NATIONAL JUDICIAL ACADEMY

NATIONAL CONFERENCE FOR HIGH COURT JUSTICES ON CYBER LAW & AI

[P-1462]

11TH & 12TH OCTOBER 2025

DR. SUMIT BHATTACHARYA & PRASIDH RAJ SINGH

FACULTY

NATIONAL JUDICIAL ACADEMY

National Conference for High Court Justices on Cyber Law & AI [P-1462]
11th & 12th October 2025

Academic Coordinator(s): Dr. Sumit Bhattacharya (Research Fellow) & Mr. Prasidh Raj Singh (Law Associate)

The two day National Conference for High Court Justices on Cyber Law & AI was attended by 34 High Court judges from 14 High Court of India. The conferences delved into examination of on the contemporary subject matter of Artificial Intelligence (AI) and Judiciary. The aim of the National Conference was to i) provide an overview to the participating judges on understanding the nature of cybercrime in the age of AI, ii) to examine the global trends & Indian approaches in regulating cyberspace and AI, iii) explore the spectrum of challenges posed by AI in the adjudicatory process, including liability and accountability challenges, and those relating to appreciation of digital evidences in AI ecosystem, and iv) contemplating the avenues for safeguarding the judicial institutions from cyber-attacks etc. Five technical sessions were dedicated to clinically deal with the said areas. A session-wise brief summary of the proceeds of the same is reported hereunder.

Session – 1: Understanding the Nature of Cybercrime in the Age of AI

Speakers: Justice A. Chitkara ; Chair: Justice A. Bose

The session on *"Understanding the Nature of Cybercrime in the Age of AI"* primarily focused on evolution of cybercrime in the AI age. The session mooted questions on criminal implications of using AI as a tool to commit cybercrime. On the other hand the civil implications in the AI age wherein, what happens to the private party rights *viz.* Intellectual Property Rights (IPR) when AI creates a thing or a process. An overview of offences in the virtual world was examined. The three pronged approach to investigation i.e. 1) Offences with AI wherein AI is often used or can be potentially used as a tool; 2) Offences by AI, where AI in its agentic mode independently commits or omits to do an offence; and 3) Offences on AI, where AI itself falls victim and becomes a subject matter of offence was discussed. Moreover, the session explored the issues of dealing with cybercrime in the AI eco-system. Challenges relating to jurisdictional issues, wherein the crime may be executed involving several geo-spatial jurisdictions was examined. Another area of which was discussed during the session was relating to issues relating to the investigations. Investigation as a process in itself, the tools used in the investigation, and the system including the human behind the investigation was separately considered posing or facing bottlenecks. AI cybercrimes evade borders *via* offshore servers, slowing MLATs and fragmenting enforcement between IT Act (India) and EU AI Act. Global inconsistencies demand harmonized treaties. Whereas, forensic gaps hinder "deepfake" authentication, breaking evidence chains and admissibility under digital rules. Rapid AI evolution outpaces tools, needing multi-agency forensics. The session culminated with sharing of judge's experiences. The Chinese style integrates AI regulation into broader cyberspace governance, mandating labeled AI-generated content and aligning AI use with social stability and national values, supported by evolving administrative measures rather than a single comprehensive framework.

Session – 2: Global Trends & Indian Approaches in Regulating Cyberspace and AI

Speakers: Prof. P. P. Chakraborty; Chair: Justice S. Govindaraj

The Session on "*Global Trends & India Approaches in Regulating Cyberspace and AI*" an intense discourse on myriad proposed and enacted forms of AI governance attempted globally. Cyberspace regulations especially in an environment of artificial intelligence (AI) reflects diverse philosophies. While the United States (US), there is no unified federal AI law. The government predominantly relies on existing laws,

executive orders like the 2025 "Removing Barriers" directive, and guidelines focused on innovation and voluntary industry compliance, while state-level initiatives increasingly enact their own AI statutes. The European Union (EU) has adopted structured, risk-based legislation such as the General Data Protection Regulation (GDPR) to protect privacy and the Artificial Intelligence Act to govern AI systems with stringent transparency, safety, and accountability requirements. However, ongoing proposals seek to simplify parts of GDPR and delay some high-risk AI Rules to bolster competitiveness, drawing debate over privacy protections versus innovation incentives. Challenges in transparency, privacy, and accountability persist globally. India's Digital Personal Data Protection Act, 2023 establishes core rights and fiduciary duties but lacks explicit AI decision-making provisions, prompting calls for clearer algorithmic governance.

Session – 3: Liability and Accountability Challenges in AI-Driven Offences

Speakers: Justice A. Chitkara, Justice S. Govindaraj,& Prof. P. P. Chakraborty

The session on "*Liability and Accountability Challenges in AI-Driven Offences*" delved into the finer aspects of the liability and accountability generally settled as law in the traditional physical space. The rapid proliferation of AI technologies has amplified traditional legal challenges in criminal and civil liability, especially as AI tools are increasingly used to create and distribute harmful content such as deepfakes. "Deepfakes", which are synthetic images, videos, or audio generated or manipulated using AI, pose multifaceted risks, including defamation, identity theft, and privacy invasion. In India, courts have responded with "injunctions" and "removal orders" where AI-generated content harms reputation or dignity. It was shared that, the Bombay High Court granted urgent relief to restrain and remove AI-generated deepfake content infringing an actor's privacy and dignity, recognising that such content, though synthetic, inflicts tangible reputational harm and public disorder risks. It was discussed that one of the major challenges before the judiciary is to ascertain who has caused the actual illegality, and hence who its to be held liable or accountable, when AI is implicated in wrongdoing. Under conventional criminal law, liability attaches to actors whose intentional or negligent conduct caused the harm. However, autonomous AI systems lack legal personhood and *mens rea* (criminal intent), complicating direct attribution of liability to the AI itself. Legal scholars have noted the "black box" problem and difficulties of causation when AI systems act with limited human oversight. Consequently, liability frameworks must address whether responsibility should rest primarily with programmers or developers, who design and deploy systems; users or operators, who implement or misuse a system; or the AI system itself through new legal constructs such as "strict liability" or "shared liability" models. Singaporean and European scholarship, for example, advocates strict liability for high-risk AI harms to incentivise safer design, while shared liability models distribute responsibility across developers, deployers, and data providers. The discourse further recounted on the fact that, judicial responses to AI offences reveal evolving jurisprudence balancing innovation with accountability. Courts have consistently held that platforms cannot hide behind automation excuses when unlawful content is reported, requiring proactive content removal and cooperation with investigations. The session concluded with an active participation posing and contemplating novel questions and suggesting approaches to deal with such challenges.

Session – 4: Appreciation of Digital Evidence in AI Ecosystem

Speakers: Justice A. M. Mustaque; Chair: Justice Rajesh Bindal

The session on *"Appreciation of Digital Evidence in the AI Ecosystem"* focused on the evolving challenges and jurisprudential frameworks governing the handling of digital evidence in an increasingly technology driven justice system. The discussion commenced with an examination of the processes involved in the

collection, preservation, and production of digital evidence, emphasizing the necessity of adhering to established guidelines and protocols under Indian law as well as globally accepted standards. The session underscored that improper handling at any stage may compromise the evidentiary value of digital material, particularly in cases involving AI-generated or AI-processed data.

The session further deliberated on the core principles of authenticity, integrity, reliability, and admissibility of digital evidence. Jurisprudential developments were discussed to highlight how courts assess whether digital evidence has remained untampered, whether the source is identifiable and trustworthy, and whether the evidentiary chain of custody has been duly maintained. The importance of compliance with statutory requirements under the Information Technology Act and judicial precedents governing electronic records was emphasized.

Attention was also drawn to the standard of proof applicable to digital evidence, particularly in criminal proceedings. The session highlighted that while digital evidence can be highly probative, courts must exercise caution in evaluating its credibility, especially in the context of automated systems and AI tools, where issues of opacity, algorithmic bias, and system errors may arise. The role of judicial scrutiny in balancing technological efficiency with procedural fairness was stressed. The discussion also examined the applicability of the long arm statute and the doctrine of minimum contacts in asserting jurisdiction over foreign entities and data stored beyond national boundaries. The role of Mutual Legal Assistance Treaties (MLATs) was discussed as a crucial mechanism for enhancing international cooperation in the investigation and adjudication of cybercrimes. The session concluded by emphasizing the need for judicial officers to remain technologically informed while ensuring that constitutional safeguards and principles of natural justice are not diluted in the AI ecosystem.

Session – 5: Safeguarding Judicial Institutions from Cyber-attacks

Speakers: Justice A. M. Mustaque; Chair: Justice Rajesh Bindal

The session on *"Safeguarding Judicial Institutions from Cyber-attacks"* sensitively addressed the growing realities faced by judicial institutions in an increasingly digital environment. As courts rely more on electronic records, virtual hearings, and digital communication, the session highlighted that cybersecurity is no longer a purely technical concern but a shared institutional responsibility. The discussion began by underscoring the importance of basic cyber hygiene, encouraging participants and court staff to adopt simple yet effective practices such as being cautious with emails, safeguarding passwords, updating systems regularly, and remaining alert to online threats that may compromise sensitive judicial information.

The session then explored the idea of secured e-corridors as safe digital pathways that enable courts to communicate and function securely. These protected systems were explained as essential tools for preserving confidentiality and trust within the justice delivery system. By ensuring controlled access and secure transmission of data, secured e-corridors were presented as a means of reinforcing the integrity of judicial processes in the digital space.

A significant portion of the session focused on incident response planning, emphasizing that preparedness is key to resilience. The discussion highlighted that cyber incidents if and when they occur must be met with calm coordinated, and well-defined responses. Practical strategies such as having clear response protocols, conducting periodic drills, maintaining reliable data backups, and ensuring timely reporting were discussed as ways to minimize disruption and restore normal functioning swiftly. The role of IT security measures was discussed in a practical and reassuring manner, stressing that layered security systems such as firewalls, access controls, and continuous monitoring serve as protective safeguards rather than obstacles

to judicial work. The session emphasized the need for regular audits and updates to keep pace with evolving cyber threats while maintaining ease of use for court personnel.