Keynote Address by

Hon'ble Ms. Justice Hima Kohli,

Former Judge, Supreme Court of India,

At the **Justice S.C. Agarwal Memorial Lecture - Session 2026–27**

at **Kanoria School of Law for Women, Jaipur**

Organised by Rajasthan Education Trust (*founded by:* Shri Chiranjilal Agrawal, Advocate)

28th February, 2026 (Saturday) at 11:00 a.m.

TITLE: <u>Technology and the Legal System: *from Tech Laws to Tech in Law*</u>

5000 words; 40 minutes

[Present : -

Rajasthan Education Trust : Sh. Dinesh Ji (President), Justice V.S. Dave (Trustee), Justice JK Ranka (Trustee)

Kanoria School of Law for Women, Jaipur : Dr. Rashmi Chaturvedi (Director), Dr. Vartika Arora (Principal)]

Introduction

1. Distinguished members of the Rajasthan Education Trust, respected members of the faculty, dear students of the Kanodia School of Law for Women, ladies and gentlemen. A very good morning to all. It gives me immense pleasure to address this gathering of young law students, particularly in an institution dedicated to legal education of women. I am happy to see the future of the legal profession sitting right before us today.

2. I often reflect on how differently the law presented itself when I was a young law student. At that time, research required patience, physical effort, and perseverance. We used to spend long hours in libraries, pouring into commentaries and digests. Technology did exist, but it did not define our engagement with law. Today, many of you encounter the law first through a digital interface. Judgments are downloaded, filings are uploaded, hearings are streamed, and disputes are sometimes resolved entirely online. This shift is not merely technological. It is jurisprudential. It alters how rights are exercised, how obligations are enforced, and how justice is accessed.

3. Over the years, initially as a legal practitioner and later on as a Judge of the Supreme Court, I have witnessed how technological questions have slowly but steadily moved from the periphery to the centre of the constitutional discourse. Electronic evidence, digital speech, data protection, internet shutdowns, intermediary liability - these were no longer matters of academic curiosity. They have become pressing constitutional challenges.

4. It is against this backdrop that I propose to explore the theme for today's lecture – **'Technology and the Legal System: *from Tech Laws to Tech in Law*'**. Broadly speaking, there are two dimensions to this evolving relationship between technology and the legal system, that unfold through two interconnected strands.

5. First, technology as a subject of law, i.e. how we regulate digital conduct, protect rights, and impose accountability. The first part of my address proposes to trace the contours of India's technology laws: the statutory and judicial responses fashioned to regulate digital conduct, safeguard individual rights, and address the emerging vulnerabilities of cyberspace.

6. The second part shall deal with technology as an instrument of law, i.e. how it transforms judicial administration and dispute resolution. This section shall turn its gaze inwards, to examine how technology has entered the portals of the judicial system itself acting as a tool to render justice, supporting administration and governance, and expediting adjudication without displacing human empathy that lies at the very core of justice dispensation.

7. Together, these two strands - technology governed by the rule of law, and technology harnessed in the service of law - frame the theme of my address today.

The Constitutional Challenge of Digital Scale

8. Technology has truly become an integral facet of our lives. Today, the internet is the default doorway to our daily life. We purchase air tickets, pay taxes, and settle utility bills without leaving our desks, transforming what once demanded physical presence into digital ease. This pervasive integration is borne out by empirical data: by the end of 2025, more than **six billion** people were connected to the internet, with India alone accounting for nearly **one billion** users[1]. What was once an exception is now the rule, and what was once experimental has become routine.

9. However, ubiquity brings complexity. The scale of technological change that we are witnessing today places new demands upon law. As digital platforms, data-driven systems, and artificial intelligence increasingly shape economic activity,

[1] IAMAI and Kantar, "Internet in India Report 2025" (2026)

social interaction, and public administration, the law is required to govern conduct in areas that are often borderless, fast-moving, and technologically complex. The Constitution, that was drafted in an age of ink and paper, now governs a society that increasingly lives and communicates in the cloud. The law must therefore perform a delicate balancing act - encouraging innovation while safeguarding constitutional guarantees.

10. It is in response to this emerging digital landscape that our nation's formal engagement with technological regulation began.

The Evolution of Technology Law in India

11. The journey of our country into digital regulation commenced with the enactment of the **Information Technology Act, 2000**[2]. The statute was conceived as an enabling framework, designed primarily to accord legal recognition to electronic records and digital signatures, and to facilitate the growth of electronic commerce and e-governance. At the time of its enactment, internet in India was largely

[2] In short, '**The IT Act**'

transactional in character and modest in scale. It had not yet assumed the expansive, data-driven character that defines it today.

12. At that time, the law was not grappling with social media platforms, viral misinformation, algorithmic amplification, or large-scale data surveillance. Instead, its focus was on foundational questions. As for example, could an electronic communication constitute a valid contract? Could a digital signature substitute handwritten authentication? Could governmental processes migrate into electronic form without compromising legal validity? The Act answered these questions in the affirmative. Yet it did so within the technological imagination of its time. It did not (and perhaps could not) foresee the velocity and scale of digital transformation that would follow.

13. As technology evolved far beyond those horizons, law was compelled to expand its vision. The focus gradually shifted from merely recognising electronic transactions to regulating intermediaries, addressing cyber offences, and engaging with deeper questions of rights, accountability, and institutional

power in the digital sphere. What began as a facilitative statute evolved, over time, into a more regulatory and rights-sensitive framework. In this transition, the judiciary has played a vital interpretative role.

14. ***Shreya Singhal v. Union of India***[3] was a case where the Petitioner, a law student approached the Supreme Court challenging the constitutionality of **Section 66A** of the **IT Act** that criminalized sending "offensive" or "annoying" messages via computer resources or other devices carrying imprisonment upto three years. While striking down **Section 66A** of the **IT Act** as a violation of **Article 19(1)(a)** (freedom of speech), the Supreme Court reaffirmed that speech does not lose its constitutional protection merely because it is expressed online. The Court emphasised that vague and overbroad restrictions on expression have no place in a constitutional democracy. Equally significant was the clarification that intermediaries could not assume the role of private censors without judicial oversight. Content could be removed only on to a court order or a lawful

[3] (2015) 5 SCC 1

direction issued by the government. In doing so, the Court ensured that digital regulation remained anchored in the constitutional framework.

15. A similar emphasis on doctrinal clarity emerged in ***Sharat Babu Digumarti v. Government of NCT of Delhi***[4]. In this case, the Supreme Court clarified that where offences concern electronic records, the I.T. Act operates as a special statute and prevails over the general provisions of the Indian Penal Code. This interpretation preserved coherence in cyber prosecutions and prevented fragmentation across overlapping statutory regimes. Read alongside ***Shreya Singhal*** (*supra*), the decision reflects a consistent judicial approach - that regulation in cyberspace must rest upon principled statutory interpretation and constitutional discipline, rather than on *ad hoc* enforcement.

16. Courts were also required to address the jurisdictional dilemmas presented by a borderless internet. In the early years, mere accessibility of a website within a particular territorial

[4] (2017) 2 SCC 18

jurisdiction was sometimes treated as sufficient to confer jurisdiction on a particular State High Court. Over time, this approach matured. Courts increasingly required evidence of purposeful targeting of users within its jurisdiction before entertaining a petition. This refinement reflects a recognition that digital presence alone cannot justify universal adjudicatory reach.

17. The **2008 amendments** to the **IT Act** introduced conditional safe harbour under **Section 79** that protects intermediaries from liability for Third party content (e.g. social media, e-commerce sites) and expanded the definition cyber offences. Yet concerns about overbroad private censorship persisted. In ***Google India Pvt. Ltd. v. Visaka Industries Ltd.***[5] the Supreme Court of India reaffirmed that "actual knowledge" under **Section 79** arises only on receipt of a court order or government notification. Intermediaries cannot be compelled to remove content merely on the basis of private complaints. By reinforcing the standard laid down in ***Shreya Singhal*** (*supra*),

[5] 2019 SCC OnLine SC 1587

the Court sought to curb arbitrary takedowns and protect online speech from excessive private censorship.

18. As digital platforms began operating over the years at unprecedented scale, courts were required to deal with the limits of territorial remedies themselves. In ***Swami Ramdev v. Facebook Inc.***[6], the Delhi High Court held that where unlawful content originates in India or is directed at Indian users, platforms may be required to remove it globally, not merely restrict access within national boundaries. Reason being that, in a medium without borders, geographically confined remedies risked rendering judicial orders ineffective. This decision underscores the evolving complexities of cross-border enforcement in digital spaces.

19. This evolving understanding culminated in the enactment of the **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.** The Rules recognise that digital platforms are no longer passive conduits. They curate, amplify, and monetise speech. Regulatory obligations

[6] 2019 SCC OnLine Del 10701

have therefore been calibrated to scale. Significant Social Media Intermediaries have been subjected to enhanced compliance requirements, including appointment of resident grievance officers and periodic transparency reporting.

20. The framework now acknowledges a conceptual distinction between the platform, which facilitates communication, and the publisher, who shapes content. For a long time, the law has regulated the highway while leaving the driver comparatively untouched. As digital news portals and streaming platforms began to rival traditional media in influence, this imbalance required recalibration. **The Digital Media Ethics Code** sought to address it through structured transparency and responsible self-regulation, rather than censorship.

21. The regulatory framework has continued to evolve. The **amendments to the IT Rules notified on 10 February 2026** reflect a further development, particularly in response to artificial intelligence and deepfake technologies. In an era where artificial intelligence can replicate voice, image, and likeness with unsettling accuracy, authenticity itself becomes a matter of legal concern. **The Rules** now recognise "*synthetically*

generated information" and impose obligations on intermediaries to deploy reasonable and proportionate technical measures to prevent unlawful AI-generated content. Where such content is permissible, it must be clearly and prominently labelled, accompanied by metadata or provenance markers to ensure traceability. Significant intermediaries are also required to obtain user declarations in relation to synthetic content. These measures signal a shift from reactive moderation to anticipatory regulation. In an era where artificial intelligence can replicate voice, image, and likeness with unsettling accuracy, authenticity itself becomes a matter of legal concern.

22. Viewed in its entirety, the evolution of technology law in India reflects a gradual but steady movement - from facilitation to regulation, and from regulation to constitutional calibration. What began as a framework to validate electronic transactions has matured into a regime attentive to platform power, cross-border complexity, and now the integrity of digital content itself. The underlying principle remains constant: technological expansion must be accompanied by corresponding legal

responsibility, and innovation must remain subject to constitutional values.

Cybercrimes: Nature, Scale and Legal Responses

23. Even as the law strengthens protections for autonomy and data rights, it must confront a parallel reality - the rapid digitisation of crime. The technologies that enable connection and convenience have also enabled deception at a large scale.

24. Today, cybercrime represents a convergence of technological sophistication and psychological manipulation. Ransomware attacks can disable critical infrastructure. AI-driven phishing schemes mimic trusted voices and institutions. Fraudulent investment platforms exploit digital confidence. Deepfakes are deployed for blackmail and misinformation. These are not entirely new offences in substance, but they are new in form and reach. They exploit anonymity, speed, and the absence of territorial boundaries.

25. For example, in recent months, we have witnessed a disturbing phenomenon described as “digital arrests”, where frightened citizens receive calls from fraudsters impersonating police or investigative agencies, are told that they are under

investigation for grave offences and are coerced into transferring money to "avoid arrest." It is a chilling inversion of constitutional authority: the language of law used as an instrument of fear. It is not merely cyber nuisance, but a grave assault on public trust and financial security.

26. Taking *suo motu* cognisance, the Supreme Court while describing these scams as nothing short of "robbery and dacoity", observed that over 54000 crore rupees have been siphoned off through such frauds from April 2021 to November 2025. Recognising the gravity of these offences, the Supreme Court further issued binding directions to the Authorities to implement a Standard Operating Procedure nationwide.

27. In a recent matter before the Supreme Court of India[7], an 82-year-old man living alone became the victim of what has been described as one of the largest individual digital-fraud cases in India. Cybercriminals allegedly impersonated Mumbai Police officials and telecom authorities, sending him forged Supreme Court and RBI orders through WhatsApp messages and video

[7] https://lawbeat.in/top-stories/supreme-court-issues-notice-to-centre-rbi-cbi-over-229-crore-digital-arrest-scam-targeting-82-yr-old-man-1561115

calls. Under relentless psychological pressure and threats of arrest and seizure of property, he was coerced into transferring his life savings amounting to over ₹22 crore.

28. This episode is a stark reminder that digital fraud today is not merely technological in execution, but profoundly human in its impact, often targeting those who are most vulnerable and least equipped to navigate a rapidly digitising world. We must pause to reflect on the human cost that lies behind these staggering numbers — elderly parents losing the savings of a lifetime, young professionals watching years of earnings disappear within hours, and families left with a lingering sense of shame, fear, and helplessness. In many instances such as the one described, fraudsters have gone so far as to forge court orders and misuse the names of constitutional authorities, creating an atmosphere where citizens begin to doubt not only digital systems but even the institutions meant to protect them. It is for this reason that coordinated national action has become imperative. In a constitutional democracy, no citizen should ever be made to feel that their liberty can be negotiated through

a screen or purchased through a bank transfer; the authority of law must always rest on due process, transparency, and trust.

29. Empirical data confirms that this is not a matter of sporadic occurrence. **The India Cyber Threat Report 2025** records over **369 million malware detections** in a single year across more than **8.4 million endpoints** - amounting to hundreds of hostile cyber incidents every minute. The growing prevalence of behaviour-based and zero-day attacks demonstrates the increasing adaptability of malicious actors, while the sectoral concentration of attacks in healthcare, banking, and hospitality highlights the immediate human and economic consequences of disruption. The geographic spread of malware detections in Tier-2 cities such as Surat, Jaipur, and Ahmedabad further illustrates that digital vulnerability expands as rapidly as digital penetration.

30. [Criminal justice statistics mirror this pattern: in 2023 alone, over 86,000 cybercrime cases were registered nationwide, with financial frauds - including identity theft, online banking scams, OTP-based deception, and card fraud - constituting a substantial majority. Yet charge-sheeting rates remain modest,

reflecting the complexities of attribution, volatile electronic evidence, and cross-border data dependencies. What emerges is not merely an increase in reported offences, but a structural transformation in how crime is conceived, executed, and concealed in the digital age.]

31. In response, the statutory framework assumes renewed importance. The **IT Act** criminalises unauthorised access and interference with computer systems under **Section 66 read with Section 43**, capturing conduct ranging from basic hacking to sophisticated ransomware attacks. **Sections 66B, 66C, and 66D** address offences of receiving stolen computer resources, identity theft, and cheating by personation - provisions that now underpin prosecutions for phishing scams, SIM-swapping frauds, and OTP-based financial crimes. **Section 66E** protects bodily and informational privacy by criminalising the non-consensual capture or transmission of private images, while **Sections 67, 67A, and 67B** deal with the publication and transmission of obscene material and Child Sexual Abuse Material (CSAM). At the extreme end lies **Section 66F**, which penalises cyber-terrorism, recognising that digital intrusions

can threaten national security and critical infrastructure. These provisions reflect the attempt of the legislature to translate familiar categories of criminal harm -fraud, coercion, obscenity, and violence - into the language of networks and data.

32. The **Bharatiya Nyaya Sanhita, 2023 (BNS)**, ensures that digital form does not dilute liability for traditional crimes, and recognises organised cybercrime as a structured offence capable of targeting networks rather than merely individual actors. A significant evolution is **Section 111**, which defines **'Organised Crime'** to specifically include economic offences and cyber-crimes carried out by syndicates. This allows law enforcers to target the *network* of Mule Accounts and handlers rather than just the individual foot-soldier. This dual-track framework also permits the prosecutors to invoke the **IT Act** for the technological act and the **BNS** for the substantive harm - ensuring that digital form does not become a shield against accountability.

33. Complementing these penal measures is the **Digital Personal Data Protection Act, 2023**. Unlike the IT Act and the BNS, the DPDP Act adopts a regulatory approach by

establishing a civil and a regulatory regime. By imposing obligations upon Data Fiduciaries and prescribing substantial monetary penalties, it recognises that digital harm often arises from institutional neglect as much as individual wrongdoing. Violations attract significant monetary penalties - capped at **₹250 crore per instance** - adjudicated by the **Data Protection Board of India**. By shifting the focus from punishment to prevention, the DPDP Act supplements criminal law with a model of deterrence grounded in accountability.

34. The effectiveness of these statutory provisions ultimately depends on the machinery of investigation. India has progressively built a specialised architecture, anchored by the **National Cyber Crime Reporting Portal (NCRP)** and the '**1930' Helpline**. This system operates on the **Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS)**, which is designed to freeze fraudulent funds during the 'Golden Hour' , before they leave the banking system.

35. Yet, this entire workflow remains fraught with challenges. Electronic evidence is volatile, attribution of digital identity is complex, and data often resides in servers located outside India.

Jurisdictional questions, both territorial and subject-matter, frequently complicate prosecutions. These constraints explain the gap between the rates of registration and conviction. They also underline a central truth: that robust laws are necessary, but they are not sufficient. Effective enforcement demands technical capacity, inter-agency coordination, and international cooperation.

36. Even as the law strengthens its penal and enforcement architecture to respond to digital wrongdoing, it must confront a more fundamental constitutional question. The very technologies that enable surveillance, detection, and prosecution are also capable of intruding into the most intimate spheres of individual life. The challenge, therefore, is not merely how the law punishes misuse of technology, but how it regulates the use of technology itself. It is at this intersection - between power and restraint, efficiency and dignity - that the discourse inevitably turns to the right to privacy.

Right to Privacy in the Digital Age

37. Regulation of technology in a constitutional democracy cannot be value-neutral. It must draw its legitimacy from the

foundational guarantees of the Constitution that secures liberty, dignity, and autonomy. **Article 14** operates as a bulwark against arbitrariness, **Article 19** protects the freedom to think, speak, and receive information, and **Article 21** safeguards the individual against disproportionate intrusion into personal life. Technology may transform the means through which power is exercised, but constitutional values remain constant. They do not yield to innovation; they discipline it.

38. The most authoritative articulation of these principles has come in the case of ***Justice K.S. Puttaswamy (Retd.) v. Union of India***[8], a watershed moment in our constitutional history. In a unanimous decision, a nine-Judges Bench has recognised that privacy is not merely as a fundamental right, but a natural and inherent attribute of human existence – Therefore, not a concession by the State. The Court held that privacy lies at the core of life and personal liberty under **Article 21**, while simultaneously infusing the freedoms guaranteed under **Article 19** and the guarantee of equality under **Article 14**. Crucially, the judgment rejected the argument that privacy should be

[8] 2017 (10) SCC 1

confined to mere secrecy or the right to be left alone. Instead, it articulated privacy as informational self-determination - the right of the individual to control the collection, use, and dissemination of personal data. To guard this right against arbitrary State action, the Court laid down a rigorous **three-fold test**: legality, necessity, and proportionality. In doing so, it relocated privacy from the periphery to the very centre of constitutional protection, laying the moral and legal foundation for data protection framework in India.

39. The **Digital Personal Data Protection Act, 2023**[9] translates this constitutional vision into statutory form. It defines consent with precision, vests enforceable rights in Data Principals, and introduces institutional mechanisms of accountability. The framework recognises that trust is foundational to digital participation.

[Regulation of Data and Digital Platforms

40. The protection of personal data cannot be viewed in isolation from those who collect, process, and monetise it. Once the

[9] The DPDP Act 2023 is partially in force and moving through a phased implementation. While the Act received Presidential assent in August 2023, its full operationalisation began with the notification of the **DPDP Rules, 2025 on November 14, 2025**.

individual is recognised as a rights-bearing Data Principal, the constitutional inquiry necessarily extends to the responsibilities of digital platforms and intermediaries that exercise unprecedented control over data, visibility, and attention. The law has therefore shifted from addressing isolated misconduct to confronting the structural power of intermediaries who curate content, influence attention, and shape behaviour. Safe harbour under the IT Act and the 2021 Guidelines is no longer unconditional; immunity is now contingent upon due diligence, reflecting a calibrated balance between fostering innovation and ensuring accountability, particularly through heightened obligations for Significant Social Media Intermediaries.

41. Parallel to this content-based regulation, the Digital Personal Data Protection Act, 2023, establishes a data-centric framework that reimagines intermediaries as Data Fiduciaries bound by duties of care extending beyond consent to include data security, purpose limitation, and accuracy, acknowledging the limits of consent in contexts of informational asymmetry. Crucially, this accountability is substantive rather than symbolic: the Act empowers the Data Protection Board to

impose significant monetary penalties, signalling a decisive move from criminal sanction to institutional responsibility and affirming that innovation must remain anchored in transparency, restraint, and trust.]

Technology in Law and Justice Delivery

42. Thus far, I have spoken of technology as the subject of regulation. Yet technology has also transformed the functioning of the legal system itself.

43. During the COVID-19 pandemic, technology ensured continuity in judicial functioning. When physical courtrooms across the country fell silent, the justice system did not come to a standstill. Instead, it reinvented itself in real time. Judges, court staff, and members of the Bar worked almost round the clock to ensure continuity of judicial functioning. Physical files were rapidly converted into digital records, voluminous paper books were scanned into PDF compilations, and entire case histories were uploaded onto virtual platforms. Court functioning, in many places, became nearly paperless and, in spirit, almost 24×7. What might have once taken weeks of

logistical preparation was achieved within days through collective institutional effort.

44. Virtual courts dissolved geographical barriers that had long shaped access to justice. Lawyers and litigants from any part of the country could participate in these virtual hearings. Proceedings were no longer confined to those who could physically enter a courtroom.

45. At the same time, this transition underscored the importance of institutional safeguards to prevent digital exclusion. Initiatives such as e-Seva Kendras assumed critical importance, providing assisted access to litigants who lacked devices, stable internet, or digital literacy. The objective was clear: technology must expand access, not narrow it. A digital court could not become an exclusive court.

46. [**Personal Example** - I recall several instances from that period that vividly demonstrate how profoundly the system adapted. In Delhi, we constituted virtual benches where my brother judge joined proceedings from Chennai while I participated from Delhi, seamlessly hearing matters as though we were seated side by side on the same Bench. The discipline,

decorum, and seriousness of judicial work remained intact, even though the courtroom was now virtual.

47. Similarly, while I was serving as Chief Justice of the Telangana High Court, matters were heard by a Bench where one learned judge joined from Chicago and another from Hyderabad. Across continents and time zones, the court assembled, arguments were heard, and orders were passed without interruption. These were not technological experiments for novelty's sake; they were living demonstrations of institutional resilience. They showed that with the aid of digital tools, the justice system could remain accessible, responsive, and steadfast—even in the midst of unprecedented disruption.]

Digital Transformation of Indian Courts

48. However, this resilience was not accidental. Implemented in phases under the stewardship of the Chief Justice of India and in coordination with High Courts and the Ministry of Law & Justice, **Phase I** focused on basic computerisation and the nationwide rollout of the Case Information System, creating uniform digital records across thousands of courts. **Phase II** marked a shift to automation through e-filing, e-payments,

large-scale video conferencing, and the operationalisation of the National Judicial Data Grid, enabling crores of virtual hearings and unprecedented transparency in pendency data. **Phase III** now moves towards fully digital and paperless courts.

49. Districts such as Kalpetta in Kerala exemplify the possibilities of AI-assisted, file-free courtrooms supported by fully integrated digital infrastructure, where judges work with digitised case records, automated systems streamline workflow, and the traditional physical burden of files has virtually disappeared.

50. Today, technology supports almost every stage of litigation, from electronic institution of cases and digital vakalatnamas to automated case tracking through unique identifiers and QR-based systems[10]. Even traditionally paper-based records are being integrated through OCR[11] enabled digitisation, enabling faster retrieval and paperless hearings.

---

[10] Through the e-Courts portal, cases filed electronically are instantly entered into the Case Information System (CIS). Every case is assigned a unique 16-digit CNR (Case Number Record) and a QR code for easy tracking.

[11] Optical Character Recognition

51. Automated notifications now inform parties of listings and orders. Digital cause lists and display boards provide real-time updates. The live display boards automatically refresh, showing court numbers, case numbers, and listed items in real time or near-real time.

52. Video conferencing enables participation across geographical boundaries, reducing time and cost for litigants and lawyers alike. Several courts have also experimented with hybrid courtrooms, where proceedings can take place simultaneously in physical and virtual modes.

53. Judgment search portals[12] now provide free public access to judicial decisions across courts, allowing structured searches by statute, subject, or keywords. In 25 High Courts, large "**Justice Clocks**" have been installed, with screens displaying live and transparent data of the cases filed, pending, and disposed of.

54. Speech-to-text tools assist judges in real-time transcription, saving judicial time and improving record accuracy, and Case

[12] Judgment Search Portal has been launched under the eCourts Project

Information Systems allow judges to monitor pendency and manage their dockets more effectively.

55. For students entering the profession, these developments have practical implications. Advocacy today requires clarity, preparation, and precision, particularly in written submissions. No digital platform can compensate for unclear thinking or imprecise drafting. At the same time, familiarity with digital tools is now an integral part of professional competence.

Pitfalls of Artificial Intelligence

56. As we increasingly integrate artificial intelligence into legal research, drafting, and adjudication, it is also important to recognise that technology, while powerful, is not infallible. Generative AI systems can produce responses that appear authoritative and convincing, yet may be entirely fabricated, a phenomenon now widely described as "AI hallucination."

57. Since we are discussing technology as an instrument of law, we must also confront its pitfalls with honesty. Artificial intelligence can accelerate research, assist in drafting, and improve access to justice, but it cannot replace professional judgment, ethical responsibility, or human verification. The

danger lies not in the technology itself, but in over-reliance upon it without scrutiny. For young students such as you, the temptation to treat AI outputs as authoritative can be strong; yet duty demands that every citation be verified, every precedent authenticated, and every submission carefully examined.

58. Courts across jurisdictions are being confronted with instances where lawyers have relied on AI-generated material containing non-existent precedents, distorted quotations, and even imaginary judgments. What makes this particularly dangerous in the legal field is that the authority of law rests heavily on precedent and citation. In a profession where authenticity and accuracy are foundational, the unregulated and blind use of AI can transform a tool of assistance into a source of misinformation.

59. Recent incidents from both India and the United States illustrate these risks vividly. In the United States, the case of *Mata v. Avianca*[13] saw attorneys sanctioned after submitting a legal brief containing fictitious cases generated by an AI chatbot.

---

[13] 678 F. Supp. 3d 443

In *Amarsingh v. Frontier Airlines*[14], the 10th Circuit Court of Appeals ordered a lawyer to pay penalties for submitting filings with fabricated case references produced through AI tools.

60. Indian courts, too, have to deal with this emerging challenge. The Supreme Court has expressed serious concerns about petitions being filed with the assistance of AI tools that contain fabricated case citations and misleading quotations, describing such practices as "alarming".

61. In short, technology must remain an aid to legal reasoning, not a substitute for it. The challenge is not whether to use artificial intelligence, but how to use it responsibly. We must ensure that in our pursuit of efficiency, we do not compromise the accuracy, integrity, and trust upon which the justice system ultimately rests. Digital tools do assist in decision-making, but they cannot replace the human thought process. Judicial discretion, reasoning, and constitutional interpretation continue to remain human functions. Efficiency is desirable, but it can never come at the cost of fairness or of due process.

[14] 2026 WL 352016 (10th Cir)

Closing Remarks

62. The strength of any legal system is not in its tools, but in its temperament. Technology will continue to evolve - faster than statutes, faster than precedents, and perhaps even faster than our imagination. But the enduring task of law remains constant: to balance power with restraint, innovation with accountability, and efficiency with fairness.

63. To you young students I say that you will inherit a profession transformed by artificial intelligence, digital courts, and global networks. Yet the essence of your role will remain unchanged. You will be called upon to think clearly, argue honestly, and uphold constitutional values in environments that may look very different from the courtrooms of the past. Technology may alter the medium, but justice remains a constant human endeavour. As long as it is guided by the conscience, human reasoning, and the principles laid down in our Constitution, the rule of law will endure - in any age, in any form, and in any circumstance.

64. Thank you for your patience.