



**Luthra *and* Luthra**  
LAW OFFICES INDIA

## **TECH LITIGATION**

*Newsletter – February 2026 Edition*





## INSIDE

- **Meity raises concerns over X Corp’s compliance with intermediary due diligence norms**
- **Judicial intervention against non-consensual AI depiction**
- **Andhra Pradesh High Court limits use of Artificial Intelligence in judicial decision-making**
- **Towards integrated Techno-Legal governance of Artificial Intelligence in India**
- **Madras High Court allows use of Artificial Intelligence software in arbitration proceedings**
- **Indian Computer Emergency Response Team’s (“CERT-IN”) critical android vulnerability advisory**
- **Supreme Court examines WhatsApp - Meta privacy policy dispute**
- **Digital stamp duty in Karnataka: legal implications of the KAVERI-2 e-Stamping framework**



## MeitY raises concerns over X Corp's compliance with intermediary due diligence norms

In early January 2026, the Ministry of Electronics and Information Technology (“MeitY”) issued a formal notice to Elon Musk’s social media platform X Corp., after reports emerged that its AI chatbot “Grok” was being misused to generate and circulate obscene, vulgar, and non-consensual images and videos of individuals. The notice was addressed to X’s designated compliance officer for India and was issued under the Information Technology Act, 2000 (“IT Act”) and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (“IT Rules”), calling upon the platform to explain its failure to prevent such content and to take immediate corrective action.

MeitY grounded its notice in Section 79 of the IT Act, which grants intermediaries a conditional safe harbour from liability, subject to compliance with due diligence requirements. The ministry specifically relied on Rule 3(1)(b)(ii) of the IT Rules, which obligates intermediaries to make reasonable efforts to ensure that their platforms are not used to host or transmit content that is “*obscene, pornographic, paedophilic, or invasive of another’s privacy, including bodily privacy*”. MeitY clarified that these obligations apply equally to AI-generated content and that the use of automated systems does not dilute statutory responsibility.

The Grok AI feature is designed to take user-provided images and generate or modify them through prompts. The notice recorded that users, including fake and anonymous accounts, had exploited Grok to generate unlawful content, indicating lapses in X’s oversight and moderation mechanisms. MeitY directed X to remove such content, take action against offending accounts, and submit a detailed Action Taken Report (ATR) outlining the measures adopted to ensure compliance and prevent recurrence of such incidents. It also warned that failure to exercise due diligence could result in withdrawal of safe harbour protection under Section 79 of the IT Act.

The notice reflects MeitY’s position that intermediaries deploying AI tools must demonstrate proactive, design-level compliance, and that adherence to the IT Act and IT Rules is mandatory for platforms operating in India.

## Judicial intervention against non-consensual AI depiction

The Hon’ble Delhi High Court, by an order dated 23 January 2026, in *Akira Desai v. Sambhawaami Studios LLP*<sup>1</sup>, granted urgent interim relief restraining the circulation and broadcast of an AI-generated film that allegedly utilised the personality and likeness of Akira Nandan, the son of the Deputy Chief Minister of Andhra Pradesh, without his consent. The order assumes importance in the evolving jurisprudence on personality rights, privacy, and misuse of generative artificial intelligence.

The Plaintiff approached the Hon’ble Court contending that Defendant 1, i.e., Sambhawaami Studios LLP had created and uploaded on YouTube a full-length AI-generated film of approximately one hour, which was promoted as the “*world’s first global AI movie*”. The film allegedly portrayed the Plaintiff in a lead

<sup>1</sup> *Akira Desai vs Sambhawaami Studios LLP*, 2026 SCC OnLine Del 283.



role by synthetically recreating his persona through artificial intelligence, without any authorisation, licence, or consent.

It was the Plaintiff's case that the impugned content amounted to a grave violation of his right to privacy and personality rights, inasmuch as the AI-generated avatar replicated his facial features, image, photograph, and overall persona with such accuracy that it created a deceptive impression of association or endorsement. The Plaintiff further argued that the Defendants had unlawfully capitalised on his identity for commercial gain, thereby infringing his right to control the commercial use of his name and likeness. The Hon'ble Delhi High Court was satisfied that a *prima facie* case had been made out and that irreparable harm would ensue if interim protection were not granted and accordingly issued an urgent *ad-interim* injunction, directing Sambhawaami Studios LLP and other unknown entities to immediately cease the creation, publication, dissemination, or sharing of any AI-generated or deepfake content that uses the Plaintiff's name, image, likeness, or identity without his express consent.

In addition to injunctive relief against the content creators, the Hon'ble Court passed directions to social media intermediaries, such as Meta Platforms, directing them to take down the infringing content and related websites identified in the plaint. The takedown is carried out under Section 79(3)(b) of the IT Act, read with Rule 3(1)(d) of the IT Rules, which mandate intermediaries to remove or disable access to unlawful content upon receiving actual knowledge through a court order, failing which they lose safe harbour protection. Further, the Hon'ble Court required the intermediaries to disclose specific account details and IP address information of the infringing entities within the prescribed time frame, thereby facilitating effective enforcement and identification of anonymous wrongdoers. While granting relief, the Hon'ble High Court placed reliance on its earlier decision in *DM Entertainment Pvt. Ltd. v. Baby Gift House*<sup>2</sup>, wherein it was held that for a claim of infringement of the right to publicity to succeed, the Plaintiff must be identifiable from the unauthorised use complained of. Applying this principle, the Court found that the AI-generated depiction in the present case had sufficiently captured the Plaintiff's distinctive attributes, making him clearly identifiable to the public.

The order reinforces the judicial position that personality rights extend to digital and AI-generated representations, and that the unauthorised synthetic recreation of an individual's persona amounts to actionable misappropriation. It also signals a growing judicial intolerance towards the misuse of generative AI technologies and marks an important step in adapting existing doctrines of privacy and publicity rights to emerging AI-driven forms of infringement, while simultaneously emphasising the role of intermediaries in promptly curbing unlawful content under court supervision.

### **Andhra Pradesh High Court limits use of Artificial Intelligence in judicial decision-making**

The Hon'ble High Court of Andhra Pradesh, in its judgment dated 21 January 2026 in *Gummadi Usha Rani & Another v. Sure Mallikarjuna Rao & Another*<sup>3</sup>, undertook a significant examination of the permissible scope and limits of the use of artificial intelligence in judicial decision-making. The ruling

<sup>2</sup> DM Entertainment Pvt. Ltd. v. Baby Gift House, 2010 SCC OnLine Del 4790

<sup>3</sup> Gummadi Usha Rani & Another vs Sure Mallikarjuna & Another, 2026 SCC OnLine AP 194



addresses an increasingly relevant concern regarding the uncritical reliance on AI-generated legal material within court proceedings and judicial orders. The matter arose out of a Civil Revision Petition filed under Article 227 of the Constitution of India, challenging an order passed by the learned Additional Junior Civil Judge, Vijayawada. The grievance before the Hon'ble High Court was that the subordinate court, while rendering the impugned order, had cited a judgment that did not exist, which was subsequently revealed to be a product of an AI-based legal research tool. The Petitioners contended that reliance on such fictitious authority vitiated the judicial order and reflected non-application of mind.

In addressing this contention, the Hon'ble High Court made important observations on the current capabilities and inherent limitations of artificial intelligence systems. The Hon'ble Court noted that, at present, AI tools may at best function as assistive technologies, capable of tasks such as data organisation, summarisation of pleadings, and retrieval of information. However, the Hon'ble Court categorically held that AI systems lack consciousness, moral reasoning, and adjudicatory discretion, and are incapable of appreciating evidence, evaluating credibility, or understanding the subtleties of human behaviour and factual context, functions that lie at the heart of judicial decision-making. The Hon'ble Court further cautioned against the uncritical adoption of AI-generated outputs in legal research and adjudication, particularly in the absence of meaningful human oversight. It was observed that most AI tools do not have access to the entire corpus of binding and persuasive legal authorities, including updated case law, local precedents, or nuanced procedural developments. Moreover, such tools may misinterpret queries, generate incomplete responses, or, as in the present case, fabricate citations.

The Hon'ble High Court highlighted the systemic harms arising from the introduction of fictitious judicial opinions into court proceedings. These practices lead to wasting limited and valuable judicial time that should be spent on deciding genuine cases, weaken the trust and credibility of judicial reasoning and deny parties the opportunity to present arguments based on real and binding legal precedents. The Court observed that relying on questionable authorities seriously undermines confidence in the justice system and creates a grave threat to the rule of law.

Notwithstanding these observations, the Hon'ble High Court declined to set aside the impugned order solely on the ground that it referred to a non-existent AI-generated citation. The Hon'ble High Court held that the determinative factor is not the citation itself, but whether the legal principles applied in the order are correct and have been correctly applied to the facts of the case. Where the impugned order reflects a proper understanding and application of settled law, the mere inclusion of an erroneous or fictitious reference does not, by itself, render the decision unsustainable. The Hon'ble High Court thus adopted a substance-over-form approach, emphasising that judicial orders must be evaluated on the correctness of the legal reasoning and conclusions reached, rather than on peripheral defects in citation. At the same time, the judgment serves as a clear cautionary note to courts and practitioners alike to exercise due diligence, verification, and intellectual responsibility when employing AI-assisted research tools.

In effect, the decision strikes a careful balance: it recognises the utility of AI as a supplementary aid, while firmly rejecting its use as a substitute for judicial reasoning or legal verification. The judgment contributes meaningfully to the emerging discourse on ethical and responsible use of artificial intelligence in the



justice delivery system, reaffirming that accountability for judicial decision-making remains unequivocally human.

### **Towards integrated Techno-Legal governance of Artificial Intelligence in India**

In January 2026, the Government of India, through the Office of the Principal Scientific Adviser, released a White Paper titled “*Strengthening AI Governance Through a Techno-Legal Framework*”, outlining India’s evolving approach to regulating artificial intelligence. The White Paper provides the policy context for a shift from purely reactive, enforcement-based legal regulation towards an integrated techno-legal model, recognising the increasing deployment of AI systems across governance, finance, healthcare, media, and public infrastructure. The White Paper identifies a core regulatory challenge, i.e., traditional legal frameworks are largely designed to respond after harm has occurred, whereas AI-related risks, such as data misuse, biased outputs, opacity, and security vulnerabilities, often arise during the design, training, and deployment stages of AI systems. To address this gap, the techno-legal approach focuses on using laws, regular oversight, internal controls and technical safety tools together, so that legal rules are built into how AI systems are designed, developed and used, rather than being applied only after a dispute arises.

India’s existing AI governance regime continues to be anchored in statutes such as the IT Act, the Digital Personal Data Protection Act, 2023, sectoral regulations issued by bodies such as the Reserve Bank of India and Securities and Exchange Board of India, and policy instruments including the India AI Governance Guidelines. While these frameworks provide baseline protections relating to privacy, security, and accountability. The White Paper acknowledges that they do not fully address operational challenges arising during data collection, model training, inference, and deployment, particularly in the case of adaptive or opaque AI systems. To bridge this gap, the techno-legal framework proposes embedding compliance and risk-management mechanisms directly into technical workflows. These include data governance protocols, privacy-enhancing technologies, audit logs, model documentation, bias and security assessments, and continuous monitoring during deployment. Such measures support legal obligations by enabling traceability, auditability, and early risk detection, thereby reducing reliance on post-deployment enforcement alone.

A key feature of the framework is its lifecycle-based orientation, applying governance controls across stages such as data use, model development, inference, and autonomous system operation. Institutionally, it emphasises coordination between government bodies, sectoral regulators, technical experts, and industry participants through mechanisms such as expert committees, AI safety institutions, incident reporting systems, and voluntary compliance programmes. Overall, the techno-legal framework reflects India’s preference for strengthening the implementation of existing legal obligations through technical safeguards, sector-specific guidance, and institutional coordination, rather than introducing a standalone AI statute. This approach seeks to balance innovation with accountability while allowing flexibility across sectors as AI technologies continue to evolve.



## Madras High Court allows use of Artificial Intelligence software in arbitration proceedings

The Hon'ble High Court of Madras ("Madras High Court"), in its order dated 28 January 2026 in the matter titled *M/s. Gammon -OJSC Mosmetrostory JV vs M/s Chennai Metro Rail Limited*<sup>4</sup> allowed regulated use of an Artificial Intelligence based algorithm called 'Superlaw Courts' for supporting court proceedings and filtering the required information from the case documents. The Madras High Court passed the order with the concurrence of the parties to the arbitration case, and after the algorithm was duly demonstrated before the Hon'ble Court, with the participation of the counsel.

As per a note circulated on the directions of the Madras High Court, Superlaw Courts is a computer-assisted system designed to help professionals locate, organise and understand information strictly within the documents placed before it for a particular matter. It was further averred in the note that the system is intended to reduce the time and effort involved in manual searching and cross-referencing of voluminous documents.

The Hon'ble Madras High Court outlined that the AI software can be used only within strict limits. The Hon'ble Court also noted that the system works solely on the documents submitted in the case and does not rely on outside sources, general knowledge, or any material beyond the case record. It was also clarified that the AI Tools are not meant to replace legal reasoning or judicial decision-making. Further, Hon'ble Justice N. Anand Venkatesh stressed the importance of transparency and directed that all interactions with the AI systems, either by Lawyers or the court, must be recorded through a separate link, which would allow anyone to check how and to what extent the algorithm was used.

The Hon'ble High Court took note of the fact that it would be for the first time that the assistance of AI would be used for preparing a draft order by the Court, containing the facts of the case and the arguments put forth by both sides, covering the pleadings, evidence, and findings of the arbitral tribunal. This is a watershed moment and would significantly reshape courtroom practice to the extent of record management and organization.

## Indian Computer Emergency Response Team's ("CERT-IN") critical android vulnerability advisory

The Indian Computer Emergency Response Team ("CERT-In") issued a **critical vulnerability advisory** ("CIVN-2026-0016") relating to Android devices on 05 January 2026, warning that unknown sources could be exploited to gain unauthorised control. The advisory is part of CERT-In's ongoing effort to warn users and organizations about serious cybersecurity weaknesses that could affect the functioning and data security of systems that depend on Android-based technology. From a regulatory perspective, the advisory triggers compliance obligations under the **IT Act**. Affected entities, including intermediaries, service providers, data centres, bodies corporate and government organisations are required to take prompt mitigation measures, preserve relevant logs and evidence, and assess whether the incident falls within the

---

<sup>4</sup> *M/s. Gammon -OJSC Mosmetrostory JV vs M/s Chennai Metro Rail Limited*, Arb O.P(COM.DIV.) No. 247 of 20272



category of reportable cyber incidents. Where applicable, incidents must be reported to CERT-IN within the prescribed timelines, accompanied by documented remediation steps.

Organisations using Android platforms should therefore prioritise the deployment of vendor recommended security patches and maintain clear records of vulnerability assessment, patch implementation and internal escalation. Technical remediation must be coupled with procedural compliance, including adherence to reporting formats, points-of-contact requirements and log-retention obligations prescribed by CERT-In. The advisory highlights the increasing regulatory focus on proactive cyber-risk management and accountability. Enterprises that respond swiftly, document remediation comprehensively, and align technical responses with statutory reporting obligations will be better positioned to manage regulatory exposure, contractual risk and reputational impact arising from cybersecurity incidents.

### **Supreme Court examines WhatsApp - Meta privacy policy dispute**

On 03 February 2026, the Supreme Court of India expressed constitutional concerns while hearing a batch of appeals filed by Meta Platforms Inc. and WhatsApp LLC, along with an appeal by the Competition Commission of India (“CCI”), arising out of WhatsApp’s 2021 privacy policy. The matter was heard by three-judge bench led by Chief Justice Surya Kant, and comprising Justices Joymalya Bagchi and Vipul M. Pancholi. During the hearing, the Hon’ble Court made observations regarding the companies’ data-sharing practices and categorically observed that it would not permit the sharing of user data in violation of Indian law. Emphasizing that the right to privacy is a constitutionally protected right, the Hon’ble Court remarked that privacy cannot be diluted in the name of commercial data sharing.

The appeals stem from CCI’s November 2024 order holding that WhatsApp had leveraged its dominant position by linking continued access to its messaging service on acceptance of expanded data sharing arrangements within the Meta entities, and had imposed a penalty of ₹213.14 crore. While the National Company Law Appellate Tribunal upheld the penalty in November 2025, it set aside certain findings relating to advertising-related data sharing, prompting appeals by both the companies and the CCI before the Hon’ble Supreme Court.

The Bench noted the imbalance of power between digital platforms and users, observing that the opt-out mechanisms were inaccessible to ordinary users, particularly those lacking technological or legal literacy. The Court noted that users’ dependence on WhatsApp raises certain concerns regarding behavioral data, user trends and digital “*footprints*” being allegedly monetized within the Meta ecosystem. The Court also directed WhatsApp to file a detailed affidavit explaining the operation of its privacy policy and the mechanics of data sharing and ordered that the Union Government be impleaded as a party to the proceedings.

Signaling the possibility of interim directions restraining data sharing, the Court made it clear that commercial interests cannot override constitutional rights, even where services are offered free of cost.



## Digital stamp duty in Karnataka: legal implications of the KAVERI-2 e-Stamping framework

On 16 January 2026, the Government of Karnataka formally notified the KAVERI-2 module as the State's authorised "*Digital e-Stamp Application*" under the Karnataka Stamp (Digital e-Stamp) Rules, 2025, and published in the Karnataka Gazette on 19 January 2026. While presented as a technological reform, this development represents a structural shift in how stamp duty is assessed, evidenced, and enforced, replacing paper-based instruments with a system-generated, data-native compliance framework. By moving stamp duty from physical stamp paper to a government-controlled digital system, the decisive element of compliance shifts from possession of stamped instruments to the existence and traceability of records within an official database. Legal validity and admissibility are now anchored in system provenance rather than physical form. This reallocation of compliance also redistributes legal risk, with traditional safeguards, such as vendor controls and manual scrutiny by sub-registrars, being embedded into software through instrument-specific stamping, real-time valuation linkage, and immutable audit trails. As a result, sub-registrars increasingly function as verifiers of system compliance rather than gatekeepers of stamping.

The shift to digital stamping under KAVERI-2 has a clear impact on how legal transactions are handled. Mistakes in stamp duty compliance are likely to be addressed much earlier, which means lawyers, in-house legal teams, banks, and document preparers will need to be more careful from the very beginning. The order in which documents are executed, how corrections are made digitally, and how system records are preserved will become very important, since any changes made later will be clearly visible in the digital trail. Courts are also likely to presume that digitally stamped documents are valid, making it harder to challenge them on technical grounds and pushing disputes to focus on the accuracy and reliability of the digital system instead of paper defects. While initial issues such as mixed use of old and new systems, technical glitches, and early court challenges are expected.. Overall, KAVERI-2 marks a major shift in stamp duty compliance in Karnataka, requiring legal professionals to combine drafting skills with technical understanding and readiness to rely on digital records as key legal evidence.



*This newsletter is only for general informational purposes, and nothing in this edition of the newsletter could possibly constitute legal advice (which can only be given after being formally engaged and familiarizing ourselves with all the relevant facts). However, should you have any queries, require any assistance, or clarifications with regard to anything contained in this newsletter, please feel free to contact Sanjay Kumar / Abhishek Kumar Singh, at the below mentioned coordinates. © Luthra and Luthra Law Offices India 2025. All rights reserved.*

## **KEY CONTACTS**



### **SANJAY KUMAR**

Senior Partner

Email - [sjkumar@LUTHRA.COM](mailto:sjkumar@LUTHRA.COM)



### **ABHISHEK KUMAR SINGH**

Partner

Email - [abhishekks@luthra.com](mailto:abhishekks@luthra.com)

## **OFFICES**



### **NEW DELHI**

1st and 9th Floors, Ashoka Estate,  
 24 Barakhamba Road, New Delhi - 110 001  
 T: +91 11 4121 5100  
 F: +91 11 2372 3909  
 E: [delhi@luthra.com](mailto:delhi@luthra.com)



### **MUMBAI**

20th Floor, Indiabulls Finance Center,  
 Tower 2 Unit A2, Elphinstone Road,  
 Senapati Bapat Marg, Mumbai - 400 013  
 T: +91 22 4354 7000  
 F: +91 22 6630 3700  
 E: [mumbai@luthra.com](mailto:mumbai@luthra.com)



### **BENGALURU**

3rd Floor, Onyx Centre, No. 5, Museum Road,  
 Bengaluru - 560 001  
 T: +91 80 4112 2800 / +91 80 4165 9245  
 F: +91 80 4112 2332  
 E: [bengaluru@luthra.com](mailto:bengaluru@luthra.com)



### **HYDERABAD**

Serene Towers,  
 House No. 8-2-623/A,  
 Road No. 10, Banjara Hills,  
 Hyderabad, Telangana - 500034  
 T: +91 40 7969 6162  
 E: [hyderabad@luthra.com](mailto:hyderabad@luthra.com)



### **CHENNAI**

Prestige Palladium Bayan,  
 8th Floor, Greams Road, Nungambakkam Division,  
 Egmore, Chennai - 600 006,  
 Tamil Nadu  
 T: +91 95604 88155  
 E: [chennai@luthra.com](mailto:chennai@luthra.com)