DIGITAL FORENSICS UNDER ATTACK: CRIMINAL LIABILITY AND THE INTEGRITY OF FORENSIC DATABASES

Dr. Bhagwan Das

Assistant Professor, Government Law College, Pali (Rajasthan)

Abstract

The increasing use of digital forensic databases in modern criminal justice systems has changed the way evidence is collected, protected, analyzed and presented in courts. These archives have improved the efficiency of investigations and the accuracy of evidence but have also made the archives vulnerable to cyberattacks, unauthorized access, data tampering, and other digital interference. The integrity of forensic databases is necessary to ensure fair trials, public confidence in the judicial system, and the evidentiary value of digital recordings. The article presents a detailed analysis of the legal consequences of cyber manipulation of forensic databases, especially focusing on criminal liability for the illegal change, destruction, falsification or compromise of forensic evidence. This present study uses a doctrinal and comparative research methodology to examine the adequacy of India's existing legal framework, namely the Bharatiya Nyaya Sanhita, 2023, Information Technology Act, 2000 and Bharatiya Sakshya Adhiniyam, 2023, to restrict cyber intrusions of forensic evidence. It also considers the institutional processes necessary to protect critical forensic infrastructure and evaluates whether the current regulatory framework is sufficient to address new cyber risks. The study compares forensic database protection systems in the United States, the United Kingdom, and China, and identifies global best practices that could inform future reforms in India. The paper delves into the judicial ramifications of compromised forensic data, demonstrating how breaches in database integrity can undermine the credibility of evidence, reduce the effectiveness of criminal prosecutions and increase the risk of wrongful convictions or acquittals. The article also calls for extensive legal, technological and institutional reforms to bolster cybersecurity standards, increase accountability, improve chain-of-custody procedures and set up strong governance structures for forensic databases. It argues for the protection of the integrity and security of forensic databases as a technological necessity and constitutional responsibility to provide due process, maintain the credibility of criminal investigations, and enhance the rule of law in a more digital criminal justice system.

Keyword: Chain of Custody, Criminal Liability, Cybersecurity, Digital Evidence, Forensic Databases, Rule of Law

1.INTRODUCTION

Forensic science, medicine, and toxicology have experienced remarkable breakthroughs in recent decades, resulting in a substantial shift from physical evidence storage to highly centralized digital forensic databases. A forensic database is a systematic digital repository utilized to consolidate, analyze, and preserve essential medicolegal and investigative information. Currently, these databases contain very sensitive information, including DNA profiles, fingerprint databases, ballistics data, criminal records, toxicological reports, and facial recognition databases. The criminal court system has increasingly depended on digital forensic records. In instances like those of Switzerland and the Philippines, integrated intelligence databases are crucial for linking crime scenes, exonerating persons from suspicion, and expediting investigations. In India, where the conviction rate is approximately 50%—significantly lower than that of countries such as the US

and UK—the incorporation of state and central forensic science laboratories into digital databases has become essential.[1]

This swift technical advancement has both advantages and disadvantages, leading to the significant rising risk of cyber manipulation. The World Economic Forum identifies cybersecurity as a significant global issue, rendering government digital forensics (DF) systems especially susceptible to attacks. The manipulation of DF information is even more catastrophic than mere cyber theft, as it transcends financial loss and undermines the fundamental principles of justice.

The principal contention regarding this vulnerability is clear: A modified forensic database might lead to unjust convictions, exonerate the culpable, and ultimately undermine public confidence in the justice system. Considering that forensic evidence often influences judicial procedures, an inaccurate biometric signature or a modified toxicological report might potentially devastate lives, careers, and parental rights.

2. FORENSIC DATABASES AS THE BACKBONE OF DIGITAL CRIMINAL EVIDENCE

A Forensic Database is a centralized electronic repository, predominantly managed by governmental and investigative agencies, that archives forensic evidence gathered from the onset of an inquiry until the resolution of a trial. It integrates many forms of forensic data provided by several participants in criminal cases. The database comprises several types of forensic data, including DNA profiles, fingerprint records, ballistics, trace evidence, toxicological reports, and digital forensics, ensuring that essential information is efficiently kept and accessible.

The forensic database serves as the scientific foundation across the four primary stages of criminal proceedings, with data integrity influencing the verdict for the accused.

- **Investigation:** This functions as an intelligence instrument, utilizing DNA, fingerprints, or ballistics to elucidate criminal networks, identify transnational offenses, and exonerate individuals who are ultimately innocent.
- **Charge Framing:** The database offers prima facie evidence supporting a case, fulfilling the legal criterion for "grave suspicion," which is crucial for instituting formal charges and denying immediate release.
- **Trial:** During this phase, the database records are regarded as expert evidence, and their legitimacy hinges on an impeccable chain of custody, as data loss could undermine the burden of proof beyond a reasonable doubt.
- **Sentencing:** In sentencing, forensic investigation serves as a pivotal determinant, elucidating aggravating factors like as cruelty or establishing mitigating factors.

3. CYBER MANIPULATION AND THE FRAGILITY OF EVIDENTIARY INTEGRITY

Having acquired an understanding of the function of forensic databases in crime resolution, it is crucial to contemplate the possible cyber risks that may jeopardize their security and integrity.

3.1 Attacks on the Integrity of Data

Unauthorized Access: Unauthorized access refers to the illicit infiltration of a forensic database by breaching its security protocols, thereby allowing the perpetrator to see, modify, or destroy critical information contained inside, such as DNA samples, fingerprint data, and investigative records. Privilege escalation is regarded as a form of unlawful access, wherein an individual with minimal access to the database exploits their position to elevate their access permissions, hence circumventing the system's security measures.

Man-in-the-Middle (MitM): This type of attack entails covert surveillance and interception of all communications between the forensic laboratory and the database server. Consequently, the assailant is capable to reading, modifying, or intercepting any transmitted data.[2]

[1] S. Das et al., *A New Model of Integrated Forensic Database in India: Road to Future*, 46 J. Indian Acad. Forensic Med. 99 (2024).

[2] Md Shariar Sozol et al., *Building an Impenetrable Vault: Advanced Cybersecurity Strategies for Database Servers*, 8 INT'L J. SCI. RSCH. ENG'G & MGMT. 1 (2024).

3.2 Attacks Against Integrity

SQL Injection: The assailant use input fields to insert harmful SQL code into the database server, such as via a search field utilized by the investigator. They employ this method to bypass authentication and access restricted STR/SNP profiles or manipulate data to fabricate a false match or eliminate a suspect's records.[3]

3.3 Attacks Against Availability

DoS/DDoS Attacks: The assailants inundate the database servers with excessive traffic produced by the botnet. Such attacks culminate in a complete system failure and cause significant operational disruptions.[4]

4. CRIMINAL ACCOUNTABILITY FOR ATTACKS ON FORENSIC DATABASES: EVALUATING INDIA'S LEGAL RESPONSE

Envision an individual named Arjun, employed as a data entry operator for a private cybersecurity firm. One evening, he employs his technical expertise to infiltrate a state forensic laboratory's digital database. He replicates fingerprint records, DNA profiles, and case evidence associated with ongoing criminal investigations and sells this information to a third party. What occurs to him inside India's existing legal framework?

4.1 The Information Technology Act, 2000:

The Information Technology Act of 2000 remains the principal statute concerning Arjun. According to section 43, any individual who accesses a computer or computer network without authorization and downloads or copies data must compensate the aggrieved party. This constitutes the civil penalty.[5]
Regarding criminal penalties, Section 66 of the IT Act, 2000 stipulates that any individual who engages in computer trespassing, data theft, or the dishonest and fraudulent use of a computer contaminant has committed an offence.[6] Arjun may face imprisonment for a maximum of three years, a fine of up to five lakh rupees, or both penalties. Furthermore, since Arjun utilized his computer to transmit stolen material, the stipulations of section 66B of the IT Act, which pertains to the receipt or retention of stolen computer resources, are applicable in conjunction with this, carrying the same maximum sentence penalty.[7]

4.2 The Bharatiya Nyaya Sanhita, 2023:

Section 303(2) of BNS safeguards against data theft, encompassing any digital record, since "documents" is defined in Section 2(8) of BNS to include electronic documents and digital records.[8]

Criminal breach of trust, as delineated in Section 316 of BNS, may be applicable if, for instance, Arjun had been granted access to such systems as part of his employment, even remotely. In this situation, a sentence of up to five years' imprisonment is applicable. Nonetheless, if the perpetrator is a public official or operates in a fiduciary role, a sentence of up to ten years' imprisonment may ensue.[9]

Forgery is defined in Section 336 of the BNS. Forgery today encompasses electronic forgery, including the creation of counterfeit credentials, modification of digital documents, or fabrication of access logs to obscure one's actions. The sentence may extend to a maximum of two years in this instance.[10]

Section 238 of BNS encompasses acts aimed at causing the loss of evidence related to any offense or providing false information to conceal an offense. Currently, if Arjun engages in the deletion, destruction, alteration, or concealment of any evidence, including DNA profiles,

[3] Vugar Abdullayev & Alok Singh Chauhan, *SQL Injection Attack: Quick View*, 3 MESOPOTAMIAN J. CYBERSEC. 30 (2023).
[4] Mohammed Amin Almaiah et al., *Classification of Cybersecurity Threats, Vulnerabilities and Countermeasures in Database Systems*, 81 COMPUT. MATER. CONTIN. 3189, 3195 (2024).
[5] The Information Technology Act, 2000, § 43 (India).
[6] The Information Technology Act, 2000, § 66 (India).
[7] The Information Technology Act, 2000, § 66B (India).
[8] The Bharatiya Nyaya Sanhita, 2023, §§ 2(8), 303(2) (India).
[9] The Bharatiya Nyaya Sanhita, 2023, § 316 (India).
[10] The Bharatiya Nyaya Sanhita, 2023, § 336 (India).

fingerprint records, or other forms of digital evidence, he would be classified inside this category.[11]
Significantly, if Arjun engaged in a coordinated manner with others, he would be penalized under the stipulations of Section 111 of the BNS, which delineates and sanctions organized crime. This section clearly defines cybercrimes as a component of organized crime. The penalty stipulated in the aforementioned clause ranges from a minimum of five years to life imprisonment, accompanied by a fine of no less than five lakh rupees.[12]

4.3 Official Secrets Act, 1923 and The Digital Personal Data Protection Act, 2023:

In the event of a breach of the database associated with a government forensics laboratory, Section 5 of the Official Secrets Act, 1923 may be used if the compromised material relates to an ongoing criminal investigation or contains classified government information. It involves a maximum of three years of incarceration as a penalty.
The DPDP Act, 2023 is relevant as the forensics database contains biometric and sensitive personal data.[13]

5. GOVERNING CRITICAL FORENSIC INFRASTRUCTURE: INSTITUTIONAL RESPONSIBILITIES AND REGULATORY CHALLENGES

In addition to statutory provisions, India has created multiple institutions tasked with safeguarding important information infrastructure and enhancing cybersecurity measures.
The National Critical Information Infrastructure Protection Centre (NCIIPC), established under Section 70A of the IT Act, 2000, serves as the official entity for safeguarding critical information infrastructure in India.[14] This entity offers counsel on cybersecurity issues and collaborates with organizations to protect their systems from threats that could negatively affect national security, the economy, health, and other critical services.
The Data Protection Board of India (DPBI), established under Section 18 of the Digital Personal Data Protection Act, 2023, will address matters related to breaches and non-compliance concerning personal data protection.[15]
The Data Protection Board will possess the authority to investigate breaches, mandate corrective actions, levy penalties, and supervise compliance by Data Fiduciaries. Nevertheless, the board has yet to be established.

6. COMPARATIVE REGULATORY MODELS: LESSONS FROM THE UNITED STATES, THE UNITED KINGDOM, AND CHINA

A nation's legal response to forensic database breaches illustrates its strategy for balancing law enforcement requirements, individual rights, and national security. An analysis of the USA, UK, China, and India uncovers substantial disparities in their legal frameworks and priorities.

6.1 United States: A Federated System with Strong Federal Teeth

The United States manages its primary DNA database through the Combined DNA Index System (CODIS), administered by the FBI. The DNA Identification Act of 1994 empowers the FBI to establish the National DNA Index System, which presently includes over 190 cooperating law enforcement laboratories in the United States. This system is arranged hierarchically at the federal, state, and local levels, indicating that any violation of CODIS entails multi-tiered legislation.[16]
A person who hacks into CODIS may be prosecuted under the Computer Fraud and Abuse Act (CFAA), which prohibits unauthorized access to protected computers owned by governmental entities.[17] Depending on the varying motivations for the activity, the punishment could range from one to ten years or more of incarceration. If the breach is deemed an attack on

[11] The Bharatiya Nyaya Sanhita, 2023, § 238 (India).
[12] The Bharatiya Nyaya Sanhita, 2023, § 111 (India).
[13] The Digital Personal Data Protection Act, 2023 (India).
[14] The Information Technology Act, 2000, § 70A (India).
[15] The Digital Personal Data Protection Act, 2023, § 18 (India).
[16] DNA Identification Act of 1994, Pub. L. No. 103-322, 108 Stat. 2065 (1994); Federal Bureau of Investigation, Combined DNA Index System (CODIS), FBI (accessed June 24, 2026), https://le.fbi.gov/science-and-lab/biometrics-and-fingerprints/codis-2.
[17] Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030 (2026).

important national infrastructure, the charges would be substantially elevated. The Health Insurance Portability and Accountability Act and the Privacy Act of 1974 encompass genetic information and establish further bases for criminal and civil responsibilities. The distinguishing feature of the US method is that enforcement occurs at both federal and state levels, allowing an offender to be prosecuted for the same offense by both jurisdictions.[18]

6.2 United Kingdom: Strong Database, Measured Legal Response

The United Kingdom manages the National DNA Database (NDNAD), established in 1995 and governed by the Police and Criminal Evidence Act 1984 (PACE). Between April 2001 and March 2024, there were 821,794 inquiries regarding unsolved crimes via NDNAD, while the count of subject profile records in March 2024 exceeded 7.2 million. The Forensic Information Databases Strategy Board bears the responsibility and submits an annual report to Parliament in accordance with section 63AB(8) of the PACE.[19]

Any infringement of the National DNA Database will be prosecuted under the Computer Misuse Act 1990 (CMA). Section 1 of the Act addresses illegal access to computer material, with a penalty of up to two years upon indictment. When a crime causes substantial harm to the nation's key infrastructure, the Serious Crime Act 2015 included Section 3ZA to the CMA, imposing a penalty of up to 14 years if it poses a threat to national security or public welfare.[20]

6.3 China: State Security First, Individual Rights Secondary

The strategy used by China is distinctly state-centric. Forensic databases are encompassed within the overarching legal framework that includes the Cybersecurity Law of 2017, the Data Security Law of 2021, and the Personal Information Protection Law of 2021. The Cybersecurity Law addresses cybersecurity concerns and aims to ensure the secure processing of personal information, while forensic databases, as government systems, will be classified as important information infrastructure receiving the highest level of protection.[21]

A violation would be tried under Article 285 of China's Criminal Law, which prohibits unauthorized access to computer systems. If the compromised material is classified as state data, which forensic recordings readily qualify as, charges under the Guarding State Secrets Law may be imposed, with penalties potentially reaching life imprisonment. According to Article 287 of the Criminal Law, electronic theft, including breaches of confidence related to state secrets, is subject to prosecution under the applicable criminal statutes for those specific offenses.[22]

6.4 Where India Stands

Efforts to establish specific legislation for forensic DNA in India commenced with the DNA Technology (Use and Application) Regulation Bill, 2019, which was retracted in July 2023 after the government asserted that its fundamental provisions were already encompassed in the Criminal Procedure (Identification) Act, 2022. The latter facilitates agencies in the collection, maintenance, and analysis of biometric and biological samples utilizing the database managed by the NCRB. However, in contrast to the CODIS or NDNAD databases, India currently lacks a distinct forensic database statute with specific sanctions for cyber breaches, depending instead on the BNS, BNSS, BSA, and IT Act to address this deficiency.

[18] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996); Privacy Act of 1974, 5 U.S.C. § 552a (2026).
[19] Forensic Information Databases Strategy Board, *Forensic Information Databases Strategy Board Annual Report: April 2023–March 2024* (2024), https://assets.publishing.service.gov.uk/media/670793d2080bdf716392f102/E03188121_FIND+Strategy+Repor_t+23-24_Accessible_v02.pdf; Police and Criminal Evidence Act 1984, c. 60, § 63AB(8) (U.K.).
[20] Serious Crime Act 2015, c. 9, § 41 (U.K.); Computer Misuse Act 1990, c. 18, § 3ZA (U.K.).
[21] DLA Piper, Data Protection Laws of the World: China, DLA Piper (accessed June 24, 2026), https://www.dlapiperdataprotection.com/index.html?c=CN.
[22] Criminal Law of the People's Republic of China, arts. 285, 287 (China); Law of the People's Republic of China on Guarding State Secrets, 2010 (China).

7. FROM DATABASE TO COURTROOM: THE CONSEQUENCES OF COMPROMISED DIGITAL EVIDENCE

The Supreme Court in *Dharam Deo Yadav v. State of Uttar Pradesh*[23] recognized the "crucial importance" of forensic science in criminal investigations, particularly in situations reliant on "circumstantial evidence. The Court emphasized the necessity of a scientific methodology in crime scene management, mandating that investigating personnel ensure the protection of evidence against "contamination" and any efforts of "tampering with the material. The Court indicated that forensic evidence assists in "identifying the suspect" and ascertaining the guilt or innocence of the accused. The Court asserted that the credibility of DNA evidence is contingent upon the "quality control and quality assurance methods in the laboratory. Consequently, it is imperative to maintain precise and secure forensic records, as any alteration of forensic data might affect the integrity and dependability of criminal investigations.

Additionally, in the case of *Rahul Vs. State of Delhi, Ministry of Home Affairs and Others*[24], the Supreme Court underscored the necessity for forensic evidence to be credible in criminal investigations, particularly where the prosecution's case relies on scientific evidence. The Court examined DNA evidence, the retrieval of items, and the methodology employed in the acquisition of forensic evidence. It was determined that the forensic evidence lacks scientific and legal validation. Moreover, there were cases where errors in the investigative process, particularly with the recovery and seizure of items, could affect the evidence presented by the prosecution. This case illustrates that the importance of forensic evidence resides in the processes of collecting, preservation, and presentation of evidence before the Court. Consequently, safeguarding forensic databases from unauthorized access, modification, or manipulation is paramount.

8. REIMAGINING INDIA'S FORENSIC SECURITY FRAMEWORK: A ROADMAP FOR REFORM

The existing cybersecurity regulations in India were established to address data breaches and business crimes. Forensic databases significantly differ from conventional databases, as altering a DNA profile or fingerprint evidence can not only infringe upon privacy but may also lead to wrongful convictions or the exoneration of offenders. The subsequent reforms are imperative:

8.1 Secure Cybersecurity Measures for Forensic Databases

Specialized steps are necessary to safeguard forensic databases against cybercrime. Legislation like the IT Act and DPDP Act must be complemented by safeguards against the manipulation of forensic data.

8.2 Monitoring of Audit Logs and Access

All access to, alteration of, or deletion of forensic records must be documented. Audit trails can be scrutinized to identify any unlawful alterations in forensic documents.

8.3 Encryption and Access Rights Based on Roles

Forensic data, including DNA profiles and fingerprints, must be safeguarded by encryption and limited access protocols. Access to these records should be restricted to authorized individuals only.

8.4 Digital Chain of Custody Mechanism

A chain of custody mechanism must be established in forensic databases, similar to the court-recognized chain of custody for physical evidence, to document the history of all interactions involving forensic evidence.

8.5 Legal Protection for Informants of Tampering

Given that forensic database tampering may involve actions by insiders within the business, legal protections should be afforded to those insiders who report any tampering as a violation of access privileges.

[23] *Dharam Deo Yadav v. State of U.P.*, MANU/SC/0298/2014, ¶¶ 25, 28, 34 (India).

[24] *Rahul v. State of Delhi, Ministry of Home Affairs & Ors.*, MANU/SC/1455/2022, ¶ 31 (India).

9. CONCLUSION

Forensic databases are exceptional, as the information included inside them—be it a DNA profile, a fingerprint, or a case file—directly impacts an individual's release or prolonged incarceration. The Supreme Court, in *Dharam Deo Yadav v. State of U.P.* [25], determined that forensic evidence is entirely dependent on quality assurance and the integrity of its transit chain. A compromised database signifies more than only a cybersecurity breach. It signifies a miscarriage of justice, potentially resulting in erroneous convictions or allowing the culpable to evade accountability altogether.

Therefore, forensic database cybersecurity should not be ignored. A constitutional requirement. Forensic data integrity equals criminal justice system integrity.

[25] Dharam Deo Yadav, *supra* note 23, ¶ 34.