

Artificial Intelligence at the Crossroads of Law: Reimagining Intellectual Property, Data Privacy, and Cyber Governance in India

PRATISTHA PRIYADARSHI¹, (PRATISTHAPRIYADARSHI.1311@GMAIL.COM)¹

ARUNAV², (ARUNAV.SINGH757@GMAIL.COM)²

AKANKSHA KUMARI³, (AKANKSHA11JHA@GMAIL.COM)³

SHANTANU SHRESHTHA⁴, (SHRESHTHAKAUNDILYA@GMAIL.COM)⁴

RAUSHAN KUMAR⁵, (RAUSHAN.KUMAR020301@GMAIL.COM)⁵

^{1,2,4}L.L.M. , NATIONAL UNIVERSITY OF STUDY AND RESEARCH IN LAW, RANCHI.

³L.L.M. INDIAN LAW INSTITUTE, DELHI.

⁵ADVOCATE, NATIONAL UNIVERSITY OF STUDY AND RESEARCH IN LAW , RANCHI

Abstract

AI is changing how knowledge is created, how personal data is used, and the nature of digital threats, and these changes in India are happening within a legal framework that predates the machine learning boom. We systematically review the law and its application to AI in India in three inter-connected sectors: intellectual property, data protection and information technology (cyber law). We employ a structured narrative review methodology by reviewing the indexed peer-reviewed literature in Scopus and Web of Science, statutes, subordinate legislation, case law and policy documents until September 2026. Indian IP law continues to envision a human author/inventor as a requisite for protection, as demonstrated by the Indian Patent Office's rejection of DABUS in 2026. Training AI on copyrighted materials remains legally uncertain in India. The interim order in ANI v. OpenAI and the DPIIT's discussion paper on a hybrid licensing regime are favorable trends. The Digital Personal Data Protection Act, 2023 and its 2025 Rules have laid down a consent-driven framework for data privacy, but the law is unclear on public-facing data, state exemptions, and automated decision-making. In cyber governance, the 2026 amendment to the intermediary rules was India's first binding regulation for synthetic media. AI-specific cyber security risks remain governed by general provisions. The review finds that the three domains are interrelated throughout the lifecycle, and regulation across the domains should therefore be aligned. The review concludes with a research agenda, including training-data governance, public sector automated decisions, institutional capacity and international interoperability.

Keywords: Artificial intelligence; Intellectual property rights; Data protection; Digital Personal Data Protection Act; Cyber governance; Deepfakes; India.

1. Introduction

AI has left the research laboratory and has been deployed in everyday applications for generating text, images, code and predictions, driving decisions in finance, healthcare, education and public administration. Such capabilities are economically attractive and at the same time rattling to existing legal frameworks relying on human actors. This has led to legal questions that include the question of ownership of the output from machines, using personal data to train decision-making algorithms, and how the state should respond to AI-inflicted harm [1].

India offers a unique country lens for exploring these questions. It has one of the largest numbers of digital users worldwide and in its National Strategy for Artificial Intelligence [2], has articulated a vision of utilizing AI for inclusive growth. Conceptually, the early literature acknowledged that, while AI could help India plug gaps in provision of public services, it could also worsen social inequalities if the data infrastructure and accountability frameworks were not established in tandem with the technology [3]. The legal architecture has been piecemeal. Intellectual property regulations, data protection legislation and cybersecurity have their own regulations, which are enforced by different organizations.

The Parliament passed the Digital Personal Data Protection Act, 2023 (DPDP Act); the Rules with which it has to be implemented were issued in November 2025 [4,5]. The month also saw the Ministry of Electronics and Information Technology (MeitY) issue the India AI Governance Guidelines. They preferred principle-based regulation to a separate law for AI. The intermediary rules were amended in February 2026, bringing synthetically generated content under platform due diligence obligations [6]. Other notable events include a historic rejection of a DABUS patent application and the first litigation regarding the training of generative AI in ANI v. OpenAI [7,8].

Additionally, existing discussions of these domains have tended to focus on the topics in isolation, looking at AI and copyright mainly through the lens of authorship and originality concepts [9,10], and privacy through the lens of consent and automated decision making [11,12]. Cybersecurity research also focuses more on technical defences [13]. Less attention has been placed on how these areas relate to each other within a single national legal system. This matters in practice because a single AI model can simultaneously generate copyright, privacy and security concerns.

This review seeks to fill this gap by examining Indian law on all three of these areas in an integrated fashion. This paper has three objectives. The Project has two main objectives. The first, is to map the law and policy landscape on AI in regards to IPR, data privacy and cyber governance in India. The second, is to compare India's approaches with those of other major jurisdictions, to identify divergences, if any. The third is to point out areas of convergence and outline a research and policy agenda. The text seeks to provide a consolidated account of the rapidly changing field to legal scholars and policymakers/practitioners.

2. REVIEW METHODOLOGY

2.1 Sources and search strategy

A narrative literature review is an appropriate method for law-related research, where original sources (statutes, cases) are as important as scholarly commentary. For peer-reviewed research, Scopus, Web of Science and Google Scholar databases were queried using the search terms "artificial intelligence", "machine learning", "generative AI", "copyright", "patent", "inventorship", "data protection", "privacy", "cybersecurity", "deepfake", "India". The reference lists of the key articles were also searched for other relevant work.

The primary legal materials referenced were the Gazette of India, the websites of the Ministry of Electronics and Information Technology (MeitY), the Department for Promotion of Industry and Internal Trade (DPIIT) and the Office of the Controller General of Patents, Designs and Trade Marks and reported Indian and foreign judicial decisions. For the review period up to September 2026, material already available was referenced to understand the implementation of the DPDP Rules and the latest judicial developments.

2.2 Selection criteria and analysis

These articles were published in Scopus- or Web of Science-indexed journals, or were published in conference proceedings indexed in those databases, and they covered one of the three types of law in relation to AI. However, articles that did not contain analysis of the relevant law and governance were excluded. Technical studies that explain AI-controlled cyber threats have been exceptions to this rule, as the work is fundamental to understanding the regulatory issue. Material directly relevant to India, or material that collects comparative studies of these kinds of questions that Indian law has now to deal with. Table 1 summarizes the source base by theme and source type.

Table 1. Distribution of the sources reviewed, by legal domain and source type.

Legal domain	Peer-reviewed sources	Primary legal and policy sources	Total
Intellectual property rights	8	2	10
Data privacy	6	2	8
Cyber governance	2	1	3
AI policy and cross-cutting governance	4	0	4
Total	20	5	25

Note: peer reviewed sources are articles published in indexed journals, primary sources are statutes, subordinate legislation, judicial decisions and policy documents. Each is counted once in its main category.

The thematic analysis used coding of the sources in relation to the legal domain they discussed; the stage of the AI lifecycle they considered; and the regulatory solution being proposed. The structure of these codes made it easier to identify domain-specific issues, as well as points of overlap between domains.

3. EVOLUTION OF INDIA'S LEGAL AND POLICY LANDSCAPE FOR AI

The Indian legal framework does not have a single thorough or overarching law governing AI. Instead, it uses an abundance of existing general laws, sectoral regulations and non-binding policy instruments. The Information Technology Act, 2000 (IT Act) is the primary law that governs electronic records, intermediary liability and cyber crimes. The Copyright Act, 1957 and the Patents Act, 1970 govern the protection of intellectual property. The processing of personal data is based on the right to privacy guaranteed by the constitution. The most important laws and policies in these three domains are represented in Fig. 1.

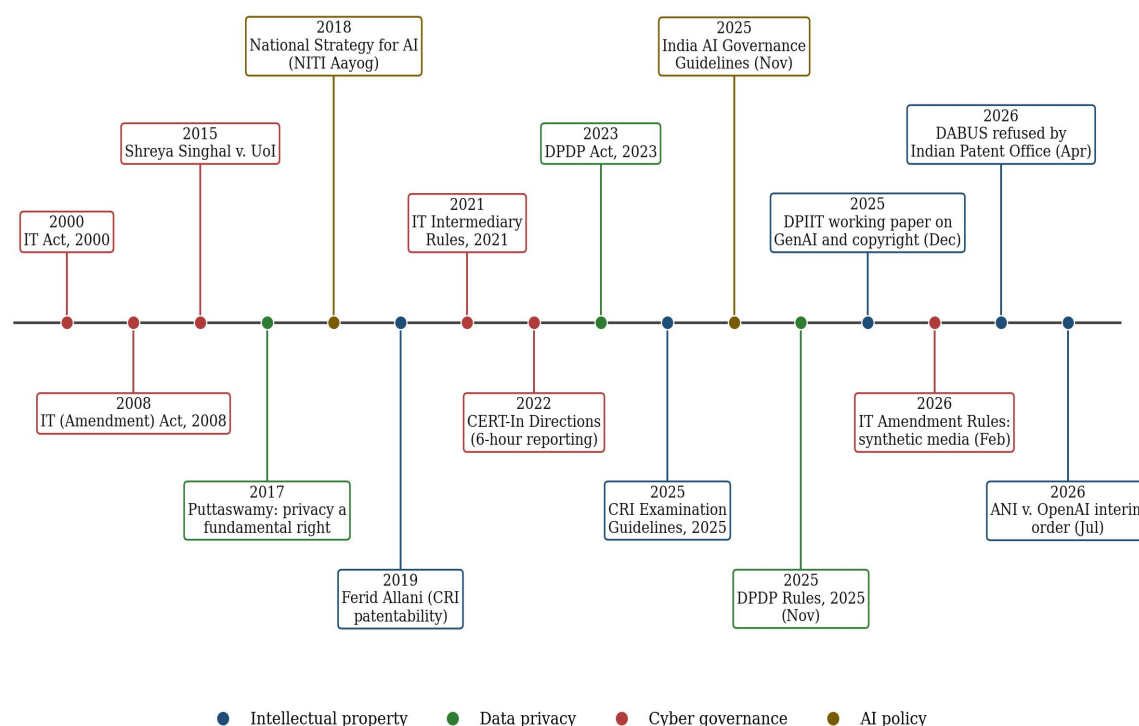


Fig. 1. Key legal and policy developments for Artificial Intelligence in India (2000-2026) according to area of work are displayed below. Source: Prepared by the authors from the primary instruments and decisions cited in this review.

The first governmental policy attention to artificial intelligence was in 2018 with the National Strategy for Artificial Intelligence, which framed it as a tool for bringing social and economic inclusion under the motto "AI for All". Though it focuses on development, it has been critiqued for its silence on accountability and rights or redress [2]. Marda has argued that in India, data-driven decision-making must also confront the limits of the underlying datasets, to account for missing or biased data on marginalized groups [3].

These issues were addressed with the constitutional right to privacy recognized in 2017, when a nine-judge bench of the Supreme Court held in Puttaswamy that the right to privacy is a fundamental right under Article 21, but that the interference must meet the tests of legality, legitimate aim and proportionality. The verdict legislatively triggered the introduction and withdrawal of several draft bills on data protection, until the passing of the DPDP Act by Parliament in 2023 [14].

Unlike the legally binding duties enshrined in the European Union's (EU) Artificial Intelligence Act, which classifies AI systems by risk and applies obligations across the value chain to their providers and deployers, the consensus appears to be moving towards more flexible, principle-based regulation such as in the India AI Governance Guidelines (November 2025), which set cross-sector principles. Smuha describes the current state of the world as a shift from a race to develop AI to a race to regulate AI, in which every jurisdiction races to set the rules that others will adopt. Reflecting a desire not to stifle innovation, India's approach is to build on existing laws by amending them to tackle specific harms.

4. AI AND INTELLECTUAL PROPERTY RIGHTS

4.1. Authorship and originality of AI-generated works

The Copyright law of India, similar to most countries, recognizes the author as a human being. Section 2(d)(vi) of the Copyright Act, 1957 provides that the author of a computer-generated work is the

person who causes the work to be created. This provision was written to protect works by a human programmer and not systems that create complex output from a simple prompt, so its unambiguous application to generative AI is unclear. [15]

The originality threshold has since been made stricter. In *Eastern Book Company v. D.B. Modak*, the Supreme Court required a minimum level of creativity along with skill and judgment. Applying this standard to AI output can lead to challenges. For instance, the model might be generating an image or text, and the human creator might only have provided a prompt to the model. According to Ginsburg, and Budiardjo, authorship requires both conception and reduction to practice by a human; since what a machine generates is determined by the machine, it is not copyrightable [9]. Gervais agrees, noting that originality presupposes the author's choice of expression [10].

Others see more scope for protection. Guadamuz has argued that the United Kingdom and some Commonwealth systems already guarantee authorship to the person making the necessary arrangements for computer-generated works to be made, so it would not be impossible to extend this to other jurisdictions [16]. Whether Indian law will adopt this position is unclear but the Copyright Office has received an application seeking registration in which the tool and a human were listed as joint authors. Hema describes this as treating AI as a joint author [15] but the Copyright Office issued a notice to cancel the registration which leaves the position of copyright in the work unclear. Hema also discusses the implications of joint authorship for ownership and term of protection, and warns against denying copyright since it could reduce the incentive to invest in AI [15].

4.2 Inventorship and patentability

Patent law has faced the same problems. Abbott argued that computers were already inventing patentable inventions, and that naming the computer as inventor would promote innovation and avoid misleading patent literature [17]. Similar arguments have been used to register patents using DABUS as the inventor. Both the European Patent Office and the UK Intellectual Property Office have rejected comparable applications [18]. The US Patent and Trademark Office denied the application, while US and UK appeal courts in 2022 and 2023 determined that an inventor must be a natural person.

India had a similar conclusion and rejected the DABUS application on 15 April 2026 at the Indian Patent Office. The Office held that for the purposes of the Patents Act, 1970 [7], an AI cannot be the "true and first inventor" as the latter is defined under Sections 6 and 7 of the Act, which both assume a person who can hold and assign rights, without restricting patent protection to AI-assisted inventions with human inventors. Kim warns that much of this debate relies on assumptions of AI autonomy that do not match the reality of how these systems are engineered, in which human engineers determine what problems are solved, which data is captured, and how outputs are evaluated [18]. Table 2 compares the position on AI inventorship and authorship across several territories.

Table 2. Comparative position on AI inventorship and authorship in selected jurisdictions.

Jurisdiction	AI as inventor	Protection of AI-generated works	Key sources
India	Refused. The inventor must be a person capable of holding and assigning rights under Sections 6 and 7 of the Patents Act, 1970.	No express rule. Section 2(d)(vi) names the person who causes a computer-generated work to be created; originality requires human skill, judgment and minimal creativity.	[7,15]; <i>Eastern Book Co. v. D.B. Modak</i> (2008)
United States	Refused. The Patent Act requires the inventor to be a natural person.	Human authorship is required; output determined by the machine is not protected.	<i>Thaler v. Vidal</i> (2022); [9]
United Kingdom	Refused. An inventor under the Patents Act 1977 must be a natural person.	Statute allocates authorship of computer-generated works to the person making the necessary arrangements.	<i>Thaler v. Comptroller-General</i> (2023); [16]
European Patent Office	Refused. The European Patent Convention requires a human inventor to be designated.	Originality is tied to the author's own intellectual creation, which presupposes human choices.	[10,18]

Another debate is whether AI technology themselves may be patented. Section 3(k) of the Patent Act excludes mathematical techniques, business procedures, computer programs, and algorithms. The Delhi High Court declared in *Ferid Allani's* case that innovations with technical effects or contributions should not be denied just because they are implemented through software. The 2025 Guidelines for Examination of Computer Related innovations include guidelines on AI and machine learning innovations. They also need better disclosure of the underlying architecture and training methodologies, as they believe AI claims

may be too opaque to fulfil these criteria.

4.3 Training data, text and data mining, and fair dealing

The most pressing commercial issue of IPRs in AI is the data behind the training of the AI models. The models use large datasets of text, images, and audio that are often protected by copyright. Lemley and Casey have argued that to the extent the works are used in a way that trains for unprotectible features (such as facts, data or patterns), use is likely permitted under fair use in the US law [19]. However, as Samuelson notes, litigation against generative AI companies is moving rapidly, and may reveal ultimately how much expression is treated as protected. [20]

Indian Copyright Law does not contain any exception on text and data mining. Section 52 of the Copyright Act of 1957 provides the circumstances under which exceptions to copyright can be made under the fair dealing exception, such as private use, research or study, criticism or review, or reporting current events. The legality of whether the training of AI is covered under fair dealing was first tested when news agency ANI filed a suit against OpenAI in the Delhi High Court. In a *prima facie* interim ruling on 24 July 2026, the High Court ruled against granting an injunction against OpenAI, owing to the possibility that training a language model to read and understand news articles could fall within the fair dealing exception [8]. The Court found the outputs to more likely be the product of retrieval-augmented generation rather than the memorized training data, and not substantially similar to ANI's reports, but these conclusions were tentative, and the case continued toward trial.

The executive's proposal took a different form: in December 2025, a committee at DPIIT released a working paper proposing a hybrid framework. This model would allow developers to obtain a mandatory blanket licence allowing them to train AI systems on any legally-acquired copyright work, in exchange for a statutory remuneration to rights holders upon commercialisation of the trained system. Thus, this paper rejects the possibility of an open-ended exception, as well as a regime purely based on consent. Should this paper's proposal be adopted, it would be the first mechanism linking access to training data to a collective remuneration scheme, which has only been adopted in a handful of jurisdictions. The interplay of the developing jurisprudence and this proposal shall likely influence the future of Indian copyright policy concerning artificial intelligence.

5. AI AND DATA PRIVACY

5.1 Constitutional foundations and the limits of consent

The Puttaswamy judgment is the normative foundation for data protection in India. It recognized informational privacy as part of the right to life and personal liberty and discussed the dangers of aggregation in the digital economy. These dangers are particularly acute in the case of AI, which is dependent on large data sets, and may use seemingly innocuous information resources to infer sensitive attributes [12].

Scholars have long recognized that the notice-and-consent model is ineffective in these settings. Solove argues that people cannot meaningfully understand or evaluate downstream uses of their data, especially those that involve aggregation and inference [12]. AI further complicates matters as the processing purpose can evolve, especially when models are fine-tuned or repurposed. Veale, Binns and Edwards show that trained models can disclose personal information through model inversion and membership inference attacks. This result blurs the distinction between the data set and the model that was trained on it [21].

5.2 The DPDP Act and Rules across the AI lifecycle

The DPDP Act adopts a consentbased model. Processing is permissible in either case if the data principal provides free, specific, informed and unambiguous consent or if it falls within a closed list of legitimate uses [4]. Data fiduciaries must inform data principals, implement reasonable security measures, report on data breaches, and delete data once the purpose of its collection has been fulfilled. Significant data fiduciaries have additional obligations, such as data protection impact assessments and periodic audits [14,22].

The Rules notified in November 2025 come into force in a phased manner. The provisions for the Data Protection Board of India come into force the same day. However, those for the consent manager framework come into force after 12 months and the majority of substantive provisions after May 2027. The staggered rollout gives organisations time to adjust and means that AI systems already in use will remain covered by the previous IT Act framework for now. The Act's core features as they relate to the different stages of the AI lifecycle are shown in Table 3.

Table 3. Key provisions of the DPDP Act, 2023 mapped against the AI lifecycle.

AI lifecycle stage	Relevant provisions	Issues raised for AI systems
Data collection	Notice and consent (Sections 5 and 6); exclusion of publicly available personal data (Section 3(c)(ii)).	Large-scale scraping of public data may fall outside the Act; individual notice is impractical for web-scale datasets.
Training and processing	Consent tied to a specified purpose; closed list of legitimate uses (Section 7).	Reusing data to train or retrain models may exceed the purpose for which consent was given.
Storage and security	Reasonable security safeguards and breach intimation (Section 8(5) and 8(6)).	Trained models may leak personal data through model inversion or membership inference.
Deployment and decisions	Rights to information, correction and erasure (Sections 11 and 12); impact assessments and audits for significant data fiduciaries (Section 10).	No specific right against solely automated decisions; erasure of data already learned by a model is technically difficult.
Cross-border transfer	Transfers permitted unless restricted by notification (Section 16); additional duties for significant data fiduciaries under the Rules.	Uncertainty over future restrictions affects where models are trained and hosted.
Use by the State	Exemptions for notified instrumentalities of the State (Section 17).	Broad exemptions reduce safeguards for AI used in welfare, policing and surveillance.

There are three key features of the Act particularly relevant to AI. The first is publicly available data, as per section 3(c)(ii), which exempts personal data that the data principal has made public or that anyone else is legally required to publish [4]. This could allow developers to train models on data from public websites, without needing to obtain user consent. Commentators have said it offers wider latitude than the European model, under which public availability does not remove data from protection [14,23].

The second feature is the extent of the exemptions to the State. Section 17 allows for the exemption of an instrumentality of the central government from most obligations on grounds of sovereignty, security and public order [4]. Sonkar considers the exceptions and limited independence of the Data Protection Board to be especially problematic for AI, given the increasing use of automated systems in welfare, policing and surveillance [23] [3].

Third, there is no express right to object to a decision based solely on automated processing, and there is no express right to explanation (as there is under the General Data Protection Regulation (GDPR) [22]), which the European debate shows to be difficult to implement. Wachter, Mittelstadt and Floridi consider that the GDPR does not give rise to a general right to explanation but rather a more limited right to be informed of the automated decision-making. In India, therefore, there are no other legal remedies available to the affected parties apart from general principles of administrative law or sectoral laws.

5.3 Cross-border data flows and localisation

Policy goals around data localisation are closely aligned with privacy and AI policy. The early drafts of the Indian data protection law also included strong localisation requirements for certain classes of personal data due to law enforcement surveillance concerns and the economic value of data. The DPDP Act takes a softer approach [14] on cross-border transfers, permitting them unless specifically restricted from transferring data to any other country or territory, as specified by the government. The Rules also provide for additional data localisation for certain important data fiduciaries on recommendation of the government committee [4, 5]. For AI developers, this role could factor into where to train and host their models.

6. AI AND CYBER GOVERNANCE

6.1 AI as a defensive and offensive capability

Applications of machine learning as a defender include intrusion detection, malware detection, classification of content for phishing detection or automated response to detections. Kaur, Gabrijelcic and Klobucar conducted a survey of research on these applications, classifying them according to the functions of the NIST cybersecurity framework: identify, protect, detect, respond, recovery [13]. The review also

reports increased interest in using advanced algorithms to enable defensive technologies to adapt to previously unknown and novel threats [13].

The same techniques can also be used for attack, such as automated scanning, luring users with realistic social engineering messages, and generating synthetic speech and video for deception. Like other AI systems, these methods are vulnerable to adversarial inputs and data poisoning, and Taddeo, McCutcheon and Floridi argue that they should be used cautiously. This ambivalence of AI systems complicates the governance of cyberspace more than that of other more traditional tools of cyberspace.

6.2. India's institutional and regulatory framework

Cybersecurity law in India is mainly governed by the Information Technology Act. It defines computer crimes and provides the government with the power to block illegal content. It empowers the Indian Computer Emergency Response Team to lead the response to the nation's cybersecurity incidents. In April 2022, CERT-In issued directions for service providers, intermediaries and other entities that require reporting certain forms of cyber incidents within six hours and retaining logs for 180 days, including those related to AI systems. However, they are not focused on the specific risks of AI, such as the theft of a model or the poisoning of training data. Table 4 summarizes the main instruments with AI related gaps.

Table 4. Principal Indian instruments relevant to AI in cyber governance and their AI-related gaps.

Instrument	AI-relevant provisions	Gaps identified
Information Technology Act, 2000 (amended 2008)	Computer-related offences, identity theft and cheating by personation; blocking powers; conditional safe harbour for intermediaries.	No offences specific to AI, such as data poisoning or model theft.
CERT-In Directions, 2022	Six-hour incident reporting and 180-day log retention for covered entities.	Incident categories do not expressly cover adversarial attacks on AI systems.
IT Intermediary Rules, 2021 (amended 2026)	Definition of synthetically generated information; labelling and provenance; three-hour and two-hour takedown periods.	Depends on imperfect detection tools; short deadlines may lead to over-removal. [6]
Bharatiya Nyaya Sanhita, 2023	Offences of personation, defamation and intimidation applicable to deepfake misuse.	Difficulties of attribution and digital evidence for content generated at scale.
DPDP Act, 2023 and Rules, 2025	Security safeguards and breach notification for personal data processed by AI systems.	Substantive duties apply only from May 2027. [5]
India AI Governance Guidelines, 2025	Cross-sector principles and institutional recommendations for responsible AI.	Non-binding; no enforcement mechanism.

The intermediary framework is now the primary regime governing the content moderation of AI outputs. In *Shreya Singhal*, the Supreme Court read down the duties of intermediaries to require a court order or government notice before they could be held to have actual knowledge. The 2021 Intermediary Rules added due diligence obligations for large social media intermediaries. In 2026 this was expanded to cover information produced synthetically (i.e., deepfakes, etc.), thereby bringing them under existing platform liability rules [6].

6.3. Deepfakes and synthetic media

The 2026 amendment is India's first enforceable regulation specific to AI-generated media, defining for the first time in Indian law, synthetically generated information as audio, video or audio-visual content that is artificially or algorithmically created or altered to resemble real content [6]. Platforms must clearly label, preserve provenance metadata of such content and remove specified unlawful content within three hours of notice or within two hours for non-consensual intimate imagery. Significant social media intermediaries must receive declarations from their users whether user-generated content is synthetic and deploy technical measures on verification of synthetic content.

These measures will help fix concrete problems such as fraud, damage to reputation, and election misinformation, but they depend on the reliability of detection and watermarking systems, which have limitations. Very short takedown durations may, to avoid the risk of losing safe harbour protection, cause platforms to remove legitimate content risking the free speech concerns in *Shreya Singhal* again. Finding an appropriate balance between expeditious removals and free speech considerations remains the task of

the courts.

Criminal law also may apply. The criminal offenses that the amended intermediary rules reference would be the offenses charged under Bharatiya Nyaya Sanhita, 2023, which replaced the Indian Penal Code, though other offenses, such as cheating by personation, defamation and criminal intimidation, may also apply. [6] Since these laws were not drafted with AI in mind, the challenges around attribution and gathering evidence for synthetic media at scale may complicate this area of law.

7. CONVERGENCE OF IPR, PRIVACY AND CYBER GOVERNANCE

Despite the common separation in study of the three domains (figure 2), they interface at every stage of the AI lifecycle. Also, copyrightable web text scraped for training data may itself contain personally identifiable data. In the training of ML systems, memorization of protected expression and personal data can raise concerns simultaneously about copyright infringement and breaches of privacy [21]. With the deployment of an ML model comes a highly valuable asset that can easily be obtained and exploited by adversaries [24]. At the output end, the generated content can infringe copyright, leak private information, or be used to perpetrate fraud.

	Data collection	Model training	Deployment and security	Outputs and use
Intellectual property	Scraping of copyrighted works; no TDM exception	Reproduction during training; fair dealing under s. 52	Model as trade secret; CRI patentability (s. 3(k))	Authorship of outputs; infringing reproductions
Data privacy	Consent and notice; public-data exclusion	Purpose limitation; memorisation of personal data	Security safeguards; breach reporting	Profiling and automated decisions; erasure requests
Cyber governance	Data poisoning of source datasets	Adversarial manipulation of training pipelines	Model theft; incident reporting to CERT-In	Deepfakes; labelling and takedown under IT Rules

Fig. 2. Points of intersection between intellectual property, data privacy and cyber governance across the AI lifecycle in India. Source: Conceptual framework developed by the authors.

These fall under the jurisdiction of courts and the DPIIT for copyright, the Data Protection Board for privacy, and MeitY and CERT-in for content moderation and security. This potentially leads to an inconsistent set of standards; for e.g. with the public-availability exemption cause in the DPDP Act, a company can use data that would otherwise have required payment of copyright license fees [4]. The provenance metadata required by the intermediary rules may also contain personal data, which must therefore be dealt with under applicable privacy law.

These ethical principles provide a common language and may drive the alignment of these regimes. Jobin, Ienca and Vayena found broad global consensus around principles of transparency, justice, non-maleficence, responsibility and privacy, although there was wide variation in their interpretation [25]. The India AI Governance Guidelines contain similar principles, but lack a mechanism for translating shared principles into coordinated obligations across the three areas of law.

8. RESEARCH GAPS AND FUTURE DIRECTIONS

The review identifies the governance of the training data as the first research gap. An area for future inquiry in Indian scholarly literature is how the DPIIT hybrid licensing model fits with the DPDP Act, especially for datasets combining copyrighted works and personal data. Further studies on dataset composition and licensing terms for datasets in India would provide insights into these questions.

A second gap relates to algorithmic decision-making by the State: the DPDP Act does not provide for rights in relation to algorithmic decision-making and regulatory gaps are wide [23]. There is potential for the constitutional principles of proportionality to regulate algorithmic decision-making in welfare, policing and taxation. The experience of other jurisdictions in Europe in relation to the right to explanation may also be instructive [11].

A third issue is that the Data Protection Board, the CERT-In and the Patent Office need technical skill to assess AI systems. Regulatory resourcing, inter-agency cooperation, and regulatory sandboxes may inform mechanisms for enforcement, and investigating legal obligations' feasibility may help explain technical options such as reliable watermarking, deepfake detection, and privacy-preserving training.

Finally, there is therefore important scope for work on India's role in global AI governance. As the

European Union and others pass AI governance laws, India will have to decide how far it will align itself with rules made elsewhere [1]. With interoperability, such as cross border data flows and mutual recognition of compliance, India could be a leader in setting international standards rather than just a follower.

9. CONCLUSION

The review has also examined similar legal frameworks in India regarding intellectual property, data privacy and cyber governance. For example, Indian intellectual property law requires human authorship and inventorship, as indicated by the rejection of the DABUS application. The ANI litigation and DPIIT hybrid licensing proposal will set standards for training AI on copyrighted data. The DPDP Act and DPDP Rules provide a consent-based regime for processing personal data but leave open numerous issues concerning public data, exemptions to data protection for the State, and automated decision-making. In the context of cyber governance, the 2026 intermediary amendments would apply to intermediaries in the context of synthetic media for the first time, with general rules covering AI-specific security risks.

Despite all three domains, India has preferred targeted amendments or principles-based regulation over a thorough AI law. While that offers flexibility, it can lead to fragmented regulation where a single AI system may fall under several regulations. Greater coordination between regulators, clear definitions of how training data can be used, and better protections for impacted people, could help India advance a diverse framework for innovation, while also ensuring appropriate and effective rights for people affected by algorithms. What India chooses to do in the next several years could impact both domestic and international governance.

References

1. Smuha NA. From a 'race to AI' to a 'race to AI regulation': regulatory competition for artificial intelligence. *Law, Innovation and Technology* 2021;13(1):57-84. <https://doi.org/10.1080/17579961.2021.1898300>
2. Chatterjee S. AI strategy of India: policy framework, adoption challenges and actions for government. *Transforming Government: People, Process and Policy* 2020;14(5):757-775. <https://doi.org/10.1108/TG-05-2019-0031>
3. Marda V. Artificial intelligence policy in India: a framework for engaging the limits of data-driven decision-making. *Philosophical Transactions of the Royal Society A* 2018;376(2133):20180087. <https://doi.org/10.1098/rsta.2018.0087>
4. The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023). *Gazette of India*, 11 August 2023.
5. Ministry of Electronics and Information Technology. Digital Personal Data Protection Rules, 2025. *Gazette of India*, notified November 2025.
6. Ministry of Electronics and Information Technology. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E). *Gazette of India*, 10 February 2026.
7. Indian Patent Office. Decision on Indian Patent Application No. 202017019068 (Stephen L. Thaler; DABUS), order dated 15 April 2026.
8. ANI Media Pvt. Ltd. v. OpenAI OpCo LLC, I.A. 45300/2024 in CS(COMM) 1028/2024, order dated 24 July 2026 (Delhi High Court).
9. Ginsburg JC, Budiardjo LA. Authors and machines. *Berkeley Technology Law Journal* 2019;34(2):343-456.
10. Gervais DJ. The machine as author. *Iowa Law Review* 2020;105(5):2053-2106.
11. Wachter S, Mittelstadt B, Floridi L. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law* 2017;7(2):76-99. <https://doi.org/10.1093/idpl/ixp005>
12. Solove DJ. Privacy self-management and the consent dilemma. *Harvard Law Review* 2013;126(7):1880-1903.
13. Kaur R, Gabrijelcic D, Klobucar T. Artificial intelligence for cybersecurity: literature review and future research directions. *Information Fusion* 2023;97:101804. <https://doi.org/10.1016/j.inffus.2023.101804>
14. Sundara K, Narendran N. The Digital Personal Data Protection Act, 2023: analysing India's dynamic approach to data protection. *Computer Law Review International* 2023;24(5):129-141. <https://doi.org/10.9785/cr-2023-240502>
15. Hema K. Protection of artificial intelligence autonomously generated works under the Copyright Act, 1957: an analytical study. *Journal of Intellectual Property Rights*

- 2023;28(3):193-199. <https://doi.org/10.56042/jipr.v28i3.708>
16. Guadamuz A. Do androids dream of electric copyright? Comparative analysis of originality in artificial intelligence generated works. *Intellectual Property Quarterly* 2017;(2):169-186.
 17. Abbott R. I think, therefore I invent: creative computers and the future of patent law. *Boston College Law Review* 2016;57(4):1079-1126.
 18. Kim D. 'AI-generated inventions': time to get the record straight? *GRUR International* 2020;69(5):443-456.
 19. Lemley MA, Casey B. Fair learning. *Texas Law Review* 2021;99(4):743-785.
 20. Samuelson P. Generative AI meets copyright. *Science* 2023;381(6654):158-161. <https://doi.org/10.1126/science.adi0656>
 21. Veale M, Binns R, Edwards L. Algorithms that remember: model inversion attacks and data protection law. *Philosophical Transactions of the Royal Society A* 2018;376(2133):20180083. <https://doi.org/10.1098/rsta.2018.0083>
 22. Naithani P. Analysis of India's Digital Personal Data Protection Act, 2023. *International Journal of Law and Management* 2025;67(5):543-553. <https://doi.org/10.1108/IJLMA-05-2024-0174>
 23. Sonkar A. The Digital Personal Data Protection Act, 2023: analysing its implications, challenges, and future prospects. *International Cybersecurity Law Review* 2025;6(4):547-569. <https://doi.org/10.1365/s43439-025-00164-2>
 24. Taddeo M, McCutcheon T, Floridi L. Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence* 2019;1(12):557-560. <https://doi.org/10.1038/s42256-019-0109-1>
 25. Jobin A, Ienca M, Vayena E. The global landscape of AI ethics guidelines. *Nature Machine Intelligence* 2019;1(9):389-399. <https://doi.org/10.1038/s42256-019-0088-2>