Developing AI within India's regulatory framework

Thought Leadership • March 8, 2025

'First published on India Business Law Journal'

By: Pravin Anand, Dr. Ajai K Garg, Vibhav Mithal, Siddhant Chamola and Alvin Antony

The rapid advancement in artificial intelligence subsequent to the maturation of generative artificial intelligence (GenAI) models in the past few years marked a milestone in technological innovation.

Many creative processes, be it writing and visualising scripts, gathering comprehensive sector specific information, enabling drug discoveries or creating next-generation business processes, have been disrupted. GenAI models involve a combination of algorithms trained on large datasets comprising billions of words, images, video, etc., that contain both proprietary and public data.

Most jurisdictions including India are still contemplating a holistic AI governance framework. In view of this evolving landscape, it is imperative that existing legal frameworks be effectively utilised to ensure holistic AI governance for developers/deployers to ensure that their innovations do not come about at the expense of ethical standards and legal compliance.

AI and copyright infringement

Recently, a news corporation, in the case of *ANI Media v OpenAI*, brought claims against the storage and use of copyright protected material to train ChatGPT. The court acknowledged that the case involves novel questions as to whether storage and use of copyright protected data for training AI

models qualifies as infringement or fair use.

Copyright owners argue that unlicensed storage and use of their copyright protected work to train AI models infringes their copyrights under sections 14 and 51 of the Copyright Act, 1957. Also, as many of these processes are for commercial purposes, it may be argued that fair use may not apply.

In this regard, India's concept of "fair dealing" under section 52(1)(a), unlike the US doctrine of fair use, is limited to three scenarios: private use or research; critique or review; and reporting current affairs. The government of India has previously taken a stance in the parliament, that AI developers must obtain a licence from copyright holders to use their work for training AI, as long as such use is not covered under the "fair dealing" exceptions.

Perspective of AI developers

Fair dealing. The developers' argument can revolve around the fact that there is a transformative difference between an AI output and the data on which the AI tool has been trained. So, the storage and use of copyrighted work to train an AI model qualifies as fair dealing under section 52(1)(a), as the copying of data is specific to the purpose of training and not to allow users to access or read the original copyrighted work.

De minimis. The de minimis (too small to be considered by courts) doctrine may further provide a defence for AI developers that training AI models involves copying and storing data only once, and so qualifies as insignificant use of copyrighted work as per the five factors there: (1) size of harm; (2) costs and practicality of a legal action; (3) purpose of infringement; (4) effect on third parties; and (5) intent of the accused.

To bolster their argument, a stance may be taken that learning for an AI model is different from copying, that its subsequent retrieval is not reproduction, and thus that there is no intent to use copyrighted data unauthorisedly.

User harm and liability

Inherent algorithmic bias and lack of comprehensive training data have many a time resulted in false or misleading output by an AI model. With time and increasing reliance on AI, societal and commercial harms due to such false or misleading outputs may compound if reasonable care and audits are not incorporated as part of AI development processes.

GenAI model outputs often contain fabricated and imaginary information (a phenomenon known as hallucination), which raises issues of credibility. To address such issues, the current legal framework provides the following:

Users' perspective

The tort of negligent misinformation can be successfully invoked against those who deploy AI to engage with clients, e.g., complaint redressal chatbots or mental health agents. To succeed, one will have to show negligent misinformation on which the user relied and consequently has suffered harm. This tort was invoked by a Canadian court in *Moffatt v Air Canada* to penalise an airline whose chatbot provided wrong information about airfares, resulting in financial harm to the user.

A promise of extraordinary results/claims in relation to an AI product or service that culminates in a lack of credible information may attract product or service liability under sections 84, 85 and 86 of the Consumer Protection Act, 2019. These provisions can also be invoked if a consumer was not adequately warned against relying on AI-generated content for decision making.

Further, under sections 17 and 18 of the act, consumers can also complain about misleading advertisements and unfair trade practices. In addition, such AI practices, which may trick a consumer to do something the person originally did not intend to, may attract action under the Guidelines for Prevention and Regulation of Dark Pattern, 2023.

Deepfakes manipulate audio and video content to create deceptive representations and pose distinct risks to privacy and public trust. They violate common law principles by infringing on privacy and constituting defamation if they harm an individual's reputation.

Courts have extended protection to celebrities such as Anil Kapoor, Jackie Shroff, Arijit Singh, Vishnu Manchu and others whose personality rights were violated through AI-enabled deepfakes.

Moreover, depending on the nature of the content generated by the deepfakes, criminal proceedings to protect against cheating by personation or transmission of obscene material can be initiated under sections 66D, 67A and 67B of the Information Technology Act, 2000 (IT Act).

AI developers' compliance

Intermediary guidelines 2021. To the extent that AI developers/deployers can be considered "intermediaries", they are obligated to inform all subscribers that they must not post false information and ensure that they comply with this (see rule 3 (1)(b)(v)). However, whether AI developers/deployers qualify as "intermediaries" still requires comprehensive legal or legislative interpretation in view of the perception that they themselves are active participants in the generation of output.

Government advisory on AI generated data. Although they are not binding law, AI deployers and developers should comply with the following suggestions by the Ministry of Electronics and Information Technology in its advisory of March 2024:

1. All foundation models should clearly inform users and obtain their consent concerning the fact that AI-generated data is susceptible to mistakes and falsehoods; and

2. Any content with the potential of being used as a deepfake should be labelled and have metadata that identifies it as being AI-generated.

Data privacy and AI

The convergence of AI and data privacy in India requires navigating an evolving legal framework, with the DPDPA Act and recently published draft rules at its centre.

This act mandates obtaining explicit consent from individuals before processing their data, except under specific exceptions like legal obligations, public duties or vital interests.

Balancing innovation with privacy protection, the act requires strict safeguards such as encryption, access controls and breach notifications.

Non-compliance with these safeguards can result in heavy penalties. Complementing this regulatory framework is Nasscom's The Developer's Playbook for Responsible AI in India, launched in November 2024, which is offering AI developers guidance on adhering to the DPDPA.

Tips for success

Although our study and experience with the identified issues will continue to evolve, a few tips that will prevent being on the wrong side of the law include the following:

1. **Copyright.** Although the question has yet to be decided in court, industry trends point to an increasing number of licence agreements for the use of copyright protected data for training AI models.
   If data for innovation is a priority in an AI domain, licensing datasets instead of crawling the web without consent may be a better idea. However, this view may change if Delhi High Court decides that the use of copyright protected data to train an AI system does not infringe copyright.
2. **AI hallucinations.** Generative AI models must carry appropriate disclaimers for users and inform them not to rely solely on AI output. Failure to do so may attract liability. There is a need for a standards-based approach to evaluating/auditing AI models prior to their deployment.
3. **AI misinformation and deepfakes.** All synthetic content should be proclaimed as AI-generated and may use C2PA (Coalition for Content Provenance and Authenticity) metadata (or comply with similar standards) that helps identify its origins (provenance), and detect and track anyone who may have tampered with the data.
4. **Data privacy.** AI companies should adopt privacy by design and aim to build trust. Nasscom's The Developer's Playbook for Responsible AI in India presents a blueprint for how AI developers can employ a privacy-by-design framework within their organisations.

KEY CONTACTS

Pravin Anand
Managing Partner
View Bio of Pravin Anand

Vibhav Mithal
Associate Partner
View Bio of Vibhav Mithal

Siddhant Chamola
Associate Partner
View Bio of Siddhant Chamola