



The Role Of Technology In Advancing Criminal Justice Reform: Opportunities And Challenges In India

¹ Mr. Karthik Anand

¹ Assistant Professor, Government Law College, Holenarasipura, Karnataka

ABSTRACT

This article explores the intersection of technology and criminal justice reform in India. It highlights the opportunities presented by technological advancements such as AI, blockchain, big data analytics, and digital forensics while also discussing the challenges, including privacy concerns, the digital divide, and legal ambiguities. Through case laws, statistical analysis, and comparative perspectives, this study underscores the transformative potential of technology in India's justice system. Additionally, the article suggests crucial law reforms and policy measures required for sustainable technological integration. Technological innovation has become a vital tool for enhancing efficiency and addressing challenges in the reform of India's criminal justice system. This study explores the impact of technology on various key areas, including investigation, decision-making, and rehabilitation. It examines how advancements in forensic technologies, electronic filing systems, digital record digitization, and AI-driven predictive policing influence the effectiveness of courts, prisons, and law enforcement. Additionally, it evaluates how these developments may impact human rights, accountability, transparency, and access to justice. Through case studies and empirical research, this analysis highlights the opportunities and challenges posed by technological innovation in shaping the future of criminal justice reform in India.

Key Words: Criminal Justice, Technology, AI, Blockchain, Legal Reforms

¹ Assistant Professor, Government Law College, Holenarasipura, Karnataka

INTRODUCTION

The Indian criminal justice system has long grappled with issues of judicial backlog, inefficiency, and procedural delays. With over 4.5 crore pending cases as of 2024, the need for reform is urgent. Technology offers a way to modernize and streamline processes, enhance transparency, and improve access to justice. However, it also presents challenges that must be addressed through legal and policy frameworks. Legal reforms are necessary to ensure the ethical and equitable use of technology in criminal justice.

HISTORICAL BACKGROUND

Over the years, there have been substantial technological advancements in the administration of justice. The court system has continuously adjusted to technology developments to improve efficiency, transparency, and accessibility, starting with the early dependence on written codes and continuing with the introduction of digital case management systems and artificial intelligence (AI)-powered legal research. In addition to speeding up court proceedings, the incorporation of technology into legal frameworks has sparked worries about data security, privacy, and justice. This article examines how technology has changed throughout time in the administration of justice, from prehistoric legal systems to the digital era.

Early Technological Developments in Justice Administration

1. Written Legal Codes and Documentation

The use of written legal codes was among the first technological developments in the legal system that were known to exist. One of the earliest examples of codified legislation was the Code of Hammurabi, which was written on stone tablets for public awareness in Mesopotamia around 1754 BCE. This made it possible for laws to be applied consistently and uniformly. Comparably, the Twelve Tables (451-450 BCE) established the basis for Roman law in ancient Rome by guaranteeing that legal clauses were documented for future use.

By making legal texts publicly available, Johannes Gutenberg's invention of the printing press in the 15th century further transformed legal documentation. Access to laws and court rulings was formerly restricted by the human transcription of legal records. The printing press made it possible for statutes and case laws to be produced in large quantities, which greatly increased accessibility and legal literacy.

2. Introduction of Computers in Judicial Systems

The use of computers in case management began in the middle of the 20th century. In order to expedite judicial administration, American courts were among the first to adopt electronic case management systems (CMS) in the 1960s. Legal research, case tracking, and record-keeping were all made easier by these technologies.

By the 1970s, legal practice had changed due to the creation of legal research databases like Westlaw (1975) and LexisNexis (1973). By enabling digital searches of statutes, case laws, and legal literature, these platforms helped judges and attorneys become less dependent on physical law libraries.

3. Digitalization of Judicial Records and E-Courts

E-courts, which aimed to digitize the legal system, emerged in the late 20th and early 21st centuries. To cut down on paperwork and boost productivity, governments all over the world started putting electronic filing systems, or e-filing, into place. The E-Courts Mission Mode Projects, which were introduced in India in 2005, sought to digitize case files and make online case monitoring possible.

4. 21st Century: The Digital Transformation of Justice

The use of video conferencing for court proceedings was one of the biggest technical revolutions in the administration of justice. This shift was sped up by the COVID-19 epidemic in 2020, when virtual proceedings were required due to physical court closures. In order to maintain access to justice, the Supreme Court of India, in a suo motu order in 2020, required video conferencing for urgent cases (In Re: Guidelines for Court Functioning by Video Conferencing during COVID-19, (2020) 6 SCC 686).

5. Artificial Intelligence in Judicial Decision-Making

AI has become a game-changing tool for case prediction and legal research. Legal analysis is aided by AI-powered tools like ROSS (based on IBM Watson), which forecast case outcomes and provide pertinent precedents. With certain courts using AI to evaluate court papers and automate some lower-court decisions, China has led the way in AI-assisted judicial decision-making.

However, there are ethical issues with using AI in court, especially when it comes to algorithmic prejudice and the absence of human oversight. In order to regulate AI-driven surveillance and decision-making systems.

OPPORTUNITIES FOR TECHNOLOGY IN CRIMINAL JUSTICE REFORM

Artificial intelligence in legal research and adjudication

AI-powered legal research tools such as SCC Online and Manupatra assist legal professionals in accessing case laws, precedents, and statutes efficiently. AI can also aid in predictive analysis for case outcomes, reducing time-consuming legal research. Moreover, AI-driven chatbots and virtual assistants are being deployed to provide legal aid services to underprivileged individuals who lack access to traditional legal resources.

AI has also revolutionized contract analysis and legal documentation. AI-based tools assist lawyers in drafting legal agreements and verifying clauses for compliance, thus reducing human errors. In the judiciary, AI-driven tools such as SUPACE²) are being explored to support judges in analyzing case files more efficiently.

Case Law:

- *State of Maharashtra v Praful Desai*³ – The Supreme Court ruled that video conferencing can be used to capture evidence during a criminal prosecution. It claimed that physical presence is not required by Section 273 of the CrPC, which stipulates that evidence must be obtained in the accused's presence. The Court determined that video conferencing can be considered a form of presence under Section 273. It added that, in accordance with Section 3 of the Indian Evidence Act, video conferences would qualify as evidence. Thus, the High Court erred in banning video conferencing since it did not meet Section 273's need for physical presence.
- *Anvar PV v PK Basheer*⁴ – This case permitted consideration of an appeal to show the type and process of admitting electronic evidence, which is only pertinent where the evidence is authentic and trustworthy. A standard procedure for the admissibility of electronic evidence was established by the *Anvar* case. The court determined that while electronic evidence is covered by Sections 65A and 65B of the Indian Evidence Act, Sections 63 and 65 do not apply to it. *Generalia specialibus non derogant* means that special law will take precedence over general law. Since Sections 65A and 65B are specifically designed to address electronic evidence, they are not applicable in cases involving electronic evidence.

BLOCKCHAIN FOR EVIDENCE MANAGEMENT

Blockchain technology ensures tamper-proof digital evidence storage, enhancing the reliability of forensic data and preventing corruption in evidence handling. Courts and law enforcement agencies in multiple jurisdictions have already begun implementing blockchain solutions for secure documentation. Blockchain's decentralized nature eliminates the risk of tampering with evidence, making it a reliable tool for digital chain-of-custody management. This technology can be used to store crime scene images, forensic reports, and witness statements securely.

² Supreme Court Portal for Assistance in Courts Efficiency

³ 2003 4 SCC 601 (SC)

⁴ 2014 10 SCC 473 (SC)

Examples:

- The Maharashtra government has piloted blockchain-based land records to prevent fraud, showcasing its potential for criminal evidence management⁵.
- The judiciary in Andhra Pradesh has explored blockchain for secure documentation of court records.
- In the United States, blockchain technology has been tested to maintain a digital chain of custody in forensic evidence handling.

BIG DATA AND PREDICTIVE POLICING

Meaning of Predictive Policing

Predictive policing is a proactive approach that forecasts the expected times and locations of crimes using data analysis, statistical modeling, and artificial intelligence algorithms. To find crime hotspots and trends, it uses historical crime data, geography data, weather patterns, and other pertinent information. This data is processed by AI-powered predictive models, which provide law enforcement organizations with useful insights. Effective resource deployment, criminal activity deterrence, and crime prevention are the objectives⁶.

Big data analytics aids law enforcement in identifying crime hotspots and patterns. Predictive policing, as adopted in cities such as Hyderabad, helps in proactive crime prevention and efficient resource allocation. However, concerns about algorithmic biases and potential racial profiling must be addressed through transparent regulatory frameworks.

Big data analytics also facilitates real-time crime mapping, allowing authorities to deploy resources strategically. Machine learning models analyze past criminal activities to predict future crime trends.

| Year | Crime Rate Reduction (%) | Location |
|------|--------------------------|-----------|
| 2020 | 15% | Hyderabad |
| 2021 | 12% | Bangalore |
| 2022 | 10% | Delhi |

⁵https://aigppa.mp.gov.in/uploads/project/STUDY_FOR_ESTABLISHMENT_OF_STATE_LEVEL_FRAMEWORK_AND_STRATEGY_TO_IMPLEMENT_BLOCKCHAIN_USE_CASE_IN_THE_STATE_DR_RITU_MAHESHWARI.pdf last visited on 27.01.2025

⁶ <https://www.tandfonline.com/doi/full/10.1080/24751979.2024.2371781#d1e216> last visited on 01.02.2025

Since it places restrictions on the government's ability to gather and use personal data without a valid reason, the landmark Indian Supreme Court decision *Justice K.S. Puttaswamy v. Union of India*⁷ is extremely relevant to discussions about AI-based surveillance. It established the "right to privacy" as a fundamental right under the Constitution and essentially provides a legal framework to protect citizens from excessive surveillance practices using AI technology.

Digital forensics and cybercrime investigation

With the rise in cybercrimes, digital forensics plays a crucial role in investigating and prosecuting offenses. Technology aids in recovering lost data, tracking digital footprints, and analyzing encrypted evidence. Advanced forensic tools using AI and machine learning assist in decoding complex cyber frauds and digital impersonation cases.

Case Law:

- *Shafhi Mohammad v State of Himachal Pradesh*⁸– In *Shafi Mohammad vs. The State of Himachal Pradesh*, the Hon'ble Supreme Court (Apex Court) noted in its interim decision dated January 30, 2018, that a party who does not possess a device that has produced an electronic document cannot be required to produce a certificate under Section 65B(4) of the Act. This was in light of the importance of videography as a crucial means of evidence and the extent to which procedural requirements under Section 65B(4) of the Indian Evidence Act, 1872 (Act) can be applied.
- *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*⁹– The ruling was made in the context of earlier, contradictory rulings by the SC on the admissibility of electronic evidence. In this instance, the appellant's election to the Maharashtra legislative assembly was challenged in two petitions. The candidate who lost the election filed one petition, and one of the electors filed the other. The respondents argued, citing the camera footage, that the election was invalid because it caused a delay in the submission of nomination forms. According to Section 65 B(4) of the Indian Evidence Act, the Bombay High Court accepted the electronic evidence even though it lacked the necessary certificate. The SC made it clear that the certificate must be submitted as a requirement under Sec 65 B (4) for the admissibility of electronic evidence, supporting the Anvar PV's order and overturning the Shafhi Mohammed's ruling. Additionally, the SC overturned its earlier rulings in *Tomaso Bruno* and *Ramajyam*. SC distinguished between "content that may be regarded as evidence of the original document" and "original document." The former refers to the output of the very information that the

⁷ SCC: (2017) 10 SCC 1

⁸ 2018 5 SCC 311 (SC)

⁹ 2020 7 SCC 1 (SC)

computer provides, while the later is the original record that is saved in the computer and contains original information¹⁰.

- Ritesh Sinha v State of Uttar Pradesh¹¹ In this case the legality of compelled biometric data collection for criminal investigations was dealt. The Hon'ble Supreme Court of India primarily relied on the findings established in Kathi Kalu Oghad v. State of Bombay¹² when it ruled that recording an accused person's voice during an investigation does not violate their right to self-incrimination. In both of these instances, it has been noted that the use of exemplars is not testimonial.

E-COURTS AND VIRTUAL HEARINGS

The e-Courts project, under the National e-Governance Plan, facilitates paperless courts and virtual hearings, reducing pendency and increasing accessibility, particularly during emergencies such as the COVID-19 pandemic. Video conferencing has become a crucial component of judicial proceedings, ensuring that remote hearings are conducted efficiently.

Online dispute resolution (ODR) mechanisms have also emerged as viable alternatives for handling minor civil and criminal matters efficiently.

Examples:

- The Supreme Court of India, in 2020, mandated the use of video conferencing for urgent cases during the COVID-19 lockdown, ensuring uninterrupted access to justice.
- Virtual courts in Delhi and Mumbai have expedited minor traffic violations and bail applications, significantly reducing case pendency.

¹⁰ <https://www.alec.co.in/judgement-page/a-case-regarding-admissibility-of-electronic-evidence> last visted on 02.02.2025

¹¹ 2019 8 SCC 1 (SC)

¹² AIR 1961 SC 1808

USE OF FACIAL RECOGNITION AND BIOMETRICS

Facial recognition technology (FRT) is increasingly used for suspect identification and forensic analysis. However, ethical concerns about mass surveillance and wrongful identification persist.

In *K.S. Puttaswamy v Union of India*¹³– Reinforced privacy concerns in biometric data collection. The judgment established a three-pronged test for any state action restricting privacy:

1. Legality – Any invasion of privacy must be backed by a law.
2. Necessity – The law must be necessary and have a legitimate state aim.
3. Proportionality – The law must not have a disproportionate impact on rights. Facial recognition enables mass surveillance, potentially leading to a “chilling effect” on free speech and movement.

*Ritesh Sinha v State of Uttar Pradesh*¹⁴ – A magistrate's authority to require an accused individual to provide voice samples for verification during a criminal inquiry was established by the courts. Because it follows precedent when it makes sense and disregards it when it doesn't, the ruling is internally inconsistent. The Court's resort to Article 142 of the Indian Constitution, which grants the Supreme Court the authority to administer impartial justice, to judicially enact a coercive power is likewise improper and illegal. The Court raises the usual requirements of criminal investigations to the level of "compelling public interest" in its rush to give the State another investigative tool. It does this without offering any apparent rationale and, more significantly, without taking into account that the legislature should be in charge of such an endeavor.

USE OF DRONES IN LAW ENFORCEMENT

Drones are deployed for surveillance, crowd control, and crime scene investigation. Law enforcement agencies in Indian states such as Uttar Pradesh and Maharashtra use drone technology to monitor public gatherings and prevent riots.

CHALLENGES IN USE OF TECHNOLOGY IN ADMINISTRATION OF JUSTICE

Despite the benefits of technology in criminal justice reform, concerns such as data privacy, digital literacy gaps, and legal ambiguities remain. India needs robust data protection laws to prevent misuse of digital evidence and AI-based surveillance tools. Strengthening the Information Technology Act 2000 and aligning it with global best practices will ensure better safeguards against cybercrimes.

Unquestionably, the use of technology in the administration of justice has changed judicial systems all over the world, providing advantages including greater effectiveness, accessibility, and transparency. However, a number of obstacles prevent it from reaching its full potential during deployment. The digital divide is one

¹³ 2017 10 SCC 1 SC

¹⁴ 2019 8 SCC 1 SC

of the main issues. Many people might not have access to the devices or dependable internet connections needed to take advantage of digital justice tools like electronic evidence submission, virtual hearings, or online case filing, particularly in rural areas or developing countries. Concerns have also been raised over sensitive data privacy and security. Dependence on digital systems raises the possibility of data breaches, cyberattacks, and illegal access to private data. Strong cybersecurity measures must be implemented by governments, courts, and legal professionals to preserve the integrity of court cases and the private data of people working in the legal system.

The possibility that technology would surpass legal frameworks and judicial comprehension is another major obstacle. Concerns regarding the justice, accountability, and openness of these systems are developing as the use of artificial intelligence (AI), algorithms, and other cutting-edge technology in legal procedures—such as sentencing, bail judgments, or predictive analytics—increases. AI-driven choices could unintentionally reinforce prejudices and produce unfair results, particularly if the algorithms are not properly thought out and routinely examined. Additionally, judges and attorneys need to receive sufficient training in order to comprehend and use technology in their work.

Legal experts frequently find it difficult to keep up with the quick speed of technological advancement, which raises concerns about the fairness of digital justice when participants may lack the same resources or technological literacy. Therefore, it is crucial that politicians and legal professionals work together to create comprehensive and flexible frameworks that address these issues in order to guarantee that technology enhances rather than detracts from the justice system.

Suggestions for better use of technology in advancing criminal justice system

1. E-Court Systems and Online Case Management: To expedite case filing, tracking, and management, implement and broaden the usage of e-courts. This would increase efficiency and openness by lowering backlogs, facilitating distant case follow-up, and improving access to legal documents.
2. Police Record Digitization: All FIRs, investigation reports, and arrest records should be digitized in order to modernize police record-keeping. This will facilitate quicker data retrieval for investigations, cut down on paperwork, and make it simpler to trace criminal cases.
3. Integrated Data Systems: To ensure a smooth information flow, build an integrated database that connects the criminal justice, police, and prison systems. This would make it easier to follow criminals, avoid overlaps, and guarantee that courts and law enforcement have easy access to criminal records.
4. Using AI-based algorithms to evaluate crime data and forecast trends, hotspots, or patterns of criminal behavior is known as artificial intelligence for crime prediction and prevention. This might make it possible for law enforcement to allocate resources and prevent crimes in a proactive manner.

5. Enhance the use of digital evidence and virtual hearings, particularly in non-urgent matters, to cut down on delays and improve accessibility to the legal system. To expedite the process, permit the submission of digital evidence (documents, videos, and images) via secure channels.
6. Using blockchain technology to protect the integrity of digital evidence is a good idea. Evidence can be verified and stored in a way that prevents tampering, guaranteeing that it won't be changed throughout the investigation or trial.
7. Courtroom Automation: Include automated systems for case scheduling, document management, and real-time transcription in courts. This would speed up and increase the correctness of judicial processes, improve workflow, and lessen human mistake.
8. Mobile Apps for Public get and Awareness: Create mobile applications that make it simple for people to get legal aid, file complaints, and monitor the status of cases. In addition to offering safety advice and real-time reports on criminal activity, these apps can raise public awareness.
9. Cybercrime Units and Digital Forensics: To counter the increasing threat of online criminal activity, create specialist cybercrime units and bolster digital forensics skills. Providing law enforcement with training on digital investigation methods and technologies can help them deal with cybercrimes more successfully.
10. AI and Machine Learning for Sentencing and Rehabilitation: Take into account variables like the chance of successful rehabilitation and the risk of recidivism when making sentencing judgments. Additionally, inmates can be monitored and assisted during their recovery process with the assistance of these technology.

CONCLUSION

Technology holds immense promise for India's criminal justice reform. However, its implementation must be balanced with legal safeguards and ethical considerations. Future policies should focus on responsible AI use, stringent data protection laws, and bridging the digital divide. With comprehensive legal reforms, India can build a technologically advanced, transparent, and accessible criminal justice system.