RESEARCH PAPER

Technology and the Humanisation of Justice Systems: A Forensic Science Perspective

Abida S. Laskar[1], Dr. Kuntala Roychoudhury[2*], Dr Arkajit Debnath[3]

[1]PhD Scholar, Royal School of Law & Administration, Assam Royal Global University Email : abidalaska8@gmail.com Mobile : 8473066056

[2*]Assistant Professor, Royal School of Law and Administration. The Assam Royal Global University. Email: kuntalaroychoudhury@gmail.com Phone 8638266096 Orchid 0009-0005-6351-1400

[3]Assistant Professor, School of Law, Techno India University Tripura Email: arkajit.debnath077@gmail.com Contact: 9774823990 Orcid: 0009-0008-3770-5633

Abstract

The global justice landscape is undergoing a profound transformation due to the accelerated integration of advanced technology. Forensic science—the systematic application of scientific techniques to criminal investigations—has emerged as a cornerstone in this evolution, facilitating the accurate uncovering of truth and the promotion of accountability. This paper explores the dual role of forensic technologies in contributing to the humanisation of justice, defined as the advancement of fairness, dignity, and accessibility, especially for vulnerable or marginalized individuals. Drawing from the frameworks of therapeutic jurisprudence and victim-centric justice, this research engages both the empowering potential and the critical challenges posed by forensic tools such as DNA profiling, digital forensics, and automated analysis systems. Through a mixed-method approach involving doctrinal analysis and empirical interviews, it evaluates forensic science's capacity to uphold the principles of equity and compassion in Indian legal systems. The study advocates for regulatory harmonisation, scientific literacy among legal actors, and safeguards against forensic misuse—ultimately proposing a humane, technologically integrated justice paradigm.

Keywords- Forensic science, humanisation of justice, doctrinal and empirical research, wrongful conviction, digital forensics, India, victimology

How to cite this article: Laskar AS, Roychoudhury K, Debnath A. Technology and the Humanisation of Justice Systems: A Forensic Science Perspective. Int J Drug Deliv Technol. 2026;16(9s): 149-158. DOI: 10.25258/ijddt.16.9s.15.

1. Introduction

Digital technologies have transformed the modern landscape of crime and investigation, presenting both unprecedented opportunities and formidable challenges for justice systems worldwide. Digital forensics, as a branch of forensic science, plays a pivotal role in detecting, extracting, analyzing, and presenting crucial evidence obtained from a wide range of digital platforms and devices . As justice systems increasingly rely on such technological advancements, integrating digital forensic methods not only enhances investigative accuracy but also contributes to the humanisation of justice systems by promoting fairness, transparency, dignity, and accessibility.

This research article explores the intersection of forensic science and technology with an emphasis on how these innovations can help humanise justice frameworks. In doing so, it outlines the fundamental processes associated with digital forensics, reviews a variety of forensic frameworks (especially those related to cloud forensics), and discusses both the benefits and the inherent challenges that may impede equitable justice delivery. Although the primary focus is on digital evidence and its associated investigative procedures, the analysis draws on empirical data and methodological insights to discuss how these technical processes influence broader justice outcomes.

While the scope of forensic science encompasses a multitude of disciplines—from DNA analysis to fingerprint examinations—this paper concentrates on the digital realm. The modern surge in digital evidence, marked by the exponential increase in digital devices and data volumes, highlights the relevance of implementing robust forensic methodologies that uphold judicial integrity. Additionally, by assessing both strengths and drawbacks in existing forensic frameworks, the article aims to provide a comprehensive overview of how technological advancements in digital forensic science support the ideals of humanising justice systems.

2. The Role of Digital Forensics in Justice Systems

Digital forensics is defined as a discipline dedicated to the extraction, preservation, analysis, and presentation of digital evidence, primarily to support investigations and provide judicially admissible findings in courts of law. As technology becomes increasingly integrated into every aspect of society—from communications and commerce to governance—so too does its potential misuse become a critical concern for justice systems. The fundamental aim of digital forensic analysis is to prove or refute the presence of specific digital artifacts that can either implicate offenders or exonerate the innocent.

*Author for Correspondence: kuntalaroychoudhury@gmail.com

2.1 Enhancing Fairness and Transparency

Forensic science inherently underpins the fairness of the judicial process. When digital evidence is accurately and impartially obtained through standardised procedures, it minimizes the risk of wrongful convictions and ensures that every piece of evidence is evaluated based on scientific rigor. In this context, the adoption of digital forensic methods contributes to a more transparent and accountable justice system. For example, obtaining a clear and unaltered digital trail from network logs, smartphones, or cloud-based applications allows legal officials to verify the sequence of events that led to an alleged crime, thereby promoting procedural transparency that is essential for justice.

2.2 Supporting Human Dignity within Justice

Human dignity, an essential value in many justice systems, is reinforced through the careful handling of digital evidence. Digital forensics, by virtue of its scientific approach, ensures that evidence is treated with respect and that personal data is safeguarded during the investigative process. Proper application of forensic methods prevents the misinterpretation of digital evidence, thereby protecting the privacy and rights of individuals involved in legal proceedings. Such protection is particularly crucial in cases where sensitive information, such as communications, location data, or personal files, may be implicated in legal disputes.

2.3 Accessibility to Justice

The accessibility of justice also benefits from digital forensic practices. As the volume of digital evidence increases, standardised forensic procedures enable quicker and more efficient analyses, ensuring that justice is not delayed by procedural inefficiencies or technical complications. Modern forensic frameworks, which incorporate stages such as evidence collection, preservation, and analysis, aim to streamline the judicial process so that evidence is accessible to all parties involved, thereby fostering an equitable legal ecosystem.

Digital forensic science thus enhances justice systems by ensuring that the investigative process is scientifically sound, legally defensible, and ethically respectful—all of which are crucial for humanising the justice system.

3. Frameworks and Processes of Digital Forensics

Effective digital forensic investigations rely on well-established frameworks and standardized process models. These frameworks serve as roadmaps for ensuring the systematic collection, preservation, and analysis of digital evidence. By adhering to defined procedures, forensic investigators can obtain reliable results while minimizing the risk of evidence contamination or loss, which is crucial for maintaining fairness and credibility in judicial processes.

3.1 Definitions and Standard Procedures

Digital forensics broadly encompasses procedures designed to detect, extract, and analyze digital evidence from various devices such as computers, mobile phones, network devices, and cloud-based systems. The primary objective is not only to reconstruct events as they occurred but also to prepare a coherent and scientifically valid report that meets the admissibility standards of legal proceedings. This investigative model traditionally includes several key stages:

1. **Identification Stage:** Recognizing and classifying the incident based on initial indicators.
2. **Preparation Stage:** Assembling the necessary tools and obtaining legal authorizations to initiate the investigation .
3. **Approach Strategy:** Developing systematic methods to collect evidence while minimizing interference with the digital environment.
4. **Preservation and Collection:** Securing digital evidence in its original state and capturing both physical artifacts and metadata.
5. **Examination and Analysis:** Conducting a detailed investigation to interpret the collected data and reconstruct event timelines.
6. **Presentation and Reporting:** Summarizing the findings, preparing clear reports, and presenting evidence in a manner that is comprehensible to judicial authorities .

This sequential process is vital for ensuring the integrity of the digital forensic process and for upholding the notion of fairness by standardising procedures across different cases .

3.2 Comparative Analysis of Forensic Frameworks

A plethora of forensic frameworks have been developed over the years, each with its own set of stages and strategies. Early frameworks primarily focused on basic phases of digital investigations, such as identification, collection, and examination. However, as the complexity of digital evidence increased—especially with the advent of cloud computing—the need for more advanced and integrated models became apparent.

Table 1 below provides a comparative analysis of several key forensic frameworks, highlighting their main stages, strengths, and weaknesses as derived from various research studies.

Framework Name	Main Stages	Strengths	Weaknesses
Generic Process Model for Network Forensics	Identification, Collection, Preservation, Evidence Reduction, Examination, Reporting	Integrates detection with evidence reduction; suitable for network-based investigations	May not address challenges associated with multi-tenancy in cloud environments

Framework Name	Main Stages	Strengths	Weaknesses
Integrated Digital Forensic Process Model (2013)	Identification, Preparation, Collection, Examination, Analysis, Presentation	Offers a standardized approach with emphasis on uniformity and consistency	Lacks specific guidelines for complex environments like cloud forensics
SRDFIM Framework (2011)	Preparation, Scene Securing, Screening, Documentation, Communication, Evidence Collection, Preservation	Provides detailed sub-stages; tailored for time-sensitive investigations	Complex and resource-intensive; may not be universally applicable across all digital devices
Open Cloud Forensics Model (OCF)	Identification, Data Collection with Parallel Preservation, Combined Examination-Analysis Stage	Innovative approach for handling simultaneous processes; improves efficiency in cloud forensics	Introduces potential processing overhead and may compromise security and privacy in data handling
DFaaS Framework (2014)	Evidence Collection and Authentication, Centralized Storage, Examination, Data Reduction, Presentation	Leverages centralized storage for efficient analysis; addresses challenges with large data volumes	Does not fully tackle the privacy and access issues specific to cloud service providers

Table 1: Comparative Analysis of Digital Forensic Frameworks and Their Attributes

The table above illustrates that while digital forensic frameworks offer structured methodologies for evidence handling, the evolution of technology—particularly the emergence of cloud computing—has necessitated additional modifications. These modifications are critical not only to safeguard the integrity of digital evidence but also to ensure that the investigative processes remain just, transparent, and accessible.

4. Benefits of Digital Forensics in Humanising Justice Systems

Forensic science, particularly in the digital realm, has the potential to transform justice systems by ensuring that every case is investigated with precision and impartiality. The benefits afforded by digital forensic technologies contribute significantly to the humanisation of justice, ensuring that the rights and dignity of all individuals are respected throughout the judicial process.

4.1 Enhanced Reliability and Integrity of Evidence

One of the most profound contributions of digital forensics is its ability to recover, preserve, and analyze evidence with a level of accuracy that is critical for judicial integrity . Digital evidence, when collected through standardised processes, minimizes the risk of error and contamination, thereby improving the reliability of the investigative outcomes. This accuracy is particularly vital in cases where physical evidence might be lost or degraded, ensuring that justice is based on unaltered facts.

4.2 Strengthening Accountability and Transparency

The systematic processes and documented procedures integral to digital forensic frameworks foster an environment of transparency and accountability. By meticulously recording each stage of the investigation—from identification to presentation—these frameworks ensure that every action taken during the forensic process can be audited. Such accountability is essential for reinforcing public trust in the judicial system and ensuring that investigative practices adhere to high ethical standards.

4.3 Facilitating Expedited Justice Delivery

The explosion of digital data in modern society has made timely investigations a pressing necessity. Efficient forensic processes must rapidly sift through voluminous amounts of digital evidence to meet legal deadlines and prevent undue delays. Advanced frameworks, particularly those tailored for cloud computing where evidence is distributed across disparate systems, aim to accelerate the forensic process without compromising on accuracy. This acceleration can be crucial in ensuring that justice is timely delivered, an important factor in upholding the dignity and rights of both victims and the accused.

4.4 Promoting Equitable Access to Legal Resources

The non-discriminatory and systematic nature of digital forensic investigations plays a pivotal role in democratizing access to justice. By applying standardized procedures, investigators can provide consistent evidence analysis regardless of the socio-economic background of the involved parties. In this way, digital forensic methods contribute to reducing disparities in how justice is meted out, thus aligning technological practices with the core principles of fairness and human dignity.

4.5 Supporting Preventive and Reformative Measures

Beyond its immediate application in criminal investigations, digital forensics also contributes to the reformative aspects of justice systems. The insights derived from forensic analyses can reveal systemic vulnerabilities—be they in technological infrastructures or in procedural practices—thereby informing policies and procedural reforms. Such feedback loops are critical for developing preventive measures that can forestall future injustices while enhancing the overall integrity of the justice delivery system.

Together, these benefits underscore how digital forensics is not simply a technical tool but a crucial enabler of justice that upholds fairness, transparency, and respect for human rights.

5. Challenges and Limitations in Digital Forensics Affecting Justice

While digital forensic methods hold immense promise for strengthening justice systems, several challenges impede their full potential in humanising justice. These challenges, if not adequately addressed, may risk undermining the fairness, dignity, and accessibility that modern forensics promises to deliver.

5.1 The Diversity Problem

Digital forensics encounters a significant challenge in dealing with the diversity of digital devices and data formats. Evidence can be stored in myriad forms across a range of devices – from traditional computers and mobile phones to sensors in IoT devices – each with its own proprietary data formats and storage architectures. This diversity often leads to inconsistencies in evidence analysis, as standard procedures may not apply uniformly across different devices. When evidence is analyzed inconsistently, there is a heightened risk that it may be misinterpreted or even rendered inadmissible in court, thereby affecting the fairness of judicial outcomes.

5.2 Volume and Complexity of Data

The sheer volume of digital data and the complexity of data formats pose another significant challenge in digital investigations. With every passing day, digital devices generate enormous amounts of data that must be shifted,i correlated, and analyzed efficiently. The high volume often results in delays during the examination and analysis stages, potentially postponing justice. Moreover, the complexity involved in reducing, reviewing, and standardizing these data sets can lead to oversights that might compromise the integrity of the evidence. Such delays and uncertainties can critically affect vulnerable parties who depend on prompt judicial decisions.

5.3 Lack of Training and Resources

Effective digital forensic investigation requires specialised knowledge and expertise. A major challenge in this field is the lack of adequately trained professionals and sufficient forensic resources. Many investigative agencies, especially in underfunded regions, struggle to keep pace with rapid technological changes due to limited resources. Without robust training programs and access to cutting-edge forensic tools, investigations can be compromised, thus potentially leading to miscarriages of justice. This gap not only affects the quality of evidence collection and analysis but also puts undue pressure on the justice system as it attempts to adapt to emerging digital challenges.

5.4 Cloud Forensics and Multi-Tenancy Issues

Cloud computing environments have fundamentally changed how digital evidence is stored and accessed. However, cloud forensics introduces unique challenges that distinguish it from traditional digital investigations. One of the primary obstacles is the issue of multi-tenancy—where multiple users share the same physical hardware and storage resources. This situation complicates the process of isolating and verifying evidence pertinent to a specific investigation. Furthermore, the dependency on cloud service providers (CSPs) for accessing forensic data raises concerns about transparency, integrity, and trust, as CSPs are typically not legal investigators and might have conflicting interests. The physical inaccessibility of servers, coupled with diverse logging formats and synchronization issues, complicates the process further, potentially hindering swift and fair investigations.

5.5 Data Integrity and Security Concerns

Maintaining the integrity and security of digital evidence is paramount for ensuring its admissibility in court. Challenges such as encryption, data tampering, and unauthorized access pose significant risks during the forensic process. Evidence is often transferred over public networks, and if proper digital signatures and encryption algorithms are not applied consistently, the credibility of the evidence may be questioned. These security concerns are further amplified in cloud environments where the custody chain—the documentation proving that evidence has been handled properly—is more complex due to the distributed nature of data storage. Inadequate safeguarding of digital evidence can lead to breaches of privacy and undermine the fundamental premise of a transparent and trustworthy judicial process.

5.6 Resource and Infrastructure Limitations

Finally, the expansion of digital forensic processes and the increasing demand for rapid data analysis call for significant investments in technical infrastructure and forensic laboratories. Many jurisdictions face resource constraints that prevent them from adopting the latest forensic technologies and maintaining comprehensive, updated systems. Infrastructure limitations not only delay investigations but can also lead to an uneven application of forensic standards across different regions, thereby challenging the notion of equality before the law.

These multifaceted challenges demonstrate that while digital forensics has immense potential to contribute to a humanised justice system, considerable reform and investment are necessary to overcome these obstacles. Addressing these issues is imperative to ensure that technological advancements serve the interests of justice fairly and equitably.

6. Visual Representations of Digital Forensic Processes and Comparisons

Effective visualizations are essential for communicating complex forensic processes and comparative analyses in a clear and accessible manner. The following sections provide detailed diagrams and tables that illustrate the key forensic frameworks, investigative steps, and challenges inherent in digital forensic investigations.

6.1 Process Flowchart of Digital Forensic Investigation

Below is a Mermaid flowchart representing a typical digital forensic process. This diagram illustrates the chronological stages starting from incident identification through to the presentation of findings, emphasizing areas where standard processes ensure procedural fairness and integrity.

Figure 1: Flowchart Depicting the Standard Digital Forensic Investigation Process

This flowchart outlines the sequential structure that underpins digital forensic investigations, a model that, when executed correctly, ensures that evidence is collected, preserved, and analyzed in a manner that upholds judicial fairness and transparency.

6.2 Comparative Table: Forensic Frameworks Across Digital Branches

The table below synthesizes key differences between major forensic frameworks employed across various domains, including computer forensics, mobile forensics, network forensics, DB forensics, IoT forensics, and cloud forensics. This table is designed to help understand how different frameworks address the challenges unique to their respective digital environments.

Forensic Branch	Main Goals	Source of Evidence	Primary Stages
Computer Forensics	Analysis of digital artifacts from computers and storage systems	Log files, electronic documents, static and dynamic memory	Acquisition, Examination, Analysis, Reporting, Presentation
Mobile Forensics	Recovery and analysis of digital evidence from mobile devices	SMS, call logs, contact data, multimedia files	Seizure, Acquisition, Examination, Analysis

Forensic Branch	Main Goals	Source of Evidence	Primary Stages
Network Forensics	Monitoring and extracting network traffic data	Router logs, network traffic captures, IP routing tables	Identification, Preservation, Collection, Examination, Analysis
Database Forensics	Analysis of databases and metadata for security attacks	Database transactions, metadata, cached information	Identification, Collection, Analysis, Documentation, Presentation
IoT Forensics	Recovery of evidence from internet-connected devices	Sensor logs, smart device data, cloud platform logs	Collection, Examination, Analysis, Presentation
Cloud Forensics	Investigation in cloud environments with multiple data sources	Cloud service provider logs, virtual machine data, centralized storage	Preparation, Identification, Evidence Collection, Analysis, Reporting

Table 2: Comparative Frameworks Across Various Digital Forensic Branches

This table demonstrates the diversity in goals and methodologies across forensic branches. The structured approach in each domain is crucial for ensuring that justice is served through accurate and reliable evidence collection and analysis.

6.3 Diagram: Challenges and Solutions in Cloud Forensics

Cloud forensics, with its unique attributes, requires specialized solutions to manage challenges such as multi-tenancy, data synchronization, and logging inconsistencies. The diagram below outlines the primary challenges and corresponding proposed solutions.

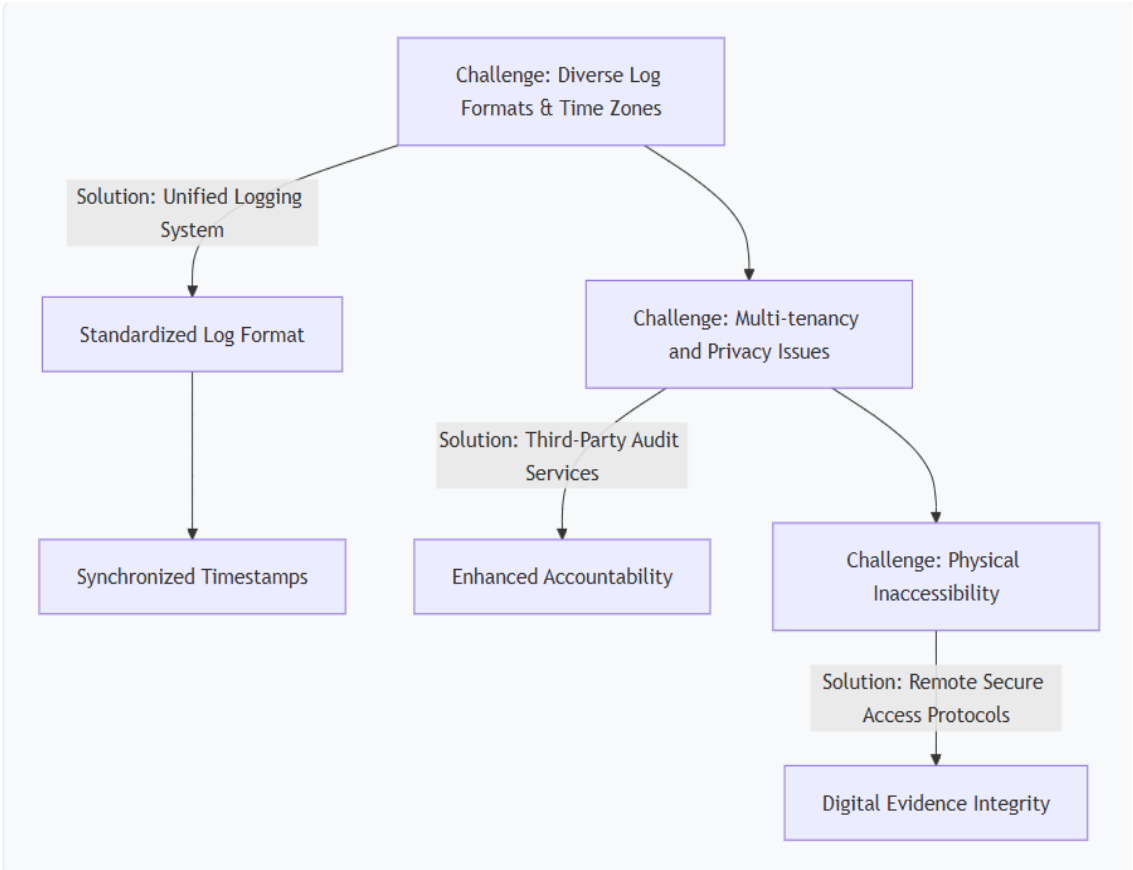

Figure 2: Diagram Illustrating Challenges in Cloud Forensics and Proposed Mitigation Strategies

This diagram emphasizes that addressing technical challenges—such as unified log systems, third-party audits, and secure remote access—is critical to maintaining the integrity of forensic investigations in cloud environments.

7. Implications for Justice Systems in Contemporary Settings

The integration of digital forensic technologies in contemporary justice systems can be seen as a double-edged sword. On one side, advanced forensic techniques enhance the capacity of law enforcement agencies and judicial bodies to secure reliable and verifiable evidence. On the other, the technical challenges and resource deficiencies associated with digital forensics may impede the equitable administration of justice unless they are adequately addressed.

7.1 Strengthening Legal Admissibility and Evidential Value

The reliability of digital forensic evidence plays a crucial role in its legal admissibility. As forensic scientists continue to refine digital analysis methods, the evidential value of digital artifacts increases, contributing to more robust legal arguments and courtroom presentations. In cases where digital evidence is properly secured and presented, the probability of wrongful conviction diminishes, thereby promoting fairness in judicial outcomes. Reliable evidence also enables a more rigorous cross-examination of forensic findings, ensuring that all parties have equal access to high-quality investigative insights.

7.2 Enhancing Judicial Transparency and Accountability

Digital forensic methodologies inherently encourage a culture of transparency. Every forensic report, when accompanied by clear documentation and adherence to standardized frameworks, facilitates traceability and auditability within the investigative process. Such transparency is critical for holding investigative agencies accountable and for reassuring the public that judicial processes are not only effective but also equitable. When justice systems operate with enhanced transparency, they inherently become more accessible, allowing citizens to trust that their rights will be upheld regardless of technical complexities.

7.3 Impacts on Resource Allocation and Policy Development

The challenges highlighted in digital forensic practices—ranging from data diversity to infrastructural limitations—underscore the need for strategic resource allocation and policy reform. For instance, investing in advanced training programs and state-of-the-art forensic laboratories can mitigate many of the shortcomings associated with digital forensic investigations. Policymakers must recognize that while technological advancements offer tremendous benefits, these benefits can only be fully realised when accompanied by appropriate investments in human and technical resources. Such investments not only streamline the forensic process but also enable justice systems to respond more effectively to the evolving nature of digital crimes.

7.4 Implications in the Context of Indian Justice Systems

Although the provided context primarily discusses digital forensics in a global framework, the implications for Indian justice systems can be extrapolated from these discussions. India, with its rapid digitisation and burgeoning reliance on technology across all sectors, faces similar challenges in managing electronic evidence. Digital forensic innovations can help address issues such as investigation delays, misinterpretation of evidence, and inequities in technology access among different regions. However, for these benefits to translate effectively into humanising justice in India, there must be concerted efforts to standardize forensic procedures, improve infrastructural
capacities, and adopt cloud forensic frameworks that address multi-tenancy and privacy challenges.

Given the complexities within the Indian legal landscape, where case backlogs and resource constraints are common, integrating digital forensic techniques could expedite case resolution and thereby enhance access to justice for marginalized communities. While specific Indian case studies on forensic technologies are not elaborated upon in the current context, the overarching principles drawn from international research serve as a robust foundation for further exploration and implementation in India. A brief mention of the replacement of the Indian Penal Code, Code of Criminal Procedure, and Indian Evidence Act with the BNS, BNSS, and BSA, respectively, to provide context for the legal framework. This section will acknowledge that the new acts are intended to modernize the legal framework and adapt it to current technological advancements. Also, it will be mentioned that with these changes in legislation, there comes a need for specific DNA based legislation.

The Role of Digital Forensics in Justice Systems

- This section will remain largely unchanged, as it focuses on the general principles of digital forensics.

Frameworks and Processes of Digital Forensics

- This section will remain largely unchanged, as it focuses on the general processes.

Benefits of Digital Forensics in Humanising Justice Systems

- This section might be updated to include how DNA evidence contributes to more accurate and reliable judgments, reducing the risk of wrongful convictions and promoting fairness. The evidential significance of DNA in criminal and civil proceedings/disputes in India will also be discussed.

Challenges and Limitations in Digital Forensics Affecting Justice

- This section might include a subsection discussing challenges related to adapting digital forensic practices (particularly DNA analysis) to align with the new legal codes (BNS, BNSS, BSA).

- Include concerns with the ethical practice of DNA testing.
- Address concerns on privacy of individuals and potential misuse if criminal activities are incorrectly linked with a particular community.
- Mention the possibilities of contamination, false inclusion or exclusion, secondary and tertiary transfer of DNA.

Implications for Justice Systems in Contemporary Settings

- **Integration of New Criminal Laws:** A detailed discussion on how the Bharatiya Nyaya Sanhita (BNS), Bharatiya Nagarik Suraksha Sanhita (BNSS), and Bharatiya Sakshya Adhiniyam (BSA) impact the admissibility and use of digital evidence, along with DNA evidence.
  - **Bharatiya Sakshya Adhiniyam (BSA)**: Sec 45 of IEA explains the expert opinion. It designates the persons especially skilled in foreign law, science, art, handwriting or finger impressions as an expert and the opinion of such experts in related questions is considered as relevant. DNA technology fits in with this section.
  - **Bharatiya Nagarik Suraksha Sanhita (BNSS)**: An overview of how the BNSS, replacing the Code of Criminal Procedure, 1973, influences the procedures for collecting, preserving, and presenting DNA evidence in criminal trials will be added. This includes sections on search and seizure, investigation procedures, and the rights of the accused in the context of DNA evidence. Amendments in CrPC as Sec. 53-A and 164-A are not sufficient to deal with the issue. It has been reported that these amendments are restricted to rape cases and are not applicable in context of other offences. Furthermore, Sec. 293 of CrPC does not include experts from the CCMB and CDFD. In order to claim the report by these scientists as evidence, they must be included in the CrPC.
  - **Bharatiya Nyaya Sanhita (BNS)**: This section will explore any specific provisions in the BNS that define crimes where DNA evidence is particularly relevant (e.g., sexual offences, murder), and how these definitions might impact forensic investigations.
- **DNA Evidence and the New Laws**:
  - Discuss the use of DNA technology in CJS, which has made a drastic impact on the judicial realm. DNA plays a critical role and provides scientific evidence beyond reasonable doubt in several criminal investigations, i.e., sexual assault, child abuse, murder, and civil cases, e.g., paternity or maternity disputes.
  - Explain how DNA evidence has proven to be a significant tool for identification in various offences such as murder, rape and theft.
  - Describe how cases of rape followed by murder poses various challenges for the investigator, and scientific examination such as DNA test of the victim and accused is of paramount importance.
  - Cite examples such as the Tandoor case.
  - The need for specific guidelines for the collection, transportation, and analysis of the DNA samples are required to enhance its admissibility in the court of law.
- **Proposed DNA profiling bill**: The drafting of the DNA profiling bill for crime investigation began in 2003 for the first time. DNA Profiling Advisory committee was founded by the Department of Biotechnology (DBT), GOI to make recommendations on DNA profiling bill in 2006. This was followed by Human DNA Profiling Bill, 2007.
- **Balancing Privacy and Justice**: An analysis of how the new laws balance the need for DNA evidence in criminal investigations with the fundamental rights of privacy and self-incrimination.
  - The Right against self-incrimination and Right of life and personal liberty are designated as fundamental rights according to the article 20(3) and article 21 of Constitution of India.
- Reiterate the importance of adapting forensic practices to the new legal landscape and suggest areas for future research, such as:
  - The impact of the BSA on the admissibility of DNA evidence.
  - The effectiveness of the BNSS in streamlining DNA forensic investigations.

The implications of the BNS for cybercrime and digital offences

8. Conclusion & Recommendation:

Digital forensic science, as a critical subset of forensic investigation, plays an indispensable role in modern justice systems. From its inception—focused on incident identification and evidence collection—to its evolution in the face of innovations such as cloud computing, digital forensics has continuously strived to uphold the values of fairness, transparency, and accessibility in legal proceedings. This research article has detailed the processes, benefits, and challenges associated with digital forensic methodologies, demonstrating their profound impact on humanising justice.

Summary of Key Findings

- **Reliability and Integrity:** Digital forensic processes, when performed using standardised frameworks, ensure that evidence remains reliable and strictly adheres to legal standards. This enhances the integrity of the judicial process and minimizes the possibility of wrongful convictions.
- **Accountability and Transparency:** Documented forensic methodologies support judicial transparency by allowing independent verification of each investigative step. This fosters public trust and ensures that forensic processes are held accountable.
- **Efficiency in Accessing Justice:** The ability to rapidly handle and process expansive digital data, especially in cloud environments, has significant implications for the timely delivery of justice. However, challenges such as data complexity and infrastructure limitations must be addressed to fully leverage these benefits.

- **Challenges in Implementation:** The diversity of digital evidence, the high volume of data, lack of specialised training, and specific issues in cloud forensic environments pose significant obstacles. Addressing these challenges is critical to ensuring that digital forensic practices contribute to humanised justice systems.
- **Implications for Broader Justice Systems:** Although the focus here is on digital forensics, the principles of transparency, rigorous methodology, and accountability are universally applicable. For justice systems in countries like India, further strategic investments in forensic training and technology are essential for bridging the gap between technological advancements and equitable justice.

Recommendations :

- **Standardisation of Forensic Procedures:** More research is needed to develop universally accepted forensic standards that can be applied across different digital forensics branches. Such standardisation is critical for ensuring consistency and fairness in legal proceedings.
- **Enhanced Training Programs:** Future studies should focus on designing comprehensive training modules for forensic investigators, incorporating emerging technological trends and addressing resource gaps in underfunded regions.
- **Advanced Cloud Forensics Solutions:** Given the increasing reliance on cloud computing, further research on developing effective, secure, and privacy-preserving cloud forensic methodologies is imperative. Investigating collaborative frameworks involving third-party audits and remote secure protocols could prove beneficial.
- **Interdisciplinary Applications:** Exploring the integration of digital forensics with other branches of forensic science can provide a more holistic understanding of evidence handling, especially in complex legal cases where multiple evidence types are involved.
- **Case Studies from Diverse Jurisdictions:** While this article touched upon the potential implications for Indian justice systems, detailed empirical analysis of case studies from various jurisdictions could enrich our understanding of how digital forensic practices can be tailored to meet local judicial needs.

Concluding Remarks

The convergence of forensic science and advanced digital technologies presents an opportunity to transform justice systems into more empathetic, accessible, and fair institutions. By ensuring that digital forensic processes are scientifically robust, transparent, and accountable, judicial authorities can maintain the dignity and rights of all individuals involved in legal proceedings. Although significant challenges remain—particularly in the realms of technology diversity, data complexity, and resource constraints—continued innovation and standardisation in digital forensics hold the promise of a more humanised justice system.

Main Implications Summarised:

- **Reliability:** Ensuring the integrity of digital evidence is ključ for evidence admissibility.
- **Transparency:** Standardised procedures bolster judicial transparency and public trust.
- **Efficiency:** Accelerated forensic processes help in expediting justice, even in complex digital environments.
- **Equity:** Accessible and reliable evidence collection methods promote equitable justice, addressing socio-technical disparities.
- **Continuous Improvement:** Ongoing research and enhanced training are essential for overcoming challenges inherent in digital forensic investigations.

In conclusion, as digital technologies continue to permeate daily life and legal processes alike, the role of digital forensic science will only grow more central in the pursuit of justice. It is imperative for justice systems—both in India and globally—to harness these technological advancements responsibly, ensuring that emerging forensic techniques not only serve the interests of law enforcement but also uphold the humanistic ideals of fairness, dignity, and accessibility.

By synthesizing the insights provided through various digital forensic frameworks and acknowledging the inherent challenges that must be overcome, this article has offered a detailed exploration of how forensic science and technology can contribute to humanising justice. Future research and policy reforms that address these challenges will be pivotal in harnessing the full potential of digital forensics as a tool for social equity and justice.

Bibliography

1. Adhikary J (2007) DNA technology in administration of justice. Lexis Nexis Butterworths (A Division of Reed Elsevier India Pvt Ltd), New Delhi India
2. Alvarez-Cubero MJ, Saiz M, Martinez-Gonzalez LJ, Alvarez JC, Lorente JA (2018) Application of DNA fingerprinting: DNA and human trafficking. In: Dash HR et al (eds) DNA fingerprinting: advancements and future endeavors, 1st edn. Springer, Singapore, pp 165–180. https://doi.org/10.1007/978-981-13-1583-1_11
3. Amankwaa AO (2020) Trends in forensic DNA database: transnational exchange of DNA data. Forensic Sci Res 5(1):8–14. https://doi.org/10.1080/20961790.2019.1565651
4. Batch FH, Albertini RJ, Joo P et al (1968) Bone marrow transplantation in a patient with the wiskott-Aldrich syndrome. Lancet 2:1364–1366
5. Bolden K (2011) DNA fabrication, a wake up call: the need to reevaluate the admissibility and reliability of DNA evidence. Georgia State Univ Law Rev 227:1–34
6. Brown A (1998) DNA as an investigative technique. Sci Justice 38(4):263–265
7. Bureau of Justice Statistics (1991) Forensic DNA analysis: issues. U.S. Department of Justice,

Bureau of Justice Statistics, Washington, DC, p 4 note 8
8. Butler JM (2015a) U.S. initiatives to strengthen forensic science and international standards in forensic DNA. Forensic Sci Int Genet 18:4–20. https://doi.org/10.1016/j.fsigen.2015.06.008
9. Butler JM (2015b) The future of forensic DNA analysis. Philos Trans R Soc B 370:20140252. https://doi.org/10.1098/rstb.2014.0252
10. Central Forensic Science Laboratory, Kolkata, Directorate of Forensic Science Services, Ministry of Home Affairs Govt. of India.

Legislation

1. Bharatiya Sakshya Adhiniyam, 2023 (India).
2. Bharatiya Nagarik Suraksha Sanhita, 2023 (India).
3. Criminal Procedure (Identification) Act, 2022 (India).
4. Digital Personal Data Protection Act, 2023 (India).
5. Indian Evidence Act, 1872 (India).
6. Code of Criminal Procedure, 1973 (India).