Artificial Intelligence. The technologies could make it possible for public bodies to recognize or analyze a person on a scale that might be hard to do otherwise. But, it is not technically correct to say that the Supreme Court explicitly banned AI-driven surveillance or facial recognition. Instead, its constitutional principles are the ones which must be used as a framework for assessing intrusive action by the State in relation to personal information.

Supreme Court's Privacy Judgements clearly tell us that privacy is not absolute. There is an interference with privacy that needs to be based on an appropriate legal ground and meet constitutional requirements, such as legitimate State objectives and proportionality, as was set out by Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017. The administrative efficiency or technological capacity, therefore, is not enough to justify unlimited intrusions of data processing by the use of AI.

The DPDP Act 2023 also provides for a statutory framework for the processing of digital personal data and imposes obligations on Data Fiduciaries and rights on Data Principals (Digital Personal Data Protection Act 2023). Therefore, the constitutional protection of privacy, along with the statutory one in relation to digital personal data, needs to be taken into account whenever formulating the rules of the governance of AI in India.

EQUALITY AND NON-DISCRIMINATION

Article 14 provides for equality before the law and equal protection of the law. Its significance for AI is the potential for patterns to be recreated or reinforced in historical or operational data, which can be used to inform automated systems. AI decision-making could trigger constitutional issues in cases of unfair differential treatment, particularly when patterns result in this.

The Supreme Court has understood Article 14 to include protection against arbitrary action by the

State. In the case of E.P. Royappa v. State of Tamil Nadu (1974), the Court has associated equality with the rejection of arbitrariness (E.P. Royappa v. State of Tamil Nadu, 1974) The principle was further expanded in Maneka Gandhi v. Union of India (1978) where the Court reiterated the need for fairness and reasonableness with regard to the State action (Maneka Gandhi v. Union of India, 1978).

These principles are applicable to the algorithmic decision-making because the algorithm can produce systematic differences in the outcomes for different people, if it was trained on incomplete, inaccurate or historically biased data. However, there is a crucial point to remember: algorithmic bias is not ipso facto a violation of the principle of equality under the law, as guaranteed by Article 14 of the Constitution. A difference in outcomes or statistical differences are not sufficient evidence of unconstitutional discrimination.

The constitutional issue would be based upon the facts of the specific decision, such as the type of classification, the governmental purpose, the significance of the criteria used and whether the action taken is arbitrary or otherwise unconstitutional. However, if an AI system is used by a public body to create an unjustified differential treatment, the use of an AI system does not mean that the public body can escape constitutional scrutiny just because the product of the machine is technology-driven.

Equality, inclusivity and non-discrimination are values of responsible AI explicitly mentioned in the Responsible AI framework by NITI Aayog, highlighting the need to consider the discriminatory risks of AI deployment (NITI Aayog, 2021).

FREEDOM OF SPEECH AND EXPRESSION

The usage of AI's content, synthetic media and deepfakes, has posed new challenges with respect to Article 19(1)(a). While AI can assist in the creation of authentic and creative expression and communication, it can also be misused to produce deceptive or manipulated content.

The Supreme Court's judgement in Shreya Singhal vs Union of India (2015) is important when it comes to restriction on online speech. In Shreya Singhal v. Union of India, 2015, the Court invalidated Section 66A of the Information Technology Act, 2000, on the grounds that it infringed upon Article 19(1)(a) of the Constitution, and reviewed what the Constitution required in terms of restrictions on speech under Article 19(2). With the rise of deepfakes, there is thus a balancing act. One is the protection of individuals and society from harmful or deceptive artificial substance, and the other is the constitutional protection of legitimate expression. The regulatory answer should therefore be confined to the bounds of Article 19(2) and not make AI-generated content automatically illegal.

This is a matter which has been recently addressed by the regulatory regime in India. In February 2026, the Information Technology Rules were amended and it was identified that provisions related to Synthetically Generated Information (SGI) (Ministry of Electronics and Information Technology [MeitY], 2026) were included in the Rules. This is an effort to overcome the new risks of synthetic content in the current digital legislation, not a new comprehensive AI law.

The Supreme Court has confirmed that there are two elements to natural justice: the first is the rule of law and the second is administrative accountability.

With the introduction of AI into governmental decision-making processes, a basic administrative-law issue arises: How can one challenge a decision if the decision maker uses an AI system and the reasoning it produces is not easily understood?

Natural justice requires the fairness in the administrative decision-making. In State of Orissa v. Dr. (Miss) Binapani Dei (1967) the Supreme Court has held that an administrative decision that has civil consequences must be based on the principles of natural justice. Likewise, Maneka Gandhi also reiterated the issue of fair procedure in State action (Maneka Gandhi v. Union of India, 1978).

The principles come into their own when an AI system has a significant impact on a governmental decision. In cases where an individual is denied a benefit, where an adverse administrative determination is made, or other action taken, as a result of an automated recommendation, meaningful review may require information about the basis for the action.

Reasons too are required. The Supreme Court has also emphasized the need to record reasons in administrative and quasi-judicial decisions as it aids in judicial review and ensures that the mind is applied (S.N. Mukherjee v. Union of India, 1990). So, an authority should not just say that the Artificial intelligence system gave a specific result. It is not an excuse for the authority who makes the decision to have technological assistance.

AI opacity can therefore pose challenges for natural justice, especially when people impacted by the outcome cannot pinpoint the reasons behind a negative outcome. This doesn't have to necessarily require the full technical specification of an AI system to be published at all times. Instead, the person should, if required under the law, be given adequate information about the decision so that they can make a valid objection.

KEY LEGAL CHALLENGES IN AI-DRIVEN DIGITAL GOVERNANCE5.1 PRIVACY AND DATA PROTECTION

Privacy is one of the key issues as AI systems typically need a large amount of data to train, analyze, or run. There are threats both related to over-collection, re-use, profiling, insecure storage and the drawing of new inferences from the information.

While the constitutional rights enshrined in Puttaswamy and the legal framework laid out in the Digital Personal Data Protection Act, 2023 are key protections, they are still relevant to increasingly complex AI systems. The question that arises is whether data processing is legal, proportionate and has sufficient safeguards.

Algorithmic Transparency and Explainability

AI systems can generate a blackbox problem that is challenging to explain why a specific answer is generated. Among the core principles of NITI Aayog's Responsible AI approach, transparency is listed, and it acknowledges that the lack of clarity regarding the process of AI decision making can pose issues around trust, auditing and liability, and compliance (NITI Aayog, 2021).

Explainability becomes crucial when AI plays a role in significant decisions. Those who would be impacted by an important governmental decision shouldn't find themselves in a situation where the only reason is that “the algorithm decided.” Transparency should, therefore, be in line with the possible influence of the AI system.

Discrimination and bias can occur in algorithms. Algorithms can be biased and discriminatory. The data/algorithmic outcomes relationship can be described as:

Inequality in data: biased model/output: potentially unequal outcome. This does not imply that all the biased outputs are the illegal discrimination. When, however, AI is used by the public authorities, there is a risk that its use could result in discriminatory or arbitrary outcomes, which will lead to a constitutional check under Article 14.

Good AI governance should then entail proper testing, monitoring and evaluation of systems that are applied for high impact decisions. Equality should continue to be a substantive governance goal, and not only a technical issue.

The ability to take responsibility and assign responsibility. AI systems typically have many stakeholders such as developers, vendors, deployers, government departments and humans making decisions. If an AI-assisted decision results in harm, finding the legally accountable party may also thus become more complex.Identifying the legally responsible party may therefore become more difficult if an AI-assisted decision causes harm.

India doesn't have a general principle that puts AI on par with humans as an autonomous legal entity for harm. Responsibility, therefore, should, in the normal course of events, be looked back through existing legal obligations, statutory provisions and institutional ties.

The legal responsibility for the use of AI in governmental decision-making cannot be delegated to the AI system. The exercise of statutory powers must be held to account by human decision makers. In this context, accountability is one of the principles of Responsive AI identified by NITI Aayog (NITI Aayog, 2021).

Cybersecurity

AI systems rely on digital infrastructure, which raises cybersecurity issues related to data security, system integrity, and potential cyber incidents. The Indian cybersecurity framework has conferred statutory roles on Indian Computer Emergency Response Team (CERT-In) under Section 70B of the Information Technology Act, 2000.

The requirements laid out in Section 70B under CERT-In's directions, cover information-security practices, prevention of cyber incidents, response and reporting of cyber incidents (Indian Computer Emergency Response Team [CERT-In], 2022). Securing AI is relevant to this framework as securing AI is interdependent with securing the broader digital infrastructure that AI relies on.

AI-Generated Content & Deepfakes

Synthetic audio-visual content is a particularly visible governance challenge as it can be used to artificially create content that misrepresents a person or an event. The risk this poses can encompass manipulation of the digital information environment, privacy breaches, reputational damage and deception.

This has led to the amendments to the IT Rules, 2026, on Synthetically Generated Information, which is a modern measure by the Government of India in this context (MeitY, 2026). The difficult task is to set up effective protection without overstepping Article 19(1)(a) of the ECHR, which guarantees the right to freedom of expression for all.

ARTIFICIAL INTELLIGENCE, DIGITAL BUSINESS AND RESPONSIBLE INNOVATION

AI governance also applies to companies, digital platforms and technology companies. Many commercial interactions with customers are handled with AI, as well as recommendations, fraud detection, data analysis, content creation, etc. Therefore, consumer protection, competition and

IP issues must be taken into account, in addition to technological development, when ensuring responsible innovation.

The CCI has published the Market Study on Artificial Intelligence and Competition in 2025, which analyzed how AI and competition are interlinked and the problems that are emerging from the changes in the AI ecosystem (Competition Commission of India [CCI], 2025). This shows that AI governance is not limited to privacy and cybersecurity but is creeping into competition policymaking in India.

AI also brings up intellectual property issues such as training data, AI-generated works, and the application of AI in the innovation process. These questions must be answered based on current intellectual-property law, as opposed to speculation about ownership of AI-generated works.

TOWARDS A RIGHTS-BASED AND RESPONSIBLE AI GOVERNANCE FRAMEWORK FOR INDIA

India's governance framework for AI must be rights-based and risk-sensitive, and not presume a uniform level of legal risk in all AI applications. NITI Aayog's Responsible AI guidelines enable a calibrated approach that is mindful of the risks of specific applications (NITI Aayog, 2021).

First, there should be a primacy of human oversight in high-stakes decision-making involving individual rights and substantial interests where AI is used. While AI could help human decision-makers, so too must the technology itself not remove legal responsibility. Second, there should be a proportionality between transparency and explainability and the risk. Those who have been the subject of important decisions made with the help of AI should be provided with relevant information around the basis of the decision and the opportunity to review it appropriately.

Third, privacy and data protection must be integrated into the design and use of AI systems that deal with personal data. This is in line with the constitutional importance of privacy as enshrined in Puttaswamy and the data protection laws in India. Fourthly, the accountability and grievance redressal must be made clear. People impacted should be able to identify mechanisms that will allow them to contest incorrect or illegal AI-driven decisions, and institutions should make sure that there is a clear accountability structure for the systems they use.

Last but not least, India needs to explore AI governance for sectors as the risks of AI vary from the healthcare field to finance, education, law enforcement, and public administration to digital platforms. General principles and sector-specific safeguards may thus allow for more flexibility than trying to establish a uniform regime across all AI applications.

A rights-based AI governance framework would consequently seek to achieve a balance between innovation and constitutional protection. This is in line with the Human Centric approach of Industry 5.0, under which technological development should be a driver of sustainable, resilient and human-centred development (European Commission, 2021). The aim is not to suppress technological innovation, but to make sure technological innovation is compatible with principles of privacy, equality, dignity, freedom, fairness and institutional accountability.

CONCLUSION

Artificial Intelligence is becoming more and more a part of digital governance, presenting several opportunities to enhance public service delivery, efficient administration, innovation, and decision-making based on data. With its increasing use, however, it is also arousing complex legal issues around privacy, data protection, algorithmic transparency, discrimination, cybersecurity and synthetic content and institutional accountability. The analysis shows that India's current system, consisting of constitutional principles, the Information Technology Act, 2000, Digital Personal Data Protection Act, 2023, the amended Information Technology Rules, judicial interpretation and policy parameters of NITI Aayog provides valuable building blocks for tackling these concerns but does not represent an integrated framework of AI governance.

Hence, the governance of AI in India should be firmly rooted in constitutional values such as privacy, equality, dignity, freedom of speech and procedural fairness. Where AI systems have an impact on critical decisions that impact individuals, human oversight, proportional transparency, meaningful grievance redressal, responsible data practices and clearly assigned institutional accountability are essential. A risk-sensitive and sector-specific approach can allow for different degrees of harm, but not also limit technological innovation.

In conclusion, the challenge of responsible AI governance is not about stifling innovation, but about ensuring trusted and sustainable technological progress. Understanding the concept of AI governance and its potential to intersect with the tenets of Industry 5.0 in a way that prioritizes human values can help India continue its technological advancement without losing sight of the rights, accountability, and trust of the general public.

REFERENCES

1. European Commission. (2021). Industry 5.0: Towards a sustainable, human-centric and resilient European industry. Publications Office of the European Union.
2. Ministry of Electronics and Information Technology. (2026). Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026. Government of India.
3. NITI Aayog. (2018). National strategy for artificial intelligence. Government of India.
4. NITI Aayog. (2020). Towards responsible AI for all: Part 1—Principles for responsible AI. Government of India.
5. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
6. The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
7. The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
8. Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India) India Code. India Code - Digital Personal Data Protection Act, 2023
9. European Commission. (2021). Industry 5.0: Towards a sustainable, human-centric and resilient European industry. Directorate-General for Research and Innovation. European Commission - Industry 5.0
10. Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, (India). India Code. India Code - Information Technology Act, 2000
11. Ministry of Electronics and Information Technology. (2026). Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021: Updated on 10th February 2026 Government of India. MeitY - IT Rules, 2021 and 2026 amendments
12. NITI Aayog. (2018). National strategy on Artificial Intelligence: #AIForAll. Government of India. NITI Aayog - National Strategy for Artificial Intelligence
13. NITI Aayog. (2021a). Towards responsible AI for all: Part 1- Principles for responsible AI. Government of India. NITI Aayog - Principles for Responsible AI
14. NITI Aayog. (2021b). Towards responsible AI for all: Part 2- Operationalizing principles for responsible AI. Government of India. NITI Aayog - Operationalising Responsible AI
15. OECD. (2021). Government at a glance 2021: Digital government index- Methodology and definitions. OECD Publishing. OECD - Digital Government Index
16. van Ooijen, C., Ubaldi, B., & Welby, B. (2019). A data-driven public sector: Enabling the strategic use of data for productive, inclusive and trustworthy governance (OECD Working Papers on Public Governance No. 33). OECD Publishing. https://doi.org/10.1787/09ab162c-en
17. Competition Commission of India. (2025). Market study on artificial intelligence and competition. Government of India.
18. Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament, 2023 (India).
19. European Commission. (2021). Industry 5.0: Towards a sustainable, human-centric and resilient European industry. Directorate-General for Research and Innovation.
20. Indian Computer Emergency Response Team. (2022). Directions under sub-section (6) of Section 70B of the Information Technology Act, 2000. Ministry of Electronics and Information Technology, Government of India.
21. Information Technology Act, 2000, No. 21 of 2000, Acts of Parliament, 2000 (India).
22. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
23. Maneka Gandhi v. Union of India, (1978) 1 SCC 248 (India).
24. Ministry of Electronics and Information Technology. (2026). Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021: Amendments relating to synthetically generated information. Government of India.
25. NITI Aayog. (2021). Responsible AI for all: Approach document for India. Government of India.
26. Office of the Controller General of Patents, Designs and Trade Marks. (2026). Guidelines for the use of artificial intelligence in patent examination procedures. Intellectual Property India, Government of India.
27. E.P. Royappa v. State of Tamil Nadu, (1974) 4 SCC 3 (India).
28. Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).
29. S.N. Mukherjee v. Union of India, (1990) 4 SCC 594 (India).
30. State of Orissa v. Dr. (Miss) Binapani Dei, (1967) 2 SCR 625 (India).
31.