Asian And Pacific Economic Review
ISSN: 1000-6052

FUTURE FRONTIERS OF FORENSIC SCIENCE: TECHNOLOGICAL ADVANCEMENTS AND EMERGING CHALLENGES IN ASIAN LEGAL SYSTEMS

Dr. Sudhir Kumar Dwivedi,[1]Ms. Mimansha,[2] Mr. Prashant Panday[3], Mr. Amar Anshul[4] Ms. Radha Gupta[5]

https://doi.org/10.5281/zenodo.20265187

Abstract

The rapid advancement of technology has significantly transformed forensic investigations across Asian legal systems. Modern forensic science increasingly relies on Artificial Intelligence (AI), genomic technologies, digital forensics, biometric surveillance, and data-driven investigative tools to improve the accuracy and efficiency of criminal investigations. Technologies such as DNA profiling, Next-Generation Sequencing (NGS), facial recognition, predictive policing, and electronic evidence analysis have strengthened the evidentiary process and enhanced crime detection capabilities.

However, the growing dependence on technology also creates serious legal, ethical, and constitutional concerns relating to privacy, data protection, surveillance, algorithmic bias, and admissibility of evidence. The use of AI-driven investigations and biometric monitoring raises questions regarding transparency, accountability, and protection of fundamental rights under modern constitutional frameworks. Additionally, digital evidence remains vulnerable to tampering, manipulation, and cybersecurity threats, thereby requiring strict procedural safeguards and robust forensic infrastructure.

This paper examines the impact of emerging technologies on forensic investigations within Asian legal systems and highlights the need for balanced regulatory frameworks, judicial awareness, ethical oversight, and statutory reforms. It argues that while technological innovations can strengthen criminal justice administration, their implementation must remain consistent with the principles of due process, privacy, and fair trial to preserve the integrity of justice in an increasingly digital era.

KEYWORDS-Forensic Technology, Digital Evidence, Genomic Forensics, AI in Law, Predictive Policing, Chainof Custody.

1. Introduction

The convergence of law, science, and emerging technologies has initiated a fundamental transformation in forensic investigations, recalibrating traditional evidentiary methodologies and

[1] Assistant Professor, JIMS, GN, GGSIPU, NEW DELHI. Email: adv.skdwwivedi@gmail.com
[2] Advocate, Delhi High Court, NEW DELHI, Email: mimansha1188@gmail.com
[3]Assistant Professor, JIMS, GN, GGSIPU, NEW DELHI. Email: prshnt.pandey1006@gmail.com
[4]Assistant Professor, JIMS, GN, GGSIPU, NEW DELHI. Email: amar.anshul3839@gmail.com
[5]Assistant Professor, JIMS, GN, GGSIPU, NEW DELHI. Email: radhasunitagupta@gmail.com

judicial epistemology. This paradigm shift is not merely an incremental improvement in crime-solving tools; rather, it represents a deep and structural change in the very architecture of criminal jurisprudence. Algorithmic reasoning, biometric surveillance, and digitized evidence are reshaping the protocols that govern everything from crime scene management to the final adjudication of guilt or innocence.[6] The implications of this technological metamorphosis are profound, offering the promise of unprecedented precision and efficiency while simultaneously introducing complex legal and ethical challenges.[7] This research probes this techno-legal frontier, seeking to understand the dynamic interaction between scientific innovation and the enduring principles of justice and constitutional governance.

1.1 The Problem: Technology, Rights, and the Legal Vacuum

The central problem confronting the Indian legal system, and indeed legal systems worldwide, is the systemic tension between the deterministic capabilities of technology and the foundational protections enshrined in constitutional and human rights frameworks.[8] This disruptive potential is rooted in a basic conflict: while constitutional doctrine is meant to be stable, it is also crafted under specific technological conditions, which are now rapidly changing.[9] As genomic forensics expands the scope of identity determination and Artificial Intelligence (AI) is operationalized in crime scene reconstruction, fundamental questions arise concerning informational privacy, bodily autonomy, the explainability of machine-generated inferences, and the probative value of novel forms of evidence.[10] The rapid deployment of such powerful tools without clear normative and regulatory frameworks has created a legal vacuum, giving rise to ethical ambiguities that threaten to undermine the very principles they are intended to serve.[11]

2.1 The Legislative Transition: Repealing the IEA, 1872

The Indian legal landscape is undergoing a monumental shift with the repeal of the Indian Evidence Act, 1872 (IEA)[12], a colonial-era statute that was replaced on July 1, 2024, by the Bharatiya Sakshya Adhiniyam, 2023 (BSA)[13]. The IEA, enacted at a time when digital communication was unimaginable, was increasingly inadequate for a legal system grappling with the complexities of modern forensic and electronic evidence.[14] The new legislation, passed to bring evidence laws in sync with the latest technological developments, represents a paradigm shift toward a digital-first judicial system. The BSA aims to update evidence laws by including provisions for electronic records and filling gaps in rules of secondary evidence.

---

[6] R. Dunton, "Examining the Relationship Between Legal Systems and Forensic Science", 11 *Themis: Research Journal of Justice Studies and Forensic Science* 1 (2023).
[7] M. Kumar, "AI in Criminal Jurisprudence in India", 5 *J. Legal Stud.* 12 (2023).
[8] Minho Kim, "Analysis of India's Criminal Procedure (Identification) Act, 2022: Determining Potential Misuse and Possible Violations of Fundamental Rights", *International Annals of Criminology* (2023).
[9] S. Han, "Constitutional Rights and Technological Change", 54 *U.C. Davis Law Review* 73 (2020).
[10] *Ibid.*
[11] A.P. Mishra, "The Legal and Regulatory Framework of Nanotechnology in India", 8 *J. Law & Policy* 45 (2024).
[12] The Indian Evidence Act, 1872, Repealed (2024).
[13] Bharatiya Sakshya Adhiniyam, 2023 (BSA), Act No. 46 of 2023, s. 1.
[14] A. Kumar, "The Criminal Procedure (Identification) Act, 2022: A Critical Analysis of its Legal, Constitutional, and Societal Implications", 13 *IJIRL* 14 (2024).

2.2 The BSA, 2023: Redefining Electronic Records as Primary Evidence

A pivotal change introduced by the BSA is the reclassification of electronic records. Under the IEA, electronic evidence was relegated to the status of secondary evidence and required a specific certificate under Section 65B for admissibility.[15] This framework, while acknowledging digital evidence, created procedural hurdles and legal ambiguities that were subject to varied judicial interpretations. In a landmark move, the BSA now classifies electronic records as primary evidence, placing them on an equal legal footing with conventional paper documents.[16] The expanded definition of a "document" now explicitly includes information stored in semiconductor memory or any communication devices, such as laptops and smartphones, encompassing a wide range of digital data from emails to geolocation information. The BSA also allows for oral evidence to be given electronically, permitting witnesses, the accused, and victims to testify through electronic means.[17] Section 93 of the BSA creates a presumption of authenticity for electronic records that are five years old and produced from proper custody.[18]

The judicial interpretation under the IEA, particularly in the case of ***Anvar P.V. v. P.K. Basheer***, established a significant principle. The Supreme Court, in this case, held that Sections 65A and 65B formed a "complete code" for the admissibility of electronic evidence, overruling previous rulings that allowed electronic evidence to be admitted without a certificate under the general provisions of Sections 63 and 65.[19] This judicial precedent was based on the legal maxim *Generaliaspecialibus non derogant*, which translates to "the general shall not derogate from the specific".[20] This position was reaffirmed in the case of ***Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal***, which held the Section 65B certificate to be a mandatory condition for the admissibility of secondary copies of electronic records.[21] The BSA retains a similar approach, requiring a certificate for electronic records to be admitted, especially when their genuineness is in question. However, the BSA also clarifies that electronic records produced from proper custody will be considered primary evidence unless disputed.[22]

3.1 ***Genomic Forensics and Next-Generation Sequencing: Transforming Criminal Investigations in Asian Legal Systems***

The emergence of genomic forensics has significantly transformed the investigative capabilities of modern criminal justice systems, particularly in technologically advancing Asian jurisdictions.

[15] S. Singh, "Digital Forensics in the BSA Era", 12 *J. Cybercrime* 45 (2024).
[16] V.S. Sengar, *Law of Electronic Evidence*, 21 (Eastern Book Co., Lucknow, 2024).
[17] K.A. Singh, "Electronic Evidence under the Bharatiya Sakshya Adhiniyam, 2023", 2 *NLUJ Law Review* 55 (2024).
[18] Bharatiya Sakshya Adhiniyam, 2023 (BSA), Act No. 46 of 2023, s. 93.
[19] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
[20] *Ibid.*
[21] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
[22] Bharatiya Sakshya Adhiniyam, 2023 (BSA), Act No. 46 of 2023, s. 61.

Techniques such as DNA profiling, forensic genetics, and disaster victim identification have enabled investigators to establish identity with a high degree of scientific accuracy. Among these innovations, Next-Generation Sequencing (NGS) represents a major advancement over conventional forensic methods. Unlike traditional capillary electrophoresis (CE), which could examine only a limited number of genetic markers, NGS technology can simultaneously analyze a substantially larger range of markers from a single biological sample, including degraded or low-quantity specimens. This enhanced analytical capacity has strengthened the reliability of forensic investigations by enabling more accurate identification in complex criminal cases, mass disasters, and missing-person investigations.[23]The growing adoption of genomic technologies in Asian legal systems has also demonstrated their increasing evidentiary significance. In India, DNA evidence has been instrumental in several landmark criminal cases, including the widely discussed Nirbhaya gang rape case, where forensic analysis contributed substantially to the conviction process.

Similarly, countries such as China, Japan, and South Korea have expanded the use of forensic DNA databases and advanced genetic technologies to combat violent crimes and improve investigative efficiency. The ability of NGS to generate comprehensive genetic profiles from degraded, mixed, or limited biological samples has greatly improved forensic precision and strengthened prosecutorial evidence. However, the expanding use of genomic forensics simultaneously raises concerns regarding privacy, data protection, genetic surveillance, and the ethical use of biological information, thereby necessitating stronger legal safeguards and regulatory oversight within Asian legal frameworks.[24]

3.2 The Constitutional Conflict: Privacy vs. State Power

However, the application of DNA profiling, especially forensic DNA phenotyping (FDP) which predicts physical traits from genetic material, presents a direct legal and constitutional conflict.[25] The central issue is the clash between the state's interest in crime-solving and an individual's fundamental rights, namely the right against self-incrimination under Article 20(3) and the right to privacy under Article 21 of the Constitution. FDP's probabilistic nature and its ability to disclose private information about an individual raise a range of ethical and social concerns.[26]

This constitutional tension has been a recurring theme in Indian jurisprudence. In the case of ***Goutam Kundu v. State of West Bengal***, the Supreme Court held that blood tests cannot be ordered by a court as a "matter of course" and that no individual can be compelled to provide a blood sample against their will.[27] The court emphasized the need to carefully examine the consequences of such an order, particularly in disputed paternity cases, due to the potential for branding a child

[23]J. Marciano, "Next-Generation Sequencing Accepted in Court for First Time", *Forensic Magazine*, Jan. 29, 2024.
[24]"Nirbhaya Gang Rape Case", *The Times of India*, (Jan. 25, 2024).
[25] F.K. Sharma, "Forensic DNA Phenotyping and the Right to Privacy in India", 12 *JILI* 211 (2024).
[26] A. Sharma, "Legal and Ethical Issues in Forensic DNA Phenotyping", 12 *J. Forens. Sci.* 32 (2024).
[27] Goutam Kundu v. State of West Bengal, (1993) 3 SCC 418.

as a bastard and the mother as unchaste. This ruling established a clear judicial restraint on the unfettered use of DNA tests. Similarly, in the landmark case of ***Selvi & Ors. v. State of Karnataka***, a three-judge bench of the Supreme Court held that involuntary administration of narco-analysis, polygraph, and brain-mapping tests was a violation of Article 20(3).[28] While the court drew a distinction between physical and testimonial evidence, it affirmed that expert opinions must be grounded in scientifically sound principles. It was held that the collection and retention of physical evidence, such as DNA samples, do not face the same constitutional hurdles as testimonial compulsion. However, DNA profiling must still be used carefully and in a way that balances the need for evidence with the right to privacy.

3.3 Legislative Ambiguity: The Criminal Procedure (Identification) Act, 2022

The journey of legislative reform in this area reveals a deeper political and legal dynamic. The DNA Technology (Use and Application) Regulation Bill, 2019, which aimed to regulate the use and application of DNA technology, was eventually withdrawn in 2023.[29] The government instead passed the Criminal Procedure (Identification) Act, 2022, which replaced the outdated Identification of Prisoners Act, 1920. This new law authorizes the collection of a broad range of biometric and behavioral data, including biological samples, from a wide class of individuals, including those merely arrested or preventively detained.[30] This legislative action appears to be a deliberate move to circumvent the stricter, rights-based approach of a specific DNA law in favor of a broad, less regulated identification framework. Critics argue that the Act's lack of judicial oversight, unclear consent mechanisms, and ambiguous language could lead to arbitrary intrusions into privacy, directly contradicting the principles established in the seminal ***K.S. Puttaswamy v. Union of India*** judgment.[31] This legislative choice places a greater emphasis on state power to collect data, leaving fundamental rights vulnerable without a robust legal check.

Table 2: Key Judgments on Scientific and Electronic Evidence in India

Case Name	Primary Legal Issue	Principle Established
Goutam Kundu v. State of West Bengal	Compulsion for DNA profiling	A court cannot order a blood test as a matter of course. Compulsion to give a blood sample against one's will is prohibited.

[28] Selvi & Ors. v. State of Karnataka, (2010) 7 SCC 263.
[29] *See* The DNA Technology (Use and Application) Regulation Bill, 2019, https://bnblegal.com/article/dna-profiling-withdrawal-of-the-dna-based-technology-use-and-regulation-bill/.
[30] The Criminal Procedure (Identification) Act, 2022, Act No. 15 of 2022.
[31] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

Selvi & Ors. v. State of Karnataka	Testimonial compulsion	Involuntary narco-analysis, polygraph, and brain-mapping violate the right against self-incrimination (Art. 20(3)). Expert opinions must be scientifically valid.
K.S. Puttaswamy v. Union of India	Right to Privacy	The right to privacy is a fundamental right under Art. 21. Any state infringement must meet the threefold test of legality, necessity, and proportionality.
Anvar P.V. v. P.K. Basheer	Admissibility of electronic records	Section 65B of the Indian Evidence Act is a "complete code" for electronic evidence. A certificate is mandatory for secondary copies of electronic records.
Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal	Admissibility of electronic records	Reaffirmed the mandatory nature of the Section 65B certificate. Clarified the distinction between primary and secondary electronic records.

4.1Artificial Intelligence and Machine Learning in Modern Forensic Investigations

The integration of Artificial Intelligence (AI) and machine learning into forensic science is rapidly transforming the nature of criminal investigations across Asian legal systems. These emerging technologies have introduced advanced methods of crime scene reconstruction, facial recognition, predictive analytics, voice identification, and behavioral pattern analysis. AI-driven forensic tools possess the capability to process enormous volumes of data, correlate information from multiple digital sources, and identify hidden patterns that may remain undetected through conventional investigative methods. As a result, forensic investigations are becoming faster, more precise, and increasingly data-oriented.

Several Asian countries, including India, China, Singapore, and South Korea, have begun incorporating AI-based technologies into policing and criminal investigations. In India, law enforcement agencies have experimented with facial recognition systems, automated surveillance mechanisms, and predictive crime mapping to improve public safety and investigative efficiency. Such technologies enable authorities to identify high-risk zones, monitor criminal activities, and anticipate potential offenses through algorithmic analysis of historical crime data and behavioral trends. The adoption of AI-assisted forensic systems has therefore strengthened preventive policing and enhanced investigative coordination.

Despite these advancements, the growing reliance on AI in forensic investigations raises significant legal and ethical concerns. Questions relating to algorithmic bias, lack of transparency, reliability of machine-generated conclusions, and accountability for erroneous outcomes remain unresolved in many Asian jurisdictions. The admissibility and evidentiary value of AI-generated findings also pose challenges for courts, particularly in legal systems where procedural safeguards and technological regulations are still evolving.[32] Consequently, the expanding role of AI in forensic science necessitates robust regulatory oversight, judicial scrutiny, and ethical safeguards to ensure that technological efficiency does not compromise constitutional rights, due process, and the principles of fair trial.

4.2 The Admissibility Challenge: Evaluating Reliability

However, the legal framework in India, including the new BSA, lacks specific provisions to govern the admissibility of machine-generated outputs and AI analyses.[33] The central challenge is establishing the reliability and probative value of AI evidence in court. International standards offer a comparative framework for this evaluation. The older American *Frye* standard required evidence to be "generally accepted" within the scientific community, while the more flexible *Daubert* test places the judge in a "gatekeeping" role, requiring them to assess the reliability and relevance of expert testimony based on several criteria: whether the methodology has been subjected to a testable hypothesis, the known or potential rate of error, peer review, and general acceptance. These criteria are increasingly relevant for evaluating complex AI systems, whose outputs may appear as objective facts but are often based on opaque, probabilistic processes.[34]

4.3 The Black Box Dilemma: Opacity, Bias, and Judicial Scrutiny

At the heart of the legal challenge is the "black box" dilemma.[35] Modern AI systems, particularly those using deep learning, operate with a level of complexity that makes it difficult, if not impossible, for humans to understand how they arrive at their conclusions. In many Asian legal systems, including India, courts require expert witnesses to clearly explain the scientific basis, methodology, and reasoning supporting their conclusions. However, AI-generated outputs may not always provide a transparent explanation capable of judicial scrutiny. The inability to examine the internal functioning of algorithmic systems raises doubts regarding the credibility, admissibility, and probative value of machine-generated evidence. If courts, lawyers, and accused persons are unable to understand how an AI system arrived at a particular conclusion, it may

[32]R. Singh, "How AI helped Delhi Police to solve a blind murder case", *The Economic Times*, Jan. 25, 2024.
[33] V. Sharma, "Admissibility of AI-Generated Evidence in Indian Courts", 14 *IJLLR* 8 (2024).
[34] A. Mishra, "The Black Box Problem: A Challenge to Transparency in AI-powered Judicial Systems", 16 *JILI* 155 (2024).
[35] R. Rawashdeh, "AI's Mysterious 'Black Box' Problem Explained", *Univ. of Michigan-Dearborn News*, May 15, 2023.

undermine the principles of natural justice, cross-examination, and fair trial..[36] If an AI produces an inference—for example, by identifying a suspect based on a complex facial recognition algorithm—but the underlying process cannot be meaningfully explained or audited, its evidence cannot be subjected to a rigorous cross-examination. This represents a profound shift in the judicial epistemology, or how courts ascertain truth. The lack of explainability makes it difficult to assess for potential biases, such as higher error rates for certain ethnic groups in facial recognition systems, which would violate principles of fairness and due process.[37] Consequently, the legal system must develop a new standard for what constitutes "reliable" evidence, one that goes beyond mere output and demands a degree of transparency in the AI's decision-making process.

5.1 Electronic Records in the BSA Era

The rapid growth of digital technology has fundamentally transformed the nature of evidence in contemporary legal proceedings, making electronic records an indispensable component of both criminal and civil investigations across Asian legal systems. Recognizing this technological shift, the Bharatiya Sakshya Adhiniyam, 2023 has expanded the scope of the term "document" to expressly include electronic and digital records. This legislative development reflects the growing dependence of modern investigations on digital evidence such as emails, text messages, server logs, CCTV footage, social media communications, cloud-stored information, mobile phone data, blockchain records, and AI-generated content, including deepfakes.

Under the BSA framework, electronic records are granted legal recognition and evidentiary value equivalent to traditional paper-based documents, subject to the establishment of authenticity, reliability, and procedural compliance. Provisions such as Section 61 reinforce the admissibility of digital evidence by recognizing electronic and digital records as valid forms of documentary evidence before courts of law. This modernization of evidentiary law is particularly significant in an era where cybercrime, digital fraud, online harassment, financial scams, and transnational electronic offenses are rapidly increasing across Asian jurisdictions.[38]

The increasing dependence on digital evidence has created significant legal and forensic challenges, as electronic records remain vulnerable to tampering, unauthorized access, and technological manipulation. Emerging threats such as deepfakes, synthetic media, and AI-generated content further complicate the verification of authenticity and evidentiary reliability. Therefore, effective implementation of the Bharatiya Sakshya Adhiniyam, 2023 requires strict forensic safeguards, judicial awareness, and strong digital forensic infrastructure to ensure fair trial and evidentiary integrity.

---

[36] Bharatiya Sakshya Adhiniyam, 2023 (BSA), Act No. 46 of 2023, s. 39.
[37] A. Sharma, "Ensuring the Integrity of Digital Evidence: The Role of the Chain of Custody in Digital Forensics", 10 *J. Dig. Forens.* 12 (2024).
[38] Grewal, M., Batar, S., & Singh, N. (2025). Forensic Science and the Judicial System: An Analysis of Post-Conviction Review and Exoneration. Advances in Consumer Research, 2(4).

5.2 The Chain of Custody Imperative: Hash Values and Metadata

A fundamental safeguard in digital forensics is maintaining a complete and unbroken chain of custody, which records every stage of handling electronic evidence from seizure to courtroom presentation. This process ensures the authenticity and integrity of digital evidence through proper documentation of time, date, and personnel involved. Investigators also use hash values, often described as digital fingerprints, to verify that electronic data has not been altered or tampered with. Under the Information Technology Act, 2000, manipulation of digital evidence or hash values may attract criminal liability and punishment.[39] The importance of maintaining an unbroken chain of custody has been highlighted in Indian courts, such as in ***Sandeep Kumar Dikshit v. Ministry of Home Affairs***, where the absence of a hash value for a DVD was a point of contention.[40]

While hash values provide a powerful tool for authentication, a deeper issue is the potential for spoliation, which refers to the destruction or significant alteration of evidence. The ease with which metadata—information that describes and provides context about other data, such as timestamps and GPS coordinates—can be modified is a significant challenge to the integrity of electronic evidence.[41] Metadata can be altered either intentionally to hide facts or unintentionally through routine system operations. This creates a procedural gap where the integrity of digital evidence can be questioned even if the primary file's hash value remains intact. The lack of standardized protocols for preserving metadata and the fragmented nature of data storage across platforms (e.g., social media and cloud services) complicate the management of a complete chain of custody. The legal system must grapple with this new layer of complexity, requiring stringent standards for metadata handling and preservation to prevent the erosion of evidentiary integrity. The burden of proving the reliability of metadata typically falls on the party seeking to introduce it as evidence.

6.1 *AI-Driven Surveillance, Privacy Concerns, and Constitutional Challenges*

The growing use of Artificial Intelligence, predictive policing, facial recognition, and biometric surveillance technologies has significantly transformed modern forensic investigations in India and other Asian legal systems. These technologies enable law enforcement agencies to analyze crime patterns, monitor high-risk areas, and prevent criminal activities through data-driven policing methods.[42] However, the rapid expansion of surveillance mechanisms has also created serious concerns regarding mass monitoring, misuse of personal data, and erosion of civil liberties. Excessive dependence on biometric technologies risks creating an “Orwellian” system of

[39] Information Technology Act, 2000, s. 66.
[40] Sandeep Kumar Dikshit v. Ministry of Home Affairs, (2022) 13 SCC 56.
[41] A.K. Sharma, “Metadata and Web Scraping: IP Issues”, 5 *J. Legal Tech.* 21 (2025).
[42]S. Khan, “India's Surveillance Landscape after the DPDPA”, *IAPP*, Jan. 21, 2024.

surveillance where individuals are continuously monitored, thereby undermining the presumption of innocence and freedom of expression.[43]

The constitutional validity of such technologies must be examined in light of the principles established in the K.S. Puttaswamy v. Union of India, which recognized privacy as a fundamental right under Article 21 and required restrictions to satisfy tests of legality, necessity, and proportionality. [44] Concerns have also been raised regarding the Criminal Procedure (Identification) Act, 2022, which permits extensive collection and long-term retention of biometric data without sufficient judicial oversight or data protection safeguards.[45] Similarly, the case of Frank Vitus v. Narcotics Control Bureau highlights the judiciary's growing recognition of digital privacy and the constitutional implications of location tracking technologies.[46]

Although the transition from the Indian Evidence Act, 1872 to the Bharatiya Sakshya Adhiniyam, 2023 modernizes evidentiary law by recognizing electronic records as primary evidence, significant procedural and regulatory gaps continue to exist. Therefore, while emerging forensic technologies promise greater investigative accuracy and efficiency, their implementation must be accompanied by robust legal safeguards, judicial oversight, ethical accountability, and strong data protection mechanisms to preserve constitutional rights and maintain public trust in the justice system.[47]

7.1 Recommendations: Towards a Rights-Based and Technology-Responsive Forensic Framework

The increasing use of advanced forensic technologies in Asian legal systems requires a balanced framework that protects both investigative efficiency and fundamental rights. The Bharatiya Sakshya Adhiniyam, 2023 should be supplemented with specific laws regulating Artificial Intelligence, biometric surveillance, and digital forensic technologies. Such legislation must clearly define AI-generated evidence and establish standards for transparency, accountability, and independent audits to address concerns arising from opaque "black box" systems. Governments should also establish independent forensic regulatory authorities to ensure uniform standards, accreditation, and quality control across forensic laboratories. Investment in modern forensic infrastructure, cyber forensic capabilities, and technical training is essential to address institutional and technological gaps.

[43]George Orwell, *Nineteen Eighty-Four,* (Secker & Warburg, London, 1949).
[44]R. Kumar, "The Criminal Procedure (Identification) Act, 2022: A Critical Analysis", 15 *IJL* 21 (2024).
[45]Digital Personal Data Protection Act, 2023.
[46]Frank Vitus v. Narcotics Control Bureau & Ors., (2024) 4 SCC 789.
[47]Susan Brenner, *Cybercrime and Digital Evidence* (Carolina Academic Press 2018).

Judicial officers and legal professionals must receive specialized training to understand the reliability, limitations, and admissibility of technologically generated evidence. Ethical oversight should remain central to forensic investigations, particularly in areas involving facial recognition, predictive policing, and genomic technologies. Human supervision must be mandatory in AI-assisted investigations to prevent algorithmic bias and wrongful identification. Strong privacy and data protection safeguards are also necessary to prevent misuse of biometric and genetic information. Asian countries should further promote regional cooperation in cybercrime investigations and harmonize evidentiary standards for cross-border offenses. Ultimately, the future of forensic science should be based on a hybrid model that combines technological innovation with human judgment, constitutional safeguards, and ethical accountability to preserve the integrity of justice and the rule of law.