© NOV 2025 | IRE Journals | Volume 9 Issue 5 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I5-1712298

Artificial Intelligence and Personal Rights in India: A Constitutional, Data Protection, and IPR Law Analysis

NATASHA TIWARI
Iilm University

I. FRAMING THE AI-RIGHTS NEXUS IN THE INDIAN CONTEXT

A. The Dual Challenge of AI: Innovation and Constitutional Safeguards

Artificial Intelligence (AI) presents India with a profound and complex legal challenge, balancing the imperative for technological advancement with the constitutional necessity of safeguarding individual rights. The rapid rise of AI creates immense opportunities globally, particularly in areas like healthcare diagnoses, labor efficiency, and social connections. India, as one of the world's fastest-growing digital economies, views AI-led innovation as crucial for achieving national goals such, as socio-economic development and global competitiveness.

However, the proliferation of AI systems also raises deep ethical and legal concerns. These systems possess the potential to embed biases, contribute to climate degradation, and threaten fundamental human rights. The associated risks often compound existing inequalities, resulting in harm to already marginalized groups. The central difficulty arises because traditional legal frameworks, which are anchored in established concepts like human authorship, identifiable data subjects, and clear chains of liability, struggle to adapt to autonomous machine learning systems that learn, adapt, and create independently.

India's strategy, formalized in the India AI Governance Guidelines (2025), is defined by a philosophical principle emphasizing agile, pro-innovation governance: "responsible innovation should be prioritised over cautionary restraint". The goal is to maximize the benefits of AI for growth and inclusion while proactively mitigating risks to individuals and society.

B. Defining Personal Rights in the Digital Age: Dignity, Autonomy, and Attribution

In the context of AI, personal rights transcend traditional privacy boundaries, forming a complex nexus that encompasses three core areas:

- Foundational Constitutional Rights**:** These include the right to privacy and dignity (Article 21), which serve as the ultimate check on state and non-state use of AI, particularly against surveillance and discriminatory algorithmic outcomes.
- Digital Rights and Autonomy**:** These are codified in the Digital Personal Data Protection (DPDP) Act, 2023, granting individuals rights over their personal data, including the right to consent, the right to access data, and the right to seek explanations and redressal for automated decisions.
- Intellectual Property and Dignitary Rights: These focus on the right to attribution for creators and, crucially, the right to control the commercial exploitation of one's identity, likeness, voice, and persona, especially in the face of generative AI technologies like deepfakes.

C. Overview of India's Legal and Regulatory Response

India's response to these challenges utilizes a multi-layered legal and policy architecture:

- Cyber Laws: The Information Technology Act, 2000 (IT Act), and subsequent rules govern the digital ecosystem and address cybercrimes, including impersonation and misinformation (deepfakes).
- Data Protection: The DPDP Act, 2023, provides the mechanism for governing the collection and processing of personal data necessary for training and deploying AI models.

- Intellectual Property Rights (IPR): The Copyright Act, 1957, the Patents Act, 1970, and the Trademarks Act, 1999, define ownership and infringement, but rely heavily on human agency.
- Soft Law: The India AI Governance Guidelines (2025) set forth non-binding standards for responsible AI deployment, focusing on risk mitigation and ethical principles.

II. THE CONSTITUTIONAL BEDROCK: PRIVACY, DIGNITY, AND ALGORITHMIC JUSTICE

A. The Puttaswamy Doctrine (2017) and the Right to Privacy (Article 21)

The foundation of personal rights protection in the digital era is the landmark judgment in *Justice K.S. Puttaswamy v. Union of India* (2017), which unequivocally declared the right to privacy as a fundamental right under Article 21 of the Constitution. This ruling established both informational privacy and decisional autonomy as intrinsic to human dignity and liberty.

The Puttaswamy judgment is pivotal because it imposes strict scrutiny on both state and non-state actors regarding data processing and surveillance. Any governmental action that infringes upon privacy must satisfy a stringent three-pronged test: it must be based on legality (backed by clear law), demonstrate necessity (serve a legitimate state aim), and be proportionate (employ the least intrusive means).

This constitutional standard fundamentally dictates the boundaries of AI regulation in India. The necessity for judicial review under the proportionality test means that any AI system deployed by the state, such as large-scale surveillance using facial recognition, must be clearly justified and demonstrably non-arbitrary. The stringent constitutional requirement for reasoned decisions and fairness dictates the subsequent policy moves to mandate transparency and prohibit the use of certain high-risk AI applications. For instance, the government's decision to ban the social scoring of citizens is not merely a regulatory choice but a necessary constitutional alignment, as deploying such systems would invariably fail the proportionality test required by Puttaswamy.

B. Anti-Discrimination Principles and the Challenge of Algorithmic Bias

The deployment of AI systems raises significant questions regarding Articles 14 and 15 (Right to Equality and Prohibition of Discrimination). The concern is not merely explicit bias, but the more subtle, yet equally destructive, form of indirect discrimination. Algorithms, even when not explicitly programmed to consider protected characteristics like caste, religion, or gender, may rely on proxy variables that correlate highly with historical discrimination, leading to systematically biased outcomes. A relevant parallel is seen in foreign cases, such as the US COMPAS system, where an algorithm produced biased outcomes by relying on factors that served as proxies for racial discrimination, even though race itself was not a factor.

In India, the application of technology such as Automated Facial Recognition Systems (AFRS) has prompted profound constitutional scrutiny. When state authorities deploy technology that has known, systematically higher error rates for certain communities, and then concentrate that technology's deployment in areas predominantly populated by those communities (e.g., areas with significant Muslim populations), the outcome is state-sponsored discrimination under the seal of technological authority. This challenges the fundamental constitutional guarantee of equality.

To mitigate this systemic risk, the consensus suggests that technical checks for bias are insufficient without genuine public consultation and robust operational oversight. The existence of opacity in advanced AI systems, sometimes referred to as the 'black box' problem, creates a precarious legal precedent. If courts accept the use of AI but express discomfort with its lack of transparency, a tension emerges between natural justice principles (which require reasoned, explainable decisions) and technical reality. Consequently, robust governance mandates non-biased human-in-the-loop oversight. Human reviewers must be empowered and accountable, with the authority to question and overturn automated

decisions affecting constitutional principles, such as those related to bail, welfare, or employment.

III. DATA SOVEREIGNTY AND ALGORITHMIC ACCOUNTABILITY UNDER THE DPDP ACT, 2023

The Digital Personal Data Protection (DPDP) Act, 2023, is the primary statutory tool designed to manage the profound conflict between AI's voracious need for data and the individual's right to privacy. The Act fundamentally changes how AI companies must collect, process, and secure personal data, significantly raising the compliance bar.

A. Foundational Principles and Consent for AI Training Data

The DPDP Act is built upon the core principles of consent, purpose limitation, and data minimization. For AI systems, which are inherently data-intensive, this means that data fiduciaries cannot rely on vague or "bundled consent". Consent must be free, specific, informed, unconditional, and unambiguous, and limited precisely to the personal data necessary for the specified purpose. Furthermore, mechanisms for a data principal to withdraw their consent at any time must be made as simple as the original consent process.

For the purpose of AI model training, the Act requires rigorous compliance with data provenance and privacy-preserving processes. If developers use personal data for training, they must implement anonymisation and utilize Privacy-Enhancing Technologies (PETs), such as federated learning, homomorphic encryption, and differential privacy, to align with the Act's requirements. This mandate necessitates robust data governance systems, meticulous tracking of dataset provenance, and the lawful processing of personal data.

For multinational firms, this compliance extends to reassessing cross-border AI training pipelines to prevent violations of Indian privacy norms. By mandating strict adherence to localization and high compliance standards for training data, the DPDP Act functions as a strategic shield favoring domestic AI development, ensuring that the personal data of Indian citizens is handled responsibly and remains protected within the Indian jurisdiction.

B. Algorithmic Accountability for Significant Data Fiduciaries (SDFs)

The DPDP Rules, 2025, introduce specific and stringent algorithmic governance requirements for entities designated a Mandatory Algorithmic Impact Assessments (AIAs)

SDFs must conduct an Annual Data Protection Impact Assessment (DPIA) and an audit every twelve months. Crucially, the due diligence obligations extend explicitly to technical and algorithmic systems. SDFs must verify that the algorithms used for hosting, displaying, modifying, or sharing personal data do not endanger the rights of Data Principals. This requires conducting algorithmic impact assessments that specifically examine fairness, transparency, accuracy, and rights implications of the deployed AI. This requirement proactively addresses algorithmic bias and positioning India ahead of many jurisdictions in operationalizing comprehensive algorithmic accountability.

The Profiling Prohibition Paradox A critical area of regulatory friction lies in the DPDP Act's treatment of user profiling. Section 18(2)(b) stipulates that the government may permit the processing of personal data for research or statistical purposes, but only on the condition that the data is *not* used to take any "decision-specific user profiling". This creates a significant legal ambiguity. Many high-value commercial AI applications—such as personalized credit scoring, targeted health diagnoses, or customized content recommendations—fundamentally rely on decision-specific profiling. The Act's rigid stance on prohibiting this profiling, potentially without adequate exceptions, directly clashes with the national objective of accelerating AI adoption and innovation. This regulatory ambiguity represents a critical compliance risk and requires urgent policy clarification to ensure the feasibility of commercial AI deployment.

© NOV 2025 | IRE Journals | Volume 9 Issue 5 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I5-1712298

C. Data Principal Rights and Redressal

The DPDP framework places the individual—the Data Principal—at the center of India's data protection system. Individuals retain clear control over their personal data, including the right to access, correct, and demand deletion of their data. This deletion right is maintained even if the data has been used in model training, requiring AI developers to establish effective processes for data removal from their operational pipelines.

The Functional Right to Explanation

Although the DPDP Act may not contain a single, explicit 'right to explanation' as codified in GDPR Article 22, the combination of principles in the Act and the India AI Guidelines implies a functional right for individuals to understand how automated systems affect them. The MeitY Guidelines emphasize "Understandable by Design" , requiring clear disclosures and explanations that can be understood by the user. The due diligence rules for SDFs necessitate transparency and accountability in algorithmic decision-making. Furthermore, the establishment of Consent Managers is expected to streamline user control, enabling individuals to grant, withdraw, track, or review consent across different services and manage their permissions for data access, correction, and deletion.

Grievance Redressal

The DPDP Act provides clear redressal mechanisms. Appeals against non-compliance or misuse will be heard by the Data Protection Board (DPB), which is established as the enforcement authority. Further appeals against the DPB's decisions are then heard by the Appellate Tribunal, TDSAT. This layered judicial and regulatory oversight is designed to ensure quick decisions and simplified grievance redressal in the face of algorithmic harm.

Table 1: AI Challenges and Corresponding DPDP Act Compliance Requirements

AI Challenge Domain	Relevant DPDP Provision	Compliance Requirement for Data Fiduciaries (DFs)
Algorithmic Bias/Discrimination	Fairness, Accountability (AIA), Purpose Limitation	Conduct mandatory Algorithmic Impact Assessments (AIAs) to examine fairness, accuracy, and rights implications annually.
Training on Personal Data	Specific, Unambiguous Consent (Section 6)	Ensure granular, documented consent; implement anonymisation/PETs for training datasets.
Automated Profiling	Rights of Data Principal, Specified Purpose	Prohibit general-purpose profiling or use of sensitive data for targeted advertising/decisions concerning children.
Cross-Border Data Transfers	Restrictions/Localization Norms	Reassess offshore AI training pipelines to ensure compliance with data transfer rules/localization if applicable.

IV. PROTECTING DIGITAL PERSONA: THE RIGHT TO PUBLICITY AND THE DEEPFAKE CRISIS

A. The Evolution of Personality Rights in India: A Fundamental Right

Personality rights in India have evolved from the constitutional guarantee of dignity and life under Article 21. This legal right protects an individual's identity and attributes against unauthorized use. It comprises two complementary facets: the dignitary aspect (personal autonomy and privacy) and the commercial aspect, commonly known as the right of publicity. The latter allows individuals, particularly celebrities, to control the commercial exploitation of their name, image, voice, and likeness.

The affirmation of privacy in *Puttaswamy* provided a strong constitutional foundation for individuals to assert control over the commercial use of their identity. The courts, recognizing that commercial exploitation can cause irreparable harm and tarnish a person's reputation, have actively applied this principle.

B. Judicial Response to AI Misuse: Landmark Deepfake and Cloning Precedents

In the absence of dedicated deepfake legislation, Indian courts have provided robust and proactive protection against unauthorized AI replication, often through the use of *John Doe* injunctions targeting unidentified individuals, websites, and platforms. These judicial interventions are establishing crucial emerging legal norms for the AI era.

Deepfakes and Unauthorized Likeness

In landmark decisions, courts have addressed the sophistication and deceptive nature of AI-generated content. The Bombay High Court, while hearing a petition filed by actor Akshay Kumar, ruled that AI-generated videos and deepfakes using a person's likeness without consent amount to a clear violation of personality rights. The court noted that fabricated content, particularly deepfakes portraying individuals making inflammatory statements, poses a grave threat not only to the person's moral and personality rights but also to the social order by provoking communal tensions and compromising public safety.

Voice Cloning and Persona Traits

Protection has been extended beyond static images to dynamic elements of a persona. The Delhi High Court, in the case of *Anil Kapoor v. Various Entities*, and subsequent rulings (e.g., *Arijit Singh*, *Asha Bhosle*), confirmed that personality rights encompass unique traits such as voice, gestures, manner of speaking, and expressions. Unauthorized AI-based voice cloning was unequivocally held to violate both personality and publicity rights, weakening the celebrity's brand equity.

The judicial approach carefully distinguishes lawful uses, such as free speech, news reporting, satire, or parody, from unauthorized commercial exploitation or use that results in tarnishment or defamation. By providing broad injunctive relief and placing the entire digital persona under protection, the judiciary has proactively established a common law principle that the right to control one's identity is paramount in the age of generative AI.

C. The Statutory Framework for Mitigation and Enforcement (IT Act & DPDP Act)

Existing cyber laws and new data legislation provide mechanisms for tackling the deepfake crisis:

- IT Act, 2000**:** The Act covers relevant cybercrimes, including identity theft, cheating by personation (Section 66D), and violation of privacy (Section 66E).
- Intermediary Due Diligence**:** The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021/2023, mandate strict obligations for social media platforms and other intermediaries. Platforms must act quickly to remove harmful deepfake content, typically within 36 hours.
- Techno-Legal Solutions: Government advisories further mandate that intermediaries must apply permanent, machine-readable labels or metadata to AI-generated content. This technological requirement, which involves the use of content authentication and provenance tools, shifts the burden of authenticity from the end-user to the platform or creator. If content lacks required provenance or violates these diligence mandates, intermediaries risk losing their "safe harbour" protection under Section 79 of the IT Act.

V. IPR EMPHASIS (PART I): AUTHORSHIP, INVENTORSHIP, AND THE HUMAN-CENTRIC MANDATE

India's Intellectual Property Rights (IPR) framework is fundamentally human-centric, creating significant obstacles for fully autonomous AI-generated content seeking protection. The consistent denial of authorship or inventorship to AI across statutes serves a critical function: enforcing human accountability and ensuring that proprietary benefits accrue to legal human entities.

A. Copyright Law (Copyright Act, 1957): The Authorship Requirement

The Indian Copyright Act, 1957, relying on Sections 2(d), 13, and 17, is anchored in the premise of identifiable human authorship and original expression.

Status of AI-Generated Output

Works produced by entirely autonomous AI—where the human role is limited to inputting a simple prompt without subsequent editorial or creative control—are unlikely to be considered "works" eligible for copyright. The consensus among scholarly and professional analyses is that creativity remains an attribute of humans, and the autonomy of machines does not generally satisfy the requirements for originality or authorship. Consequently, purely AI-generated content typically defaults to the public domain in India.

The Doctrine of Minimal Creativity

Copyright protection can be secured only where a human can be identified as the author or controller. Under the doctrine of "minimal creativity," even minor creative contributions, such as selecting, modifying, or refining an AI-generated output, may be sufficient to attribute authorship to a human. Businesses seeking to protect AI-enabled assets must therefore maintain comprehensive documentation of editorial discretion and ensure human creative control over the final expression.

B. Patent Law (Patents Act, 1970): The Inventorship Requirement

The Patents Act, 1970, clearly adheres to the global consensus that an inventor must be a natural person. AI cannot be named as an inventor, meaning only a human creator, developer, or the entity controlling the AI can apply for a patent.

Patentability of Computer-Related Inventions (CRIs)

The Indian Patent Office (IPO) Guidelines for Examination of Computer-Related Inventions (CRIs) provide clarity on the patentability of AI-related technical innovations. While a computer program *per se*, or a mere algorithm, is explicitly excluded under Section 3 of the Patents Act, inventions relying on AI are patentable if they demonstrate a "technical effect" or "technical contribution". For example, a pure data classification algorithm may not be patentable, but an AI model integrated into a medical device that improves diagnostic accuracy is likely to qualify, as it demonstrates a technical application beyond a mathematical method.

C. Trademark and Design Law

Similar to copyright, trademark law requires human involvement to establish proprietary rights.

Trademark Ownership

For trademarks generated by AI, ownership is awarded to the user or company commissioning the AI tool usage, provided a degree of human influence in the selection, modification, or approval of the mark can be demonstrated. The AI is legally treated as a tool used in a larger creative process, rather than the sole creator. To ensure legal validity, applicants must document active involvement and decision-making in the design process, making clear that a human being or corporate entity is the legal owner.

Liability and Trade Secrets

Companies involved in AI-led brand creation bear the liability for infringement. Consequently, the industry has adopted the strategy of frontier assignment of ownership and liability to the legal entities that operate the AI tool.

Given the limitations in protecting autonomous AI output under copyright and patent law, a strategic shift is observed where companies increasingly rely on trade secrets and robust technological safeguards to protect the underlying AI models, training data composition, and proprietary methodology. This allows organizations to protect their competitive advantage without the public disclosure often required by patent regimes.

Table 2: Status of AI-Generated Intellectual Property under Indian Law

IPR Type	AI Role	Current Legal Status in India (Human-Centric View)	Key Legislative Basis/Case Law
Copyright	Sole Creator	Generally unprotected; falls into the public domain due to lack of substantial human creative input.	Copyright Act, 1957 (Sec 13, 17); Minimal Creativity Doctrine.

IPR Type	AI Role	Current Legal Status in India (Human-Centric View)	Key Legislative Basis/Case Law
Patent	Named Inventor	Prohibited; AI cannot be recognized as an inventor, only a natural person.	Patents Act, 1970; IPO CRI Guidelines (Natural Person requirement).
Trademark	Designer/Suggester	Registrable only if human involvement in selection, modification, or approval is proven by the commissioning entity.	Trademarks Act, 1999; Requirement for human application.
Personality	Unauthorized Replicator (Deepfakes)	Violation of inherent personality/publicity rights, subject to injunctions.	Article 21 Constitution; High Court Precedents (Anil Kapoor, Akshay Kumar).

VI. IPR EMPHASIS (PART II): THE TEXT AND DATA MINING (TDM) INFRINGEMENT CONFLICT

The most critical interface between AI and Indian IPR law concerns the legality of utilizing copyrighted works to train generative AI models, an activity known as Text and Data Mining (TDM).

A. Exclusive Rights of Reproduction and Strict Liability

Generative AI models, by their nature, require access to vast quantities of data (text, images, music) for training. This process inherently involves mass-scale reproduction and storage of existing content. The Copyright Act, 1957, grants the author the exclusive right "to reproduce the work in any material form including storing of it by electronic means" (Section 14). Consequently, training an AI model on a library of copyrighted material without authorization triggers strict liability for infringement under Section 51.

The legal focus is not on the final AI output (which may or may not infringe), but on the antecedent act of mass copying during the training phase. This upstream liability means that AI developers can be sued for the data collection phase, necessitating robust provenance management and authorized data sourcing.

B. The Narrow Scope of Indian Fair Dealing (Section 52): Inadequacy for Commercial TDM

India's existing copyright law offers no explicit exception for automated TDM. The only clear exemption, the doctrine of *fair dealing* under Section 52, is narrowly interpreted by courts to cover only enumerated purposes, such as private research, criticism, or review.

This narrow interpretation means that the commercial use of copyrighted works for training AI models is explicitly *not* protected under fair dealing. Developers operating in this legal grey area rely either on assumed permissions for public data or face the risk of expensive infringement litigation.

C. Legal and Economic Consequences of the Lacuna

The absence of a statutory TDM exception creates a significant compliance hurdle for commercial AI development in India. This challenge is magnified by a dual compliance bottleneck: a developer using publicly available data must simultaneously ensure privacy compliance (DPDP Act, requiring consent/anonymization for personal data) and copyright compliance (TDM, requiring licensing or an exception for creative data). Since public availability does not negate either the need for copyright protection or DPDP consent, this joint friction dramatically increases compliance costs and risks.

The economic consequence of this lacuna is existential for the AI sector. While some warn that requiring licenses for the vast volume and diversity of content needed to train cutting-edge systems could "throttle a transformative technology" , others fear that unlicensed training will corrode the creative ecosystem by allowing AI to produce competing content without compensating the original authors.

D. Policy Solutions: The Case for a Statutory TDM Exception

Recognizing this conflict, the India AI Governance Guidelines suggest considering a Text and Data Mining exception. The policy challenge lies in striking an effective balance that allows innovation to flourish while protecting the creative community.

A growing number of legal experts advocate for a multi-tiered approach to TDM reform. This would involve introducing broad statutory exceptions for non-commercial TDM, such as for academic research, while preserving licensing rights or implementing limited exceptions for commercial exploitation. Such clarity would encourage innovation by reducing uncertainty while upholding the exclusive economic interests of copyright holders. Until such amendments are introduced, businesses must mitigate risk through robust contractual protections and responsible sourcing of training data.

VII. INDIA'S EMERGING GOVERNANCE FRAMEWORK AND GLOBAL ALIGNMENT

India's proactive approach to AI governance is encapsulated in the India AI Governance Guidelines (2025), a "soft law" architecture released by the Ministry of Electronics & Information Technology (MeitY) under the IndiaAI Mission.

A. The India AI Governance Guidelines (2025): A Soft Law Architecture

The Guidelines aim to foster a safe, inclusive, and responsible AI ecosystem. While not a binding statute, the framework provides a comprehensive, techno-legal guide built on seven foundational principles, or Sutras:

1. Trust as the Foundation 2. People First 3. Innovation over Restraint 4. Fairness and Equity 5. Accountability 6. Understandable by Design 7. Safety, Resilience and Sustainability

These principles ground AI governance in Indian constitutional and socio-economic realities, while mirroring global standards like those promoted by UNESCO.

B. Risk Mitigation Taxonomy and Prohibited Systems

The governance framework adopts a risk-based approach, which is critical for mitigating risks such as algorithmic discrimination, malicious use (deepfakes), lack of transparency, and systemic risks. This taxonomy provides clear boundaries, explicitly identifying use cases deemed fundamentally incompatible with constitutional rights and democratic principles.

Prohibited AI Systems

In alignment with the constitutional requirement for proportionality, the Guidelines identify specific high-harm AI systems that are banned regardless of technical safeguards:

- Social scoring of citizens for access to public benefits.
- Biometric categorization based on sensitive personal attributes (e.g., race, political opinions).
- Emotion inference utilized for high-stakes decisions (e.g., employment, education, or credit).
- Subliminal manipulative techniques targeting vulnerable populations.

High-Risk Systems

Systems operating in domains where failures could cause significant individual or societal harm are classified as High-Risk. These systems demand the highest levels of governance, continuous monitoring, standardized assurance mechanisms (like ISO/IEC 42001 adoption), and human oversight. The obligations placed on these High-Risk systems overlap significantly with the mandatory Algorithmic Impact Assessments required of Significant Data Fiduciaries under the DPDP Rules.

C. Global Alignment and Institutional Framework

India's risk-classification approach, particularly the explicit prohibitions on social scoring and sensitive biometric categorization, shows a strong convergence with the fundamental objectives and taxonomy of the European Union's AI Act concerning unacceptable and high-risk applications. This alignment suggests a shared global understanding of constitutional red lines in AI deployment.

The institutional framework designed to implement the AI governance guidelines involves a decentralized, agile approach. Instead of relying on a single omnipotent regulator, the framework maps key roles to existing government agencies (MeitY, MHA) and specialized sectoral regulators (RBI for finance, SEBI for securities, TRAI for telecom). This strategy ensures that AI risks are managed by domain experts, enabling adaptive regulation without imposing overly compliance-heavy regimes, thereby maintaining the "Innovation over Restraint" philosophy.

Future policy directions include developing clear liability regimes across the AI value chain and setting global standards around content authentication and provenance (especially against deepfakes). The roadmap is focused on developing India-specific risk assessment and classification frameworks, ensuring legal amendments keep pace with emerging risks, and promoting the responsible integration of Digital Public Infrastructure (DPI) with AI.

VIII. CONCLUSION AND EXPERT RECOMMENDATIONS

The intersection of Artificial Intelligence and personal rights in India is defined by a dynamic legal landscape where robust constitutional principles are applied to nascent technology via judicial interpretation, statutory reform (DPDP Act), and strategic soft law (AI Governance Guidelines). India has successfully anchored digital rights in the fundamental right to privacy (Puttaswamy) and has empowered its judiciary to provide swift protection against digital persona violations (deepfakes, voice cloning). However, critical legal lacunae, particularly within the IPR regime, persist and threaten to constrain innovation.

A. Summary of Key Legal Lacunae and Tensions

- Copyright and TDM: The lack of a statutory Text and Data Mining exception for commercial use forces AI developers to operate in a legal grey zone, creating significant liability risk for the training phase and increasing the cost of compliant AI development.
- Profiling Ambiguity: The rigid provision within the DPDP Act prohibiting "decision-specific user profiling," unless exempted, introduces substantial uncertainty for core commercial AI applications, risking a regulatory clash with the mandate for innovation.
- IPR Predictability: The highly human-centric IPR framework, while ensuring accountability, requires standardized criteria for defining "significant human authorship" in generative AI content to provide predictability for content creators and the Copyright Office.

B. Policy Imperatives for Legislative Modernization

To resolve these tensions and realize the vision of "responsible innovation," the following legislative modernizations are necessary:

- TDM Reform in Copyright Act: Parliament must urgently introduce a clear, multi-tiered statutory TDM exception within the Copyright Act, 1957. This reform should provide a broad exception for non-commercial and research-based TDM while either facilitating compulsory licensing or providing a carefully defined, non-opt-out exception for commercial TDM, ensuring creators receive fair compensation while enabling machine learning at scale.
- AI-Specific Graded Liability Framework: The governance system must move toward a formal, graded liability framework based on the risk level (prohibited, high-risk, minimal risk) and function performed by the AI system, ensuring that liability rests with the entity exercising control or oversight, as suggested by the MeitY Guidelines.
- Codification of Personality Rights: To provide statutory certainty and uniform application beyond disparate judicial precedents, a dedicated law or amendment should codify the right of publicity, explicitly defining protections against AI voice cloning, likeness exploitation, and deepfake creation for commercial gain.

C. Recommendations for Judicial and Regulatory Consistency

Operational clarity is essential to complement legislative reform:

- DPB Guidelines on Profiling and AIAs: The Data Protection Board (DPB) must prioritize the development and public issuance of comprehensive guidelines. These guidelines should clearly define the scope of "decision-

specific user profiling" under the DPDP Act and standardize the required methodology and metrics for Algorithmic Impact Assessments (AIAs) to be conducted by Significant Data Fiduciaries.

- Techno-Legal Synergy: Regulatory bodies, including MeitY and CERT-In, must continue promoting the use of mandatory technological solutions, such as Content Provenance and Authenticity (C2PA) standards, to ensure that legal compliance requirements (DPDP consent, IPR attribution) are facilitated by engineering solutions (PETs, machine-readable labels).

By addressing the IPR lacunae and providing clarity on data processing requirements, India can consolidate its current position, leveraging its strong constitutional foundation to serve as a global model for balanced, rights-protective, and pro-innovation AI governance.