INDIALAW



INTELLECTUAL PROPERTY RIGHTS | TECHNOLOGY LAW

Generative AI and Business Strategy: Legal and Regulatory Challenges in a Transforming Landscape

AUTHOR Arpita Dutta

PUBLISHED 20 July 2026

Generative Artificial Intelligence (“GenAI”) represents a major shift in the corporate technology landscape, evolving in a remarkably short period from an employee productivity tool to a significant concern for employers, compelling businesses across industries to reassess both their operational models and the legal and regulatory frameworks that govern them. This intersection of technological innovation and legal uncertainty is a present-day business reality requiring companies, policymakers, and legal professionals to adopt practical and forward-looking governance strategies. Against this backdrop, India is positioning itself as a global AI innovation hub through the IndiaAI Mission, a national initiative designed to encourage the responsible development and adoption of artificial intelligence. The Mission seeks to expand access to computing infrastructure, improve the availability of high-quality datasets, support the development of indigenous AI models, nurture skilled talent, strengthen industry-government collaboration, accelerate AI startups, and promote ethical and socially responsible innovation. Supported by an investment of approximately ?10,300 crore over five years, the initiative has already enabled the deployment of thousands of GPUs to provide affordable computing resources for startups, researchers, and enterprises. With AI applications rapidly expanding across healthcare, agriculture, financial services, manufacturing, and education, the Mission is expected to significantly enhance India’s competitiveness in the global AI ecosystem.

Therefore, India’s structural push to become a leading AI hub must be matched by urgent attention to risk management; the lesson from the early internet era is one business cannot afford to ignore. Technological revolutions that arrive with great promise often expose equally serious vulnerabilities: the rise of e?commerce and digital platforms spawned new waves of fraud, data breaches, and regulatory gaps that many companies addressed only after harm had occurred. Generative AI presents a comparable inflection point but with amplified stakes, given its ability to create convincing falsehoods, influence automated decision?making, and enable large?scale fraud at unprecedented speed Further, businesses that treat AI adoption as optional, or delay building the necessary legal, ethical, and security safeguards around it, risk repeating history’s mistakes on a far more dangerous footing. This article examines these risks across the three areas where Indian businesses must now build governance with equal urgency: the protection of confidential information and trade secrets, the intellectual property questions raised by AI-generated content across trademarks, copyrights, and personality rights, and the tightening data protection obligations under India’s evolving DPDP framework. Businesses should identify and manage the legal and operational risks of GenAI before they materialize into major crises. A proactive and comprehensive approach today is the most effective means of avoiding costly consequences tomorrow.

Table of contents

- Confidentiality
- Intellectual Property
  - Trademark
  - Copyright:
  - Personality rights
- Data Protection
- Conclusion:

Confidentiality

While much of the legal debate around GenAI has focused on copyright and trademarks, the more immediate and often overlooked risk for businesses lies in the protection of trade secrets and confidential information. Unlike other forms of intellectual property, trade secrets derive their value from remaining confidential, and a single careless disclosure through an AI platform can significantly weaken that protection.

A significant risk arises when employees input trade secrets or proprietary business information into public AI tools, whether client data, pricing models, source code, product designs, or internal methodologies. Once confidential information is shared with an external AI platform, a company’s ability to claim trade secret protection may be compromised. Courts generally assess whether the business took reasonable measures to preserve secrecy, and uncontrolled disclosure to a third-party AI service may itself demonstrate that such measures were inadequate, irrespective of the provider’s assurances regarding data retention or model training. The risk is compounded if the AI system retains or learns from user inputs, creating the possibility that confidential information could later be reflected in responses generated for unrelated users.

For Indian businesses, this concern extends beyond the loss of trade secret protection. Employees who use public AI tools to summarize confidential documents, draft legal advice, or process client information may inadvertently breach contractual confidentiality obligations, non-disclosure agreements, fiduciary duties, or professional responsibilities. Such incidents can expose organizations to regulatory scrutiny, contractual disputes, and reputational harm.

Mitigating these risks requires more than a general prohibition on AI use. Organizations should clearly identify what constitutes confidential information and trade secrets within their operations, prohibit the submission of high-risk information to public AI platforms, and incorporate these obligations into employment contracts, confidentiality agreements, and internal AI governance policies. These measures should be reinforced through employee training, technical access controls, and careful review of AI vendor terms to ensure appropriate safeguards for data handling, intellectual property ownership, and liability allocation. A well-designed AI governance framework protects valuable business information and lets organizations use AI responsibly without compromising their competitive advantage.

Intellectual Property

Trademark

Gen AI is rapidly becoming a default tool for naming, logo design, and brand creation, but these “generative marks” can quietly undermine the core promise of trademark law: distinctiveness. As models draw on vast, historic datasets, they tend to generate marks that echo existing names, looks, or concepts, eroding uniqueness and pushing brands closer to the brink of dilution and reduced distinctiveness. Even in the well?known Elliott v. Google line of cases, courts held that the public’s verb?form use of “Google” did not, by itself, prove the mark had become generic. In an AI era, however, the sheer volume of look?alike outputs raises a qualitatively different dilution risk. Famous marks are particularly vulnerable, as repeated AI?driven imitations blur the line between the original and a growing field of similar signs, weakening the mark’s ability to indicate a single commercial source.

At the same time, trademark squatters can weaponize AI’s speed and scale, churning out near?copy marks and racing to file them first in key jurisdictions, especially where “first?to?file” rules prevail. OpenAI’s “ChatGPT” mark has already faced opposition in India from Flaxxi AI Private Limited on a prior?use claim, so India’s first?to?use principle can block even globally dominant AI brands. For businesses relying on AI?assisted branding, this combination of diluted distinctiveness and AI?accelerated squatting turns trademarks from protective assets into potential liabilities unless strong human oversight and clearance searches are built in from the outset. Recent practice across Southeast Asia and China shows squatting is increasing, so companies expanding AI products internationally cannot treat trademark clearance as a one?time home?market exercise. They must file simultaneously and proactively in every jurisdiction where they intend to operate, well before a product’s public launch invites opportunistic registrations.

Copyright:

On copyright, the Getty Images v. Stability AI litigation illustrates how quickly and unpredictably AI disputes can turn on narrow technical and jurisdictional findings. Getty ultimately abandoned its primary copyright claims during trial, and Stability AI succeeded on the remaining secondary infringement issue, with the UK High Court holding that model weights are not a “copy” for copyright purposes because a trained model stores statistical parameters rather than reproductions of the underlying images. Crucially, this left unresolved the deeper question of whether training itself infringes copyright, since Getty had conceded there was no evidence of training within the court’s jurisdiction. Indian businesses should expect similarly technical, evidence?heavy, and outcome?uncertain terrain under Section 52 of the Copyright Act, 1957, which is precisely why strong vendor warranties on training provenance matter more than optimism about eventual judicial clarity.

Personality rights

Personality rights are emerging as a fast-growing flashpoint alongside copyright and trademark, as GenAI tools make it trivial to generate a person’s voice, likeness, or image without consent. Indian businesses using AI for marketing, dubbing, or synthetic media should treat an individual’s name, voice, and likeness as requiring the same clearance discipline as any registered trademark, particularly given India’s growing body of celebrity personality-rights case law even in the absence of a codified statute.

India’s IP Office could adopt a similar AI?assisted image and prior?art search mechanism as a core institutional efficiency tool rather than a convenience for applicants alone. In recent years, we have noticed the Japan Patent Office hosts “AI x Trademark: Image Search Competition,” which shows how AI talent can strengthen examination systems. The JPO deliberately used the

competition to improve its AI?based figurative mark search tool and then deployed the winning models to help examiners flag visually similar marks more efficiently. If we, as AI and IP professionals, channel our skills into building such responsible tools, AI can become a force multiplier for better trademark examination and faster, more reliable protection, rather than a source of additional risk.

Data Protection

In recent years, we recall the introduction of the GDPR, which prompted numerous jurisdictions worldwide to strengthen their data protection regimes in response to accelerating technological change and heightened privacy risks. Yet today, these very frameworks are revealing structural limitations, as generative AI systems challenge foundational assumptions that data protection laws were never designed to address. AI systems are, at their core, data-processing systems, which means data protection risk runs through nearly every other category discussed above. Recent global enforcement actions show how unforgiving this area can be. In an important reminder of the need for businesses to thoroughly understand data processing practices before deploying AI tools, the Italian data protection authority (Garante) initially fined OpenAI €15 million for GDPR violations involving ChatGPT. The regulator cited the lack of a valid legal basis for training the model on personal data, insufficient transparency toward users, and failure to notify of a data breach. However, in recent days, the Italian court has annulled the fine on procedural grounds related to jurisdiction under the GDPR's one-stop-shop mechanism, showing that enforcement outcomes in this space remain genuinely unsettled even in jurisdictions with a mature data protection framework, and businesses should not assume that a regulator's first move against an AI company will necessarily survive appeal. India's own Digital Personal Data Protection Act, 2023, is not yet fully in force, and its rules are still being operationalised, which means Indian businesses deploying AI tools that process personal data are, in effect, building compliance programs against a moving target. In my view, the law is evolving more slowly than the technology it is meant to govern, and this gap is only likely to widen. Practitioners must therefore stay closely engaged with emerging case law and enforcement patterns both in India and abroad, so that we can identify where the law currently falls short and advise our clients on the law as it actually stands, rather than as it existed at the time it was drafted.

In India, data protection has shifted from aspirational to operational with the notification of the Digital Personal Data Protection Rules, 2025, on 14 November 2025. The Rules provide much-needed clarity on implementation under the DPDP Act, including mandatory breach notification without undue delay, followed by a detailed report within 72 hours, and explicitly state that organisations cannot outsource compliance by relying on generic AI vendor terms of service. As data fiduciaries, businesses must also carefully assess cross-border transfers of personal data for training or operating models hosted abroad, given the government's retained power to impose stricter restrictions on specified countries. These developments underscore that effective AI adoption in India now demands proactive legal diligence and strong internal data governance, rather than passive reliance on third-party solutions.

Conclusion:

Taken together, confidentiality, intellectual property, data protection, and liability are four lenses on the same underlying problem: businesses are adopting AI faster than the law can define its boundaries. GenAI is a business reality that is reshaping how organizations innovate, compete, and grow. Its potential can only be fully realized when innovation is matched with sound legal governance. Businesses that proactively address upcoming challenges and regulatory compliance will be better positioned to use AI as a strategic advantage rather than a source of liability. As India's AI ecosystem continues to expand, legal practitioners, policymakers, and businesses must work together to build a framework that encourages innovation while safeguarding trust, accountability, and commercial certainty.

Related Practice Areas

Information Technology